

Marruecos y el Ciberespacio

Anticipando un mundo ciberseguro

Control de versiones

Versión	Por	Descripción	Fecha	Evento
1.0	#016	Versión inicial	Septiembre de 2026	

Índice

Parte I. Los fundamentos	9
Introducción	9
Principales hallazgos.....	9
Resumen ejecutivo	11
Metodología de trabajo	12
Parte II. Fundamentos estratégicos y políticos	14
Introducción	14
Política y geopolítica.....	15
El Majzén	18
Prioridades estratégicas.....	20
Parte III. La arquitectura de seguridad e inteligencia	24
La comunidad de inteligencia	24
DGED 25	
DGST 28	
Funciones de inteligencia relevantes de la DGSN	32
Orden público y seguridad interna	34
DGSN 35	
BCIJ 37	
Gendarmería Real.....	39
Fuerzas Auxiliares.....	41
Fuerzas Armadas e inteligencia militar.....	43
Arquitectura de mando de las FAR	45
Oficinas 2. ^a y 5. ^a	47
Guardia Real.....	48
Regiones militares y postura en el Sáhara Occidental	49
Otros actores relevantes	50
Empresas privadas.....	52
Universidades	54
Delincuencia.....	55
Coordinación y supervisión	57
Parte IV. El ecosistema cibernético marroquí	62
El ciberespacio marroquí	62
Derecho y regulación	62
Ciberseguridad defensiva y respuesta a incidentes	66
Recopilación de inteligencia y vigilancia	68
Ciberguerra militar, guerra electrónica y C4ISR	70
Ciberdelincuencia y análisis forense digital.....	71
Las fuerzas del orden en el ciberespacio	72
Ciberdelincuencia.....	72
Hacktivismo y confrontación de información.....	74
Otros actores	77
Proveedores privados	77
Proveedores extranjeros	78

El ámbito académico	80
Grupos APT.....	80
Dependencias clave.....	81
Parte V. Valoración	88
Modelo de capacidades	88
Limitaciones y vulnerabilidades	90
Conclusiones	91
Referencias.....	93
Acrónimos.....	106

Índice de tablas

Tabla 1. El Estrecho de Gibraltar: tres presiones estratégicas convergentes sobre la política de Marruecos hacia España.	18
Tabla 2. Los seis teatros de prioridad estratégica de Marruecos, ordenados, con su base evidencial principal y la confianza estimada.	20
Tabla 3. Episodios de cruce migratorio en Ceuta y Melilla, 2021-2026: eventos distintos, cifras solapadas.	22
Tabla 4. Los organismos marroquíes de inteligencia civil y policía de un vistazo.	24
Tabla 5. Sucesión en la dirección de la DGED, la DGST y la DGSN.	25
Tabla 6. Cuestiones de atribución en disputa en el registro de Pegasus y Jabaroot de Marruecos.	30
Tabla 7. Las cuatro fuerzas de seguridad interna de Marruecos de un vistazo.	34
Tabla 8. Comparación de cuatro organismos estructuralmente distintivos de las Fuerzas Armadas.	43
Tabla 9. Tres relaciones con proveedores extranjeros de tecnología de vigilancia identificadas para Marruecos.	53
Tabla 10. Operaciones documentadas de orden público y seguridad de 2025-2026, por fecha.	56
Tabla 11. Los principales organismos formales de coordinación y supervisión de seguridad de Marruecos.	60
Tabla 12. Instrumentos legales y regulatorios de Marruecos sobre ciberespacio y protección de datos.	65
Tabla 13. Casos notables de cibercrimen con motivación financiera y operaciones de cooperación.	73
Tabla 14. Teorías de atribución en disputa para la campaña Jabaroot/JabaROOT DZ.	75
Tabla 15. Equipos CERT/CSIRT registrados en Marruecos listados en el directorio de miembros de FIRST.	78
Tabla 16. Proveedores comerciales extranjeros nombrados en esta recopilación, confirmados y comprobados-y-ausentes.	79
Tabla 17. Sistemas de cable submarino que dan servicio a Marruecos, y el contraste de no toma de tierra de 2Africa.	82
Tabla 18. Estructura de propiedad de los tres operadores de red móvil autorizados de Marruecos.	84
Tabla 19. Presencia internacional de nube a hiperescala y CDN relevante para Marruecos.	85
Tabla 20. Principales limitaciones y vulnerabilidades del dominio cibernético de Marruecos, con confianza estimada.	91

Índice de figuras

Figura 1. Los canales constitucional y económico del Majzén, simplificados (ambos parten del rey y no del gobierno electo).	19
Figura 2. Líneas de dependencia jerárquica simplificadas de la arquitectura marroquí de inteligencia civil y policía (el rey Mohamed VI se sitúa por encima de ambas ramas como comandante supremo).25	
Figura 3. El emblema de la DGSN, calcado del propio informe anual de 2021 del servicio.	37
Figura 4. El emblema asociado a la Gendarmerie Royale en fuentes abiertas (salvedad de procedencia más abajo).	41
Figura 5. El emblema de las Fuerzas Auxiliares, procedente de un anuncio oficial de reclutamiento de la Inspection Générale des Forces Auxiliaires.	43
Figura 6. Arquitectura de mando de las FAR, en la medida en que las fuentes abiertas permiten afirmarla con confianza (la línea de dependencia de la Guardia Real está disputada, no resuelta, en este diagrama).	46
Figura 7. La insignia de las FAR, en uso continuo en los artículos de Wikipedia sobre las FAR desde 2008.	47
Figura 8. El emblema de la Guardia Real, procedente de un anuncio oficial de reclutamiento de la Garde Royale.	48
Figura 9. El Muro/Berma marroquí: sectores de construcción y localidades encerradas reportados (cifras de fuente única y señaladas como no corroboradas; ver texto).	49
Figura 10. El aparato de coordinación de seguridad de Marruecos, consolidado (los vínculos de fusión personal y la frecuencia de reunión no documentada se señalan explícitamente en lugar de suavizarse).	60
Figura 11. Estructura institucional de la DGSSI: direcciones, y su relación regulatoria con las entidades de infraestructura vital y los proveedores de nube cualificados.	66
Figura 12. El logotipo institucional de la DGSSI, obtenido directamente del sitio web oficial del organismo.	67
Figura 13. El panorama de hacktivismo de Marruecos: tres agrupaciones funcionalmente distintas y no una única rivalidad de dos bandos.	77
Figura 14. Topología de cables submarinos de Marruecos: tomas de tierra agrupadas en la costa norte frente al punto de estrangulamiento del Estrecho de Gibraltar, con 2Africa mostrado como un sistema de referencia sin conexión.	83
Figura 15. Estructura de propiedad de los tres operadores de red móvil de Marruecos.	84
Figura 16. El modelo de capacidad cibernética de tres líneas de Marruecos: ofensiva/recopilación, defensiva, e influencia/operaciones de información, cada una anotada con su vector de dependencia extranjera dominante y su confianza evidencial.	89

Parte I. Los fundamentos

Introducción

Este informe analiza el ecosistema de seguridad, inteligencia y defensa de Marruecos, con especial atención al ciberespacio —es decir, a los ecosistemas de ciberseguridad, ciberinteligencia y ciberdefensa del país—. Examina el marco político e histórico del Reino, el Majzén como concepto central de gobernanza del país, las prioridades estratégicas de Marruecos en los teatros que más le importan, la estructura y el funcionamiento de sus comunidades de inteligencia, orden público y fuerzas armadas, el ecosistema más amplio de actores privados, académicos y criminales que las rodea, la actividad de Marruecos en el ciberespacio en particular —desde su marco legal hasta los respectivos papeles de los servicios de inteligencia, las fuerzas armadas, las fuerzas del orden y los actores civiles en ese ámbito— y, por último, las dependencias digitales y el modelo de capacidades que, en conjunto, determinan hasta qué punto Marruecos puede sostener esta actividad.

Se trata de una reconstrucción completa del informe desde cero, y no de una actualización de una edición anterior: cada sección siguiente se basa en una recopilación y un análisis de fuentes abiertas realizados de nuevo específicamente para esta edición, que cubren fuentes marroquíes, españolas y argelinas en todos los ámbitos que requiere el esquema que sigue, en lugar de en material heredado de un informe anterior. Los hallazgos relevantes para España se integran directamente en la sección que ya cubre el terreno correspondiente —la migración y la presión fronteriza dentro de Prioridades estratégicas, la práctica de presión híbrida dentro del capítulo sobre la comunidad de inteligencia, y la actividad de espionaje y vigilancia dentro de Recopilación de inteligencia y vigilancia— en lugar de aislarse en un capítulo independiente, dado que la conducta de Marruecos hacia España se entiende mejor como un hilo que recorre cada ámbito que como un tema autónomo. A continuación se presenta una sinopsis de los principales hallazgos del informe, para el lector que desee obtener el panorama esencial antes de adentrarse en el análisis que lo sustenta.

Principales hallazgos

El modelo de gobernanza de la seguridad de Marruecos está centrado en Palacio y no distribuido institucionalmente, y este único hecho organiza casi todo lo demás en este informe. El Majzén —examinado más adelante no como una metáfora, sino como un conjunto identificable de instituciones, desde el Gabinete Real y sus asesores hasta el cuerpo de walis, el holding real Al Mada y empresas estatales como Maroc Telecom— coordina las palancas de seguridad, económicas e informativas en torno a las propias prioridades de Palacio, con una supervisión parlamentaria y judicial que este informe considera, según la mejor evidencia independiente disponible, consultiva como mucho y, en varios aspectos, completamente inexistente. Es casi seguro que este arreglo persista tras las elecciones legislativas del 23 de septiembre de 2026 independientemente de su resultado (confianza: alta), dado que la autoridad cotidiana sobre inteligencia, adquisiciones de defensa, política sobre el Sáhara Occidental y buena parte de la política cibernética discurre a través de instituciones adyacentes a Palacio y no a través del gobierno electo.

Dentro de ese modelo, la función se distribuye y no se duplica entre los organismos que este informe perfila en detalle: la DGED se ocupa de la inteligencia exterior y la diplomacia de seguridad en el Sahel; la DGST se ocupa del contraespionaje interno y, según la evidencia valorada en Recopilación de inteligencia y vigilancia, de la capacidad de ciber-vigilancia de origen

comercial de Marruecos; la DGSN es la policía civil nacional, fusionada con la DGST en su cúpula desde 2015 en la única persona de Abdellatif Hammouchi, un hecho estructural sin equivalente europeo directo examinado en este informe; las FAR proporcionan la defensa convencional y mandan el teatro del Sáhara Occidental; y la DGSSI, ubicada dentro del estamento de defensa y no en un ministerio civil, es la autoridad nacional de ciberseguridad, con maCERT integrado en ella como función de respuesta a incidentes. Es muy probable que esta distribución, y la posición de Palacio por encima de todo ello, siga siendo la lógica organizadora de la gobernanza de seguridad marroquí durante el resto de esta década (confianza: moderada).

En materia de capacidad cibernética específicamente, el modelo observado por este informe está impulsado por la adquisición más que por el desarrollo propio: no se identificó ningún actor cibernético ofensivo atribuido al Estado marroquí en ningún catálogo de ciberinteligencia de amenazas monitorizado, pero una secuencia bien documentada de relaciones con proveedores comerciales —Hacking Team desde 2009, Pegasus de NSO Group desde al menos 2017— dotó a la DGST de una capacidad de vigilancia confirmada mediante análisis forense, utilizada contra periodistas y activistas nacionales y, según el balance de la evidencia, contra altos cargos españoles. En el plano defensivo, la DGSSI y maCERT han construido un marco jurídicamente estructurado —la Ley 05-20, el régimen de designación de infraestructuras críticas IIV, y la aplicación de la protección de datos por la CNDP en virtud de la Ley 09-08— cuya eficacia práctica y cotidiana este informe pudo verificar de forma independiente en mucha menor medida, dada la persistente falta de datos de rendimiento publicados comparables a los que habitualmente publican los CERT nacionales con más recursos.

La autoría de la campaña de pirateo y filtración Jabaroot/JabaROOT de 2026 contra instituciones marroquíes sigue siendo genuinamente controvertida entre las fuentes de este informe, entre al menos una teoría de hacktivismo argelino, una teoría de dirección estatal argelina, una teoría de operador solitario y una teoría que señala a un antiguo alto cargo de la DGED como fuente. Este informe no da por establecida ninguna de ellas, y las mantiene todas junto con su respectiva fuente, en lugar de converger en una sola por conveniencia narrativa.

La disputa del Sáhara Occidental y la rivalidad con Argelia que esta sostiene son los dos motores estratégicos organizadores de este informe, presentes en casi todos los capítulos: explican la postura militar de Marruecos a lo largo del Muro marroquí, la mayor parte de su exposición al hacktivismo y a las operaciones de información, y una política exterior que ha ido intercambiando cada vez más el reconocimiento de la soberanía marroquí sobre el territorio —por parte de Estados Unidos, Israel y un grado creciente de respaldo en el Consejo de Seguridad de la ONU— por la normalización y la profundización de la cooperación industrial de defensa con Washington y Tel Aviv.

España ocupa una posición genuinamente multifacética en este panorama: un socio de seguridad con relaciones de enlace reales y valiosas en materia de contrterrorismo y contranarcóticos; un objetivo demostrado, de forma más patente a través de las infecciones por Pegasus confirmadas mediante análisis forense en 2021 contra altos cargos del propio Estado español y de un proceso judicial en curso en 2026 ante la Audiencia Nacional que alcanza a personal de la DGST/DGED; una dependencia estructural, a través de la infraestructura submarina eléctrica y de comunicaciones que cruza el Estrecho de Gibraltar y que se examina en detalle en Dependencias clave; y un objeto de presión migratoria y diplomática calibrada durante las sucesivas crisis de Ceuta. Mantener estos papeles a la vista simultáneamente, en lugar de reducirlos a un marco alarmista o a uno acrítico, es la principal aportación metodológica de este informe a la forma en que debe interpretarse la relación entre España y Marruecos, y cada uno de ellos se desarrolla con su cadena probatoria completa, sus etiquetas WEP y sus niveles de confianza en los capítulos que siguen.

Resumen ejecutivo

Marruecos entra en la segunda mitad de esta década gobernado, en la práctica, desde Palacio y no desde ninguna de sus instituciones electas. El relato que hace este informe del Majzén —la red de asesores reales, gobernadores territoriales y participaciones empresariales y mediáticas vinculadas a Palacio que rodea a la monarquía— no es una metáfora, sino una descripción de cómo se mueven realmente los nombramientos, los recursos y la dirección estratégica a través del Estado marroquí, con una supervisión parlamentaria y judicial que este informe considera escasa en el mejor de los casos y, específicamente en el ámbito de la seguridad y la inteligencia, en gran medida inexistente. Las elecciones legislativas del 23 de septiembre de 2026, y las reivindicaciones socioeconómicas a las que dio voz el movimiento de protesta Gen Z 212 de 2025, son la prueba más trascendente a corto plazo de la durabilidad de este arreglo, pero nada en la evidencia valorada aquí sugiere que la estructura de poder subyacente esté ella misma en juego en las urnas.

Dentro de esa estructura, el aparato de seguridad e inteligencia de Marruecos se divide claramente por función y no por rivalidad: la inteligencia exterior y la diplomacia en el Sahel recaen en la DGED, el contraespionaje interno y, según la evidencia de este informe, la ciber-vigilancia ofensiva recaen en la DGST, y el orden público ordinario recae en la DGSN —las dos últimas fusionadas en su cúpula desde 2015 en la persona de Abdellatif Hammouchi, una concentración de autoridad sin paralelo directo entre los comparadores de este informe—. El hallazgo individual más trascendente de esta arquitectura es de naturaleza forense y no testimonial: laboratorios técnicos independientes han confirmado que el programa espía Pegasus de NSO Group fue utilizado contra periodistas, activistas y, según el balance de la evidencia, contra el propio Presidente del Gobierno y la Ministra de Defensa de España, una capacidad que este informe califica de comprada más que desarrollada, dado que no se identificó en ninguna parte del material revisado un programa marroquí de desarrollo cibernético ofensivo atribuido al Estado. Un hilo aparte, aún sin resolver, que recorre 2026 es la campaña de pirateo y filtración Jabaroot contra instituciones marroquíes, cuya autoría este informe no pudo establecer entre varias afirmaciones contrapuestas y mutuamente incompatibles, por lo que se presenta como controvertida y no como resuelta.

Dos relaciones exteriores condicionan casi todo lo demás en este panorama. Argelia y la disputa del Sáhara Occidental constituyen la rivalidad estratégica organizadora detrás de la postura militar de Marruecos, su cortejo diplomático a Washington, Tel Aviv y un bloque cada vez más consolidado en el Consejo de Seguridad de la ONU, y la mayor parte de la actividad hacktivista y de operaciones de información documentada en los capítulos de ciberespacio de este informe. España, por su parte, resulta imposible de describir en un solo registro: un socio de seguridad genuino en contraterrorismo y contranarcóticos; un objetivo de vigilancia demostrado al más alto nivel de su propio gobierno; un vecino estructuralmente dependiente a través de los cables submarinos y las interconexiones eléctricas que cruzan el Estrecho de Gibraltar; y, durante las sucesivas crisis migratorias de Ceuta, un objeto de presión marroquí calibrada. El argumento central de este informe sobre la relación España-Marruecos es que estas cuatro facetas son ciertas simultáneamente, y que interpretar la relación a través de una sola de ellas —asociación o amenaza— no permite comprender cómo utiliza Rabat realmente los instrumentos de que dispone. En el plano defensivo, Marruecos ha construido un marco de ciberseguridad jurídicamente integral bajo la DGSSI y su CERT nacional, maCERT, que abarca la protección de datos, la designación de infraestructuras críticas y la cooperación en respuesta a incidentes con socios internacionales; este informe pudo verificar de forma sustancialmente más sólida la existencia de esa arquitectura legal que su eficacia operativa cotidiana, ante la falta de datos de rendimiento publicados que habitualmente difunden los CERT nacionales con más recursos. Esa asimetría —sólida sobre el papel, escasamente evidenciada en la práctica— se repite a lo largo de la valoración que este

informe hace de las instituciones marroquíes en general, y los lectores deben sopesar cada juicio que sigue frente al nivel de confianza que se le atribuye, y no frente a la confianza que transmite la propia comunicación pública de la institución correspondiente.

Metodología de trabajo

Este informe se elaboró mediante un ciclo de inteligencia estructurado, implementado como una cadena de habilidades especializadas, cada una responsable de una fase y auditable de forma independiente de las demás. La adquisición recopila material bruto de fuentes abiertas —prensa marroquí, española y argelina, sitios gubernamentales y regulatorios oficiales, producción de centros de análisis, informes técnicos forenses y, cuando son de acceso público, registros judiciales— registrando cada elemento en un archivo por referencia con su URL de origen, autor, institución, fecha de publicación y fecha de adquisición, y una clasificación explícita de fiabilidad de seis niveles (desde documentos legales/oficiales primarios hasta fuentes partidistas o terciarias), sin análisis ni interpretación en esa fase. El procesamiento traduce y normaliza el material que no está en inglés a un idioma de trabajo común, preservando entidades nombradas, transliteraciones y la fidelidad de las citas, de modo que las decisiones de traducción sigan siendo visibles y auditables en lugar de quedar absorbidas silenciosamente en el análisis posterior.

Una serie de pasadas de investigación por ámbito —que cubren el marco político y del Majzén de Marruecos, sus prioridades estratégicas, su comunidad de inteligencia, sus instituciones de orden público y militares, los mecanismos de coordinación y supervisión, su marco legal y defensivo en el ciberespacio, su panorama de cibercrimen y hacktivismo, y sus dependencias digitales clave y su modelo de capacidades— produjo cada una un documento de trabajo para su ámbito, aplicando de forma consistente las Palabras de Probabilidad Estimativa y la clasificación de fuentes OTAN/Almirantazgo, de modo que el producto final hable con una sola voz analítica con independencia de qué pasada redactó cada sección. A continuación, la fase de producción ensambló esos documentos de trabajo en el documento estructurado y referenciado que el lector tiene ahora ante sí, trasladando cada etiqueta WEP, nivel de confianza y cita exactamente como los registró la fase de investigación, en lugar de reanalizar el material subyacente, añadiendo además las figuras y tablas necesarias para presentar con claridad las estructuras de relaciones y las enumeraciones.

Esta edición es una reconstrucción completa desde cero, y no una mera actualización: cada ámbito fue investigado de nuevo íntegramente para esta edición, en lugar de trasladar el análisis de un informe anterior, de modo que el lector pueda considerar que cada cita de los capítulos siguientes pertenece específicamente a esta ronda de recopilación. Este informe se construye exclusivamente a partir de fuentes abiertas: publicaciones oficiales marroquíes, españolas, estadounidenses, de la UE y de la ONU; prensa marroquí, española, francesa e internacional; producción académica y de centros de análisis; e informes técnicos de proveedores de ciberinteligencia de amenazas y laboratorios forenses. La recopilación se desarrolló hasta el 8-9 de septiembre de 2026, con una ventana sustantiva de referencia que abarca de 2020 a esa fecha, empleándose el material anterior únicamente para establecer la trayectoria institucional.

Los juicios analíticos se expresan mediante la convención de Palabras de Probabilidad Estimativa (WEP, por sus siglas en inglés) derivada de la ICD 203 —casi seguro (95-99 %), muy probable (80-95 %), probable (55-80 %), posibilidad prácticamente equivalente (45-55 %), improbable (20-45 %), muy improbable (5-20 %), escasa probabilidad (1-5 %) —, cada una emparejada con un nivel de confianza explícito (alto/moderado/bajo) que es independiente de la banda de probabilidad; los hechos directamente documentados no llevan banda WEP, y cada cita lleva además una calificación OTAN/Almirantazgo (A-F para la fiabilidad de la fuente, 1-6 para la

credibilidad de la información), reproducida a partir del registro de recopilación y nunca alterada durante la redacción. Cuando un actor estatal tiene un incentivo documentado para negar o engañar sobre un tema —la atribución de Pegasus y la actividad de los servicios de inteligencia, sobre todo—, las negaciones oficiales se tratan como datos sobre la posición declarada del Estado, no como evidencia que las refute, y la misma disciplina se aplica a las afirmaciones hacktivistas y de incidencia advertidas con fines propagandísticos.

Varias pasadas de recopilación de esta edición operaron durante parte de su recorrido bajo un presupuesto limitado de herramientas de búsqueda, y en esos casos recurrieron a la obtención directa a partir de fuentes canónicas conocidas (sitios gubernamentales oficiales, referencias enciclopédicas consolidadas y dominios de proveedores y prensa previamente identificados) en lugar de a una búsqueda amplia; toda fuente obtenida de este modo se clasifica y señala en consecuencia, en lugar de presentarse con una confianza inflada que no merece, y varias secciones indican explícitamente, en el punto en que surge la carencia, dónde esto limitó la profundidad evidencial de un subtema concreto.

Las principales incertidumbres del informe, cada una señalada explícitamente en el punto en que surge y no suavizada, son: la cadena de mando precisa que hay detrás del uso por Marruecos de Pegasus y otras herramientas comerciales de intrusión, que descansa sustancialmente en evidencia testimonial y forense de dispositivos y no en prueba documental de la titularidad institucional; la autoría real de las filtraciones Jabaroot/JabaROOT de 2026, disputada entre al menos cuatro teorías distintas; la opacidad casi total de las Oficinas 2.^a y 5.^a de las FAR y de varios de los propios canales informales de decisión del Majzén, que las fuentes abiertas solo iluminan de forma marginal; y el papel práctico y cotidiano de recopilación cibernética, si lo hay, de la propia Dirección de Inteligencia General de la DGSN, sobre el que apenas existe información independiente. Cada una se aborda de la misma manera a lo largo de este informe: declarando la carencia explícitamente, manteniendo una banda WEP y un nivel de confianza asociados a cualquier juicio que la salve, y negándose a convertir una afirmación de fuente única o testimonial en un hecho establecido simplemente porque encaje en una narrativa por lo demás plausible.

Parte II. Fundamentos estratégicos y políticos

Introducción

La estatalidad moderna de Marruecos descansa sobre la dinastía alauita, que ha gobernado de forma continua desde el siglo XVII y a la que tanto el orden constitucional posterior a la independencia como el actual tratan como la institución central organizadora del Estado y no meramente como su cabeza ceremonial. Francia y España establecieron protectorados separados sobre el territorio marroquí en 1912, administrados respectivamente desde Rabat y desde una zona norteña y sahariana más pequeña centrada en Tetuán, y Marruecos recuperó la independencia plena en 1956 bajo el sultán Mohamed V, quien asumió entonces el título de rey. Esta partición colonial es en sí misma el hecho de fondo que explica por qué España conserva hasta hoy Ceuta, Melilla y varios enclaves menores en la costa marroquí, un legado que se examina a lo largo de los capítulos siguientes; se expone aquí como trasfondo histórico establecido y no como un juicio etiquetado con WEP.

La población de Marruecos alcanzó los 36.828.330 habitantes en el censo general de 2024, con una esperanza de vida al nacer de 77,2 años y una proyección de población para 2050 de aproximadamente 43,6 millones frente a una creciente tasa de dependencia de la vejez del 69,7 % [1]. La Constitución de 2011 describe la identidad nacional como forjada por la convergencia de los componentes árabe-islamista, bereber (amazigh) y saharauí-hasaní del país, nutrida por influencias africanas, andalusíes, hebraicas y mediterráneas, y declara el islam religión del Estado a la vez que garantiza el libre ejercicio de creencias a todos [2]. El árabe y el tamazight son ambos idiomas oficiales a nivel constitucional, este último elevado de reconocido a plenamente oficial por la reforma de 2011; el francés sigue siendo el idioma de facto de los negocios, la educación superior y buena parte de la administración, y el español conserva una presencia regional residual en la antigua zona del protectorado norteño, aunque los porcentajes actuales de bilingüismo o uso lingüístico no pudieron verificarse de forma independiente en el material disponible y se registran aquí como una carencia explícita y no como una cifra asumida [2].

Marruecos es constitucionalmente una monarquía parlamentaria, democrática y social en la que la soberanía reside formalmente en la Nación, pero el rey conserva poderes reservados decisivos que quedan fuera del control parlamentario ordinario: como Amir al-Muminín (Comendador de los Creyentes) ejerce prerrogativas religiosas exclusivas mediante dahir; como jefe de Estado es árbitro supremo entre las instituciones y garante de la independencia y la integridad territorial del Reino; nombra al jefe de Gobierno del partido mayoritario en la Cámara de Representantes y nombra a los ministros a propuesta de dicho jefe de Gobierno; y preside personalmente el Consejo de Ministros, que en virtud del artículo 49 aprueba el nombramiento, nominalmente a propuesta del jefe de Gobierno, del gobernador del Bank Al-Maghrib, los embajadores, los walis y gobernadores, y la cúpula tanto de las administraciones de seguridad interna como de los organismos y empresas estratégicos públicos [2]. Es casi seguro que esta arquitectura constitucional otorga a Palacio un canal duradero y jurídicamente fundamentado de control sobre la administración territorial del Estado, la seguridad y la dirección de las empresas estatales, con independencia de qué partido gane unas elecciones parlamentarias (confianza: alta), un juicio que se deriva directamente del texto llano de los artículos 41, 47, 49, 53 y 54 y no de ninguna interpretación controvertida.

Marruecos entra en una ventana políticamente trascendente, con elecciones legislativas previstas para el 23 de septiembre de 2026 que los comentaristas académicos marroquíes actuales analizan menos como una contienda sobre qué partido gobierna que como una prueba de si el gobierno entrante puede abordar una brecha centro-periferia de larga data, dado que el lugar de nacimiento

y el lugar de residencia siguen influyendo fuertemente en las trayectorias individuales en educación, sanidad, empleo y acceso a servicios en las regiones de Marruecos [3]. Ese análisis recomienda una financiación territorial diferenciada, contratos de rendimiento Estado-Región medibles, infraestructura digital rural prioritaria y un giro de una política lingüística del tamazight meramente simbólica a una implementada institucionalmente en las escuelas y la administración [3]. En las propias papeletas, el Partido de la Justicia y el Desarrollo (PJD) —reducido de 125 a 12 escaños en su colapso de 2021— ha vuelto a la contienda con una plataforma económico-populista que propone un tramo máximo del impuesto de sociedades para las empresas dominantes de combustibles, telecomunicaciones y cemento, y una revisión del sistema de subsidios de Marruecos alegando que los hogares más pobres reciben escaso beneficio directo del arreglo actual [4]. Es probable que esto refleje un giro estratégico deliberado, alejándose del encuadre religioso e identitario de los ciclos electorales anteriores del PJD hacia un populismo económico antimonopolio, en un intento de reconstruir una coalición tras 2021 (confianza: moderada), un juicio extraído del propio contenido de la plataforma y no de ninguna declaración de intención estratégica del propio partido.

El acontecimiento de seguridad interna más significativo y reciente de Marruecos, la oleada de protestas Gen Z 212, comenzó a finales de septiembre de 2025 como un movimiento juvenil sin líderes, organizado a través de Discord, que exigía una mejor sanidad y educación públicas, y que cristalizó en torno al contraste entre el gasto multimillonario en infraestructuras para el Mundial de 2030 y unos hospitales infrafinanciados [5, 6]. Las fuerzas de seguridad mataron a tres manifestantes en Leqliaa, cerca de Agadir, un episodio que el Ministerio del Interior atribuyó a un intento de apropiarse de armas policiales, una versión que, según señalan dos medios independientes, ningún testigo corroboró; más de 1.000 personas fueron presuntamente detenidas, alrededor del 70 % de los manifestantes eran menores según la propia estimación del Ministerio del Interior, y las protestas se extendieron por 23 de las provincias de Marruecos antes de que el primer ministro Aziz Akhannouch ofreciera su única respuesta pública, una oferta de diálogo sin especificar reformas concretas, mientras algunas multitudes pedían su dimisión y otras coreaban para que el propio rey Mohamed VI interviniera contra el Gobierno [5, 6]. Es muy probable que Gen Z 212 represente el desafío extrainstitucional sin liderazgo más significativo a la autoridad del Gobierno marroquí de la década actual (confianza: alta), dada la magnitud y el número de víctimas, corroborados de forma independiente por dos medios distintos y con múltiples fuentes.

Política y geopolítica

El alineamiento externo más trascendente de Marruecos en el periodo actual es con Estados Unidos, anclado en el reconocimiento por Washington en diciembre de 2020 de la soberanía marroquí sobre el Sáhara Occidental —el primer gobierno occidental en hacerlo— y reforzado por el patrocinio estadounidense de una resolución del Consejo de Seguridad de la ONU en octubre de 2025 que respalda la propuesta de autonomía de Marruecos para el territorio [7]. Ese alineamiento tiene una expresión comercial y simbólica visible: una adjudicación de Ventas Militares Extranjeras de EE. UU. de septiembre de 2026, de hasta 42,1 millones de dólares, a CAE Inc. para simuladores de entrenamiento F-16 Block 72 en la base aérea de Sidi Slimane, sigue a la aprobación por el Departamento de Estado en 2019 de una posible venta de 3.790 millones de dólares de 25 nuevas aeronaves F-16C/D más una modernización de 985 millones de dólares de la flota existente de Marruecos [8], mientras que una afirmación viral y no verificada según la cual Marruecos habría bautizado una nueva autopista del Sáhara Occidental con el nombre del presidente Trump —nunca confirmada ni desmentida por Rabat— ilustra, sea o no literalmente cierta, hasta qué punto se percibe que la diplomacia marroquí sigue de cerca el reconocimiento

estadounidense de su reivindicación territorial nuclear [7]. Es muy probable que Marruecos siga tratando la relación con EE. UU. como su validación externa más valiosa de la posición sobre el Sáhara Occidental durante el resto de esta década (confianza: alta).

Francia sigue siendo la asociación europea más profunda e institucionalmente densa de Marruecos, ilustrada de forma concreta por la decimoquinta Reunión de Alto Nivel Marruecos-Francia celebrada en Rabat en julio de 2026, en la que ambos gobiernos firmaron más de una docena de acuerdos de cooperación que abarcan simultáneamente la financiación de la línea de alta velocidad entre Kenitra y Marrakech, la asociación en el sector hídrico, la cooperación en política exterior feminista, la aviación civil, los servicios postales, el intercambio cultural y la investigación científica conjunta [9]. Es muy probable que esta amplitud de acuerdo institucional simultáneo refleje una relación bilateral deliberadamente profundizada y multisectorial, y no un gesto diplomático aislado (confianza: alta), dado el número y la diversidad funcional de los instrumentos firmados en una sola reunión. Esta profundidad institucional resulta notable por coexistir con, en lugar de verse visiblemente alterada por, la presunta operación de la DGED en 2021 dirigida contra siete ministros del gobierno francés mediante Pegasus, examinada más adelante en gesto (confianza: alta), dado el número y la diversidad funcional de los instrumentos firmados en una sola reunión. Esta profundidad institucional resulta notable por coexistir con, en lugar de verse visiblemente alterada por, la presunta operación de la DGED en 2021 dirigida contra siete ministros del gobierno francés mediante Pegasus, examinada más adelante en *DGED* a continuación [10]; la investigación de este informe no localizó ningún indicador de fricción específico con Francia —una disputa de visados o una protesta a nivel ministerial, por ejemplo— en la recopilación actual que contrapesar a la evidencia de cooperación de julio de 2026, por lo que trata la relación con Francia como en profundización activa a nivel técnico y ministerial en el periodo actual y no como tensa en la actualidad, revisando así una presunción de tensión que encuadres anteriores de esta relación podrían haber arrastrado sin examinarla.

La relación de España con Marruecos es, en cambio, el vínculo europeo de peso más volátil de Marruecos, alternando entre normalización y crisis aguda en un ciclo aproximadamente anual: la declaración del presidente del Gobierno Pedro Sánchez en 2022 de que el plan de autonomía de Marruecos era la solución más seria, creíble y realista para el Sáhara Occidental puso fin a una ruptura desencadenada por la admisión por España en 2021 del líder del Polisario Brahim Ghali para recibir tratamiento médico; sin embargo, el 30-31 de julio de 2026 un episodio de cruce fronterizo masivo hacia Ceuta —la prensa española citó más de 49.000 entradas en 24 horas, mientras que la prensa marroquí, al recoger cifras oficiales españolas, citó más de 70.000, dos recuentos no conciliados para lo que las fuentes de este informe tratan como la misma ventana temporal y no como dos episodios distintos, ambos diferentes de la anterior oleada de aproximadamente 10.000 personas de 2021— reabrió la tensión pocos días después de que Sánchez viajara a Argel para reparar los lazos con el principal rival regional de Rabat [11, 12]. Organizaciones humanitarias informaron posteriormente de aproximadamente 141 muertes durante los intentos de cruce de julio-agosto, un balance que ningún gobierno ha confirmado [13]. Existe una posibilidad prácticamente equivalente de que Marruecos calibre deliberadamente el volumen de cruces migratorios irregulares hacia Ceuta y Melilla como un instrumento de presión diplomática sincronizado con la evolución política española, frente a que las oleadas reflejen dinámicas migratorias genuinamente fuera del control de Rabat (confianza: baja), dado que el propio Sánchez declaró al Congreso que España carece actualmente de pruebas sólidas que vinculen directamente al Gobierno marroquí con la organización del flujo, incluso cuando esa misma información trata explícitamente la cuestión de la pasividad marroquí en el control fronterizo como deliberadamente no aclarada por las explicaciones oficiales [11, 12].

La propia ponderación que hace este informe de esa cuestión no resuelta contrapone tres explicaciones rivales en lugar de adoptar la primera plausible. Una hipótesis de facilitación desde

arriba —Palacio o la cúpula de la DGST relajando deliberadamente los controles fronterizos como señalización coercitiva sincronizada con la visita de Sánchez a Argel del 20 de julio de 2026— recibe cierto respaldo de esa coincidencia temporal y de una caracterización de la policía nacional española, trasladada a la jueza de la Audiencia Nacional María Tardón, del cruce como un proceso predefinido con objetivos distintos de los migratorios que requiere una alta capacidad de influencia en redes y personas vinculadas a las fuerzas de seguridad de Marruecos, pero las únicas afirmaciones que señalan a un artífice concreto proceden del actor hacktivista Jabaroot, cuyo propio objetivo declarado de maximizar el coste político de la crisis para Rabat es precisamente el tipo de incentivo de la fuente para engañar que este informe descuenta en lugar de aceptar al pie de la letra [14, 15]. Una hipótesis de pérdida de control pura, coherente con el propio encuadre de mafias de tráfico de personas de Madrid y con la declaración de Sánchez al Congreso, choca con la enorme dificultad logística de orquestar encubiertamente una oleada de esta magnitud y con la posterior movilización interinstitucional del propio Marruecos —DGSN, Gendarmería Real y Fuerzas Auxiliares desplegadas conjuntamente— para bloquear un intento de cruce menor el 15 de agosto cerca de Castillejos, una conducta difícil de conciliar con una política de facilitación deliberada en curso. Una tercera hipótesis intermedia —una tolerancia localizada o de nivel medio por parte de elementos de seguridad, sin llegar a ninguna orden documentada desde arriba, coherente con que la arquitectura de seguridad de Marruecos sea un conjunto de instituciones con cometidos separados (la DGST, la DGED, las Fuerzas Auxiliares y la Gendarmería Real estuvieron todas activas por separado en ese periodo) y no un mando único coordinado sin fricciones— acomoda mejor la evidencia sin requerir ni una conspiración unificada ni un accidente puro. Existe una posibilidad prácticamente equivalente de que se produjera alguna forma de tolerancia o facilitación del aparato de seguridad en algún nivel, con la hipótesis de tolerancia de nivel medio favorecida específicamente frente a la orquestación desde arriba (confianza: baja), un juicio al que este informe llega con su propio registro evidencial pero que converge con la misma estructura y conclusión de tres hipótesis obtenida de forma independiente por las pasadas de investigación diplomática y geopolítica de esta edición; debería revisarse si surgiera un cambio documentado en las órdenes permanentes de los guardias fronterizos, un vínculo forense entre las comunicaciones de la DGST/DGED y el momento del cruce, o una resolución judicial que señalara a un organismo marroquí concreto.

Argelia es el principal adversario regional de Marruecos, una ruptura que se remonta a agosto de 2021 y que desde entonces se sostiene mediante una auténtica carrera de armamentos bilateral: los dos países concentraron conjuntamente el 88 % del gasto militar medible del norte de África en 2025, unos 33.000 millones de dólares combinados, con los 25.500 millones de Argelia superando con creces los 7.510 millones de Marruecos, aunque se proyecta que el presupuesto argelino de 2026 caiga en torno a un 10 % en términos reales mientras que el de Marruecos sube hasta un récord de 7.870 millones de dólares, una divergencia que el IISS atribuye a que las finanzas públicas de Argelia dependen de los hidrocarburos frente a una economía marroquí más diversificada [16]. La misma fuente describe a Argelia apoyándose en equipamiento ruso y, cada vez más, chino, con cazas de quinta generación Su-57 reportados, frente a la preferencia de Marruecos por sistemas estadounidenses y occidentales junto con una cooperación creciente con Israel y su propia industria de defensa nacional —un raro indicio, respaldado directamente por una fuente, de una dimensión industrial de defensa Marruecos-Israel, aunque ninguna fuente localizada en esta recopilación desarrolla su contenido específico—. Es probable que los impulsos paralelos de modernización de ambos Estados sigan reforzando, en lugar de aliviar, lo que el propio IISS denomina un dilema de seguridad de cara al horizonte 2026-2027 (confianza: moderada), un juicio que el propio análisis de la fuente respalda directamente.

La importancia estratégica del Estrecho de Gibraltar para la política exterior de Marruecos se entiende mejor como el punto de convergencia de tres presiones distintas que como un único

expediente de punto de estrangulamiento bien documentado por derecho propio. Es el corredor migratorio cuyas oleadas han reabierto y cerrado repetidamente la relación entre España y Marruecos, analizada más arriba [11, 12]; es la terminal hacia la que el futuro gasoducto Nigeria-Marruecos —aprobado por la CEDEAO en julio de 2026 como un proyecto de 25.000 millones de dólares y unos 6.000 kilómetros, destinado eventualmente a conectar con el ya existente Gasoducto Magreb-Europa hasta España— entregaría un estimado de 15 de los 30.000 millones de metros cúbicos anuales de gas con destino a Europa [17]; y es, según un medio con sede en España que cita a un grupo no verificado de análisis de defensa, la línea nocalional a través de la cual se estima ahora que los sistemas de misiles y drones marroquíes podrían alcanzar la Andalucía peninsular, lo que motivó la afirmación pública de un general español en activo de que España conserva la capacidad de «apagar Marruecos en 24 horas» [18]. Esta recopilación no localizó ninguna fuente primaria o técnica dedicada —una estadística de tráfico de una autoridad portuaria o una valoración de la OTAN o del Instituto Español de Estudios Estratégicos, por ejemplo— que abordara directamente el papel del Estrecho como punto de estrangulamiento marítimo, una carencia que se señala aquí explícitamente en lugar de disimularse con una cifra sin respaldo; la tabla siguiente presenta las tres presiones una junto a otra.

Tabla 1. El Estrecho de Gibraltar: tres presiones estratégicas convergentes sobre la política de Marruecos hacia España.

Presión	Mecanismo	Evidencia clave
Corredor migratorio	Los cruces irregulares hacia Ceuta/Melilla reabren y cierran repetidamente la relación bilateral	Oleada de la crisis Ghali de 2021 (~10.000); cruce masivo de julio de 2026 (más de 70.000 según lo reportado; una cifra independiente de más de 49.000 en 24 horas)
Terminal energética/de infraestructuras	Gasoducto Nigeria-Marruecos encaminado hacia el Gasoducto Magreb-Europa hasta España	25.000 millones USD, ~6.000 km, aprobado por la CEDEAO (jul. 2026); ~15 de 30 bcm/año estimados con destino a Europa; construcción desde 2028, entregas desde 2031
Percepción de capacidad militar	Alcance estimado de misiles/drones hacia la Andalucía peninsular	Valoración no verificada de un grupo de análisis de defensa; declaración pública de un general español en activo afirmando que España podría «apagar Marruecos en 24 horas»

El Majzén

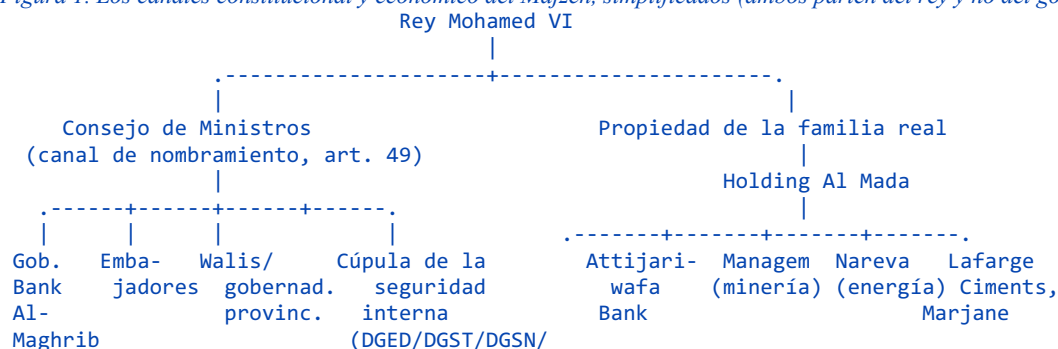
Majzén funciona en el material de fuentes abiertas actual como un término genuinamente controvertido y no como una categoría analítica asentada. Un comentarista marroquí alineado con el establishment, que escribe en la prensa marroquí de habla inglesa generalista, lo define de forma benigna como la red de autoridad tradicional centrada en la monarquía —jefes tribales, dignatarios, eruditos religiosos y notables locales—, atribuyéndole haber demostrado una gran capacidad de adaptación y haber garantizado la continuidad institucional de Marruecos a través del colonialismo, la independencia, la modernización y la actual agitación regional [19]. La agencia

estatal de noticias oficial de Argelia emplea el mismo término como instrumento de deslegitimación, describiendo a Marruecos como afianzando su posición de refugio seguro para delincuentes que huyen de la justicia europea y situando al Majzén en el centro del fomento de un entorno que permite que la delincuencia organizada transnacional se regenere, una afirmación no verificada y de fuente única formulada por un actor estatal en ruptura diplomática activa con Rabat y sin corroboración independiente localizada en ninguna parte de esta recopilación [20]. Es muy probable que ninguno de los dos marcos deba interpretarse como una definición neutral del término (confianza: alta), y no se localizó en el material revisado ninguna definición académica u organización de análisis occidental independiente, una carencia que se declara explícitamente en lugar de disimularse.

El mecanismo institucional concreto mediante el cual se ejerce la autoridad informal de Palacio sobre el Estado formal está, pese a esa laguna definitoria, directamente documentado en el propio texto constitucional y no queda librado a una caracterización controvertida. El artículo 49 encauza el nombramiento del gobernador del Bank Al-Maghrib, de todos los embajadores, de la totalidad del cuerpo de walis y gobernadores provinciales, y de la cúpula tanto de las administraciones de seguridad interna como de los organismos y empresas estratégicos públicos, a través del Consejo de Ministros presidido por el rey, nominalmente a propuesta del jefe de Gobierno, pero decidido en un órgano que el propio rey preside; el artículo 53 convierte al rey en jefe supremo de las Fuerzas Armadas Reales con potestad para nombrar cargos militares, y el artículo 54 establece un Consejo Superior de Seguridad presidido por el rey que coordina la estrategia de seguridad tanto interna como externa [2]. Es casi seguro que estos tres artículos, leídos en conjunto, proporcionan el chasis legal a través del cual la red informal de asesores, notables y responsables de seguridad que en la práctica constituye el Majzén llega simultáneamente a la administración territorial, los servicios de seguridad y la dirección de las empresas estatales (confianza: alta), dado que se trata de una lectura directa del texto constitucional y no de una inferencia que requiera evidencia adicional.

En la dimensión económica de la red, Al Mada —el mayor conglomerado holding privado de Marruecos, renombrado en 2018 a partir de la Société Nationale d'Investissement fundada en 1966— pertenece principalmente a la familia real y mantiene participaciones significativas simultáneamente en Attijariwafa Bank, Managem, Nareva, Lafarge Ciments y Marjane, con una actividad inversora en expansión en Camerún, Costa de Marfil, Ruanda y Gabón [21]. Es muy probable que esta estructura de conglomerado único otorgue a la monarquía una participación comercial directa, y no meramente regulatoria o de nombramiento, en los resultados de la banca, la industria extractiva, la energía, la construcción y el comercio minorista simultáneamente (confianza: alta), un juicio extraído directamente de la amplitud sectorial que confirma esta fuente; una participación accionarial real o de la red del Majzén comparable en los sectores marroquíes de telecomunicaciones o medios de comunicación no se verificó de forma independiente en este material y se registra aquí como una carencia explícita y no se afirma sobre la base de un conocimiento de fondo.

Figura 1. Los canales constitucional y económico del Majzén, simplificados (ambos parten del rey y no del gobierno electo).



FAR -- ver próximos
dos capítulos)

Si esta fusión de autoridad de nombramiento, seguridad y economía bajo una sola red informal funciona principalmente para distribuir los recursos del Estado con eficiencia o principalmente para aislar la toma de decisiones de una supervisión legislativa o judicial significativa no puede resolverse con la evidencia revisada, y las dos lecturas se presentan aquí como una tensión viva y no como algo dirimido. La demanda central de las protestas Gen Z 212 —redirigir el gasto público de las infraestructuras del Mundial hacia hospitales y escuelas, analizada más arriba en *Introducción* — es en sí misma evidencia de que una parte sustancial del público marroquí percibe que la asignación actual de recursos está mal alineada con la prioridad popular, una percepción que se hace eco en la propia justificación declarada por el PJD para su propuesta de reforma de subsidios de 2026, según la cual los hogares más pobres reciben escaso beneficio directo del sistema actual [4, 5]. Es probable que la concentración constitucional de autoridad de nombramiento documentada más arriba reduzca la rendición de cuentas práctica de walis, gobernadores, la cúpula de los servicios de seguridad y los responsables de las empresas estatales ante las instituciones electas, en comparación con un sistema en el que tales nombramientos requirieran confirmación parlamentaria (confianza: moderada), un juicio que se deriva de la simple asignación constitucional de esa potestad de nombramiento y no de una fuente que afirme directamente un fallo de supervisión; no se localizó ninguna fuente dedicada a auditoría o supervisión específica, y esta carencia se declara en consecuencia.

Prioridades estratégicas

Las prioridades estratégicas de Marruecos se interpretan mejor como una jerarquía ordenada en la que la seguridad interna del régimen prevalece sobre cualquier expediente exterior, ya que ningún resultado de política exterior merece perseguirse al precio de una estabilidad interna que la propia monarquía no sobreviva para disfrutar. La tabla siguiente presenta los seis teatros por orden de prioridad, junto con su base evidencial principal y la confianza estimada, antes de desarrollar cada uno de ellos por separado.

Tabla 2. Los seis teatros de prioridad estratégica de Marruecos, ordenados, con su base evidencial principal y la confianza estimada.

Posición	Teatro	Base evidencial principal	Confianza estimada
1	Seguridad interna del régimen	Oleada de protestas Gen Z 212 (sep-oct 2025); elecciones de sept. 2026; reentrada populista del PJD	Moderada
2	Sáhara Occidental	Reconocimiento de EE. UU. de dic. 2020; resolución del CSNU de oct. 2025; Resolución 2797 del Consejo de Seguridad de la ONU (2026)	Moderada
3	Rivalidad con Argelia	88 % del gasto militar del norte de África en 2025; análisis del IISS sobre la carrera armamentística	Moderada

4	Estrategia saheliana y atlántica	Gasoducto Nigeria-Marruecos (aprobación de la CEDEAO en 2026); autopista Tiznit-Dakhla; Iniciativa Atlántica	Moderada
5	España, Francia y la UE	15. ^a Reunión de Alto Nivel Marruecos-Francia (jul. 2026); retórica y cruces en Ceuta/Melilla	Moderada
6	EE. UU., Israel y los Estados del Golfo	Adjudicación FMS de simuladores de entrenamiento F-16 en sept. 2026; única referencia no desarrollada a la cooperación con Israel	Baja

La oleada de protestas Gen Z 212 y las elecciones de septiembre de 2026 son los dos indicadores en vivo del nivel de tensión actual de la seguridad interna del régimen: la reentrada populista del PJD, la propia preocupación de Palacio por el análisis de política sobre la desigualdad territorial, y un movimiento de protesta cuya demanda central —gasto en sanidad y educación por encima de los proyectos de prestigio del Mundial— desafía directamente las prioridades de gasto declaradas por el Gobierno, indican en conjunto que la gestión de la legitimidad interna, y no ninguna rivalidad externa, sigue siendo la preocupación de primer orden de la gobernanza marroquí en el periodo actual [3, 4, 5]. Es probable que las elecciones de septiembre de 2026 sean interpretadas por Palacio principalmente como un referéndum sobre esta cuestión de legitimidad interna y no como una transferencia genuina de autoridad política a la coalición que gobierne (confianza: moderada), coherente con la concentración constitucional de la potestad de nombramiento en Palacio documentada más arriba en *El Majzén*, con independencia del resultado electoral.

El Sáhara Occidental ocupa el segundo lugar, como el único asunto en el que Marruecos ha obtenido su validación externa más significativa y reciente y en el que sigue invirtiendo un capital diplomático desproporcionado. La secuencia central —el reconocimiento estadounidense de la soberanía marroquí en diciembre de 2020, una resolución del Consejo de Seguridad de la ONU patrocinada por EE. UU. que favorece la propuesta de autonomía de Marruecos en octubre de 2025, y la adopción de una nueva Resolución 2797 del Consejo de Seguridad de la ONU, referenciada de forma independiente tanto por un centro de análisis marroquí como por el ministro de Asuntos Exteriores de Grecia hacia septiembre de 2026— indica un impulso diplomático acumulativo, y no estático, detrás de la posición de Rabat [7, 22, 23]. Esta recopilación no obtuvo de forma independiente el propio texto de la Resolución 2797, una carencia señalada de forma consistente en tres fuentes distintas, y la valoración posterior no debe caracterizar el contenido de la resolución más allá de adoptada y referenciada como respaldo a una negociación mediada por la ONU sobre la base de la propuesta de autonomía de Marruecos, a la espera de una verificación directa [22, 23].

Una afirmación distinta, procedente de la prensa marroquí, sostiene que la propia retórica de Argelia sobre la disputa se está suavizando bajo la presión diplomática estadounidense, pero esta afirmación fue formulada íntegramente por analistas identificados y una figura de incidencia favorable a la posición marroquí, sin que se localizara corroboración argelina, oficial o de otro tipo

[24]. Es improbable que esto represente un cambio genuino y confirmado en la posición de Argel, frente a una narrativa interpretativa alineada con Rabat (confianza: baja), dada la ausencia total de corroboración independiente.

Argelia ocupa el tercer lugar como la rivalidad regional más activa y materialmente trascendente de Marruecos, distinta del expediente del Sáhara Occidental aunque ambos estén estrechamente vinculados; el propio uso por los medios estatales argelinos del término Majzén como término crítico, analizado más arriba en El Majzén, es en sí mismo un dato sobre la temperatura actual de esta rivalidad, dado que ataques retóricos de Estado a Estado de este tipo no son habituales entre Estados con relaciones normalizadas [20]. Superpuesta a esa hostilidad retórica está la dinámica de carrera armamentística detallada más arriba en *Política y geopolítica*, a la que esta sección se remite en lugar de repetir las cifras subyacentes; es probable que esta rivalidad siga condicionando las adquisiciones de defensa y el alineamiento diplomático marroquíes —hacia EE. UU., Israel y su propia industria de defensa nacional, alejándose de cualquier bloque alineado con Argelia— como un rasgo estructural casi permanente de la planificación estratégica marroquí durante el resto de esta década (confianza: moderada), un juicio coherente con la trayectoria que describen los propios datos del IISS [16].

La estrategia saheliana y atlántica ocupa el cuarto lugar, anclada en el gasoducto Nigeria-Marruecos, aprobado por la CEDEAO y de 25.000 millones de dólares —un proyecto de unos 6.000 kilómetros que atraviesa trece países además del Sáhara Occidental, destinado a transportar gas nigeriano hasta Marruecos y de ahí a Europa a través del ya existente Gasoducto Magreb-Europa, con la construcción prevista para comenzar en 2028 y las primeras entregas en 2031 [17]. Este proyecto se suma a la ya finalizada autopista Tiznit-Dakhla de Marruecos, plenamente operativa desde enero de 2026, con unos 1.055 kilómetros y 1.000 millones de dólares de coste, que enlaza el sur de Marruecos con la península de Dajla, donde Marruecos está desarrollando un gran puerto atlántico explícitamente vinculado a su Iniciativa Atlántica para conectar a los Estados sahelianos sin salida al mar con el comercio atlántico a través del territorio marroquí [7]. Es probable que Marruecos pretenda que este despliegue de infraestructuras orientado al Atlántico lo posicione como un corredor de exportación alternativo hacia Europa que evite estructuralmente a Argelia, cuyo propio proyecto rival de gasoducto transahariano es un competidor directo para la misma función (confianza: moderada), un juicio coherente con, aunque no demostrado de forma concluyente por, la propia geografía del gasoducto y su calendario en relación con la ruptura con Argelia [17].

España, Francia y la Unión Europea en su conjunto ocupan el quinto lugar, y la evidencia muestra un enfoque que varía significativamente según el socio y no una estrategia europea única y uniforme: Francia recibe el compromiso institucional más profundo, ya detallado más arriba en *Política y geopolítica*, mientras que España recibe una mezcla más volátil de normalización y ciclos de crisis en los expedientes de migración y de Ceuta/Melilla, ilustrada de forma patente por la referencia pública del ministro de Justicia Abdellatif Ouahbi a las dos ciudades como nuestras tierras y por la referencia del ministro de Asuntos Religiosos Ahmed Toufiq a su liberación, formulada en un acto al que asistió el rey Mohamed VI, lo que en conjunto provocó un rechazo categórico español, por parte del ministro de Asuntos Exteriores José Manuel Albares, a cualquier discusión sobre la integridad territorial de España [12]. La tabla siguiente presenta uno junto a otro los sucesivos episodios de cruce migratorio en Ceuta y Melilla, dado que la información española y marroquí ha citado repetidamente cifras solapadas pero distintas para lo que, leído con atención, son episodios separados.

Tabla 3. Episodios de cruce migratorio en Ceuta y Melilla, 2021-2026: eventos distintos, cifras solapadas.

Fecha	Magnitud reportada	Contexto
Abr-may 2021	~10.000 cruces	Desencadenado por la admisión de España del líder del Polisario

		Brahim Ghali para tratamiento médico
7 abr. 2022	n/d	Declaración de Sánchez respaldando el plan de autonomía de Marruecos; fin formal de la ruptura de 2021
30-31 jul. 2026	Más de 70.000 según lo reportado; una cifra independiente de más de 49.000 en 24 horas	Cruce masivo hacia Ceuta pocos días después de la visita de Sánchez a Argel, rival regional de Rabat

Los Estados más pequeños de la UE, por su parte, se están alineando gradualmente con la posición de EE. UU. e Israel sobre el Sáhara Occidental: el ministro de Asuntos Exteriores de Grecia acogió públicamente la propuesta de autonomía de Marruecos y la Resolución 2797 del Consejo de Seguridad de la ONU en septiembre de 2026 [23], mientras que el ministro de Asuntos Exteriores de Dinamarca, el mismo mes, calificó a Marruecos de nuestro aliado en el flanco sur e indicó que Dinamarca podría ajustar su posición para acercarse a la de Estados Unidos sobre el Sáhara Occidental de cara a un acuerdo de asociación estratégica previsto para diciembre de 2026 [25]. Es probable que este patrón de alineamiento gradual de los Estados más pequeños de la UE siga aislando la posición interna española, más controvertida y políticamente limitada, sobre el Sáhara Occidental de la tendencia europea más amplia (confianza: moderada), un juicio extraído del número creciente de Estados de la UE que ahora respaldan audiblemente el marco de autonomía frente a la postura pública más cautelosa de Madrid.

Estados Unidos, Israel y los Estados del Golfo ocupan el sexto lugar como grupo, no porque las relaciones carezcan de importancia, sino porque la evidencia disponible sobre ellas es comparativamente escasa frente a los otros cinco teatros y se concentra casi enteramente en el expediente del Sáhara Occidental ya analizado más arriba. La evidencia concreta más clara es la adjudicación de Ventas Militares Extranjeras de EE. UU. de septiembre de 2026 para infraestructura de entrenamiento de F-16, que sigue al marco de venta de F-16 de 3.790 millones de dólares aprobado en 2019 [8], junto con la única referencia no desarrollada al desarrollo de la cooperación de Marruecos con Israel hallada en la información comparativa de defensa procedente del IISS [16]; no se localizó ninguna fuente dedicada sobre inversión, propiedad o relaciones de seguridad de los Estados del Golfo con Marruecos en el material revisado para esta sección, una carencia que se señala aquí explícitamente en lugar de rellenarse con referencias a material desarrollado en otras partes de este informe. Existe una posibilidad prácticamente equivalente, sobre esta base evidencial comparativamente escasa, de que las relaciones con EE. UU., Israel o el Golfo experimenten un desarrollo materialmente nuevo a corto plazo, frente a la continuación del patrón estable actual (confianza: baja), un juicio ofrecido con baja confianza precisamente porque este teatro es el menos densamente evidenciado de los seis.

Parte III. La arquitectura de seguridad e inteligencia

La comunidad de inteligencia

La arquitectura marroquí de inteligencia civil y policía se remonta a un único dahir real del 12 de enero de 1973, dictado tras los fallidos golpes militares de 1971 y 1972 contra el rey Hassan II, que disolvió la anterior estructura de policía política CAB-1 y creó dos servicios sucesores el mismo día: la DGED para la inteligencia exterior y la DGST para la seguridad interna y el contraespionaje [26, 27]. Ese origen compartido ayuda a explicar por qué los mandatos de ambos servicios todavía se solapan en la práctica, particularmente en la recopilación técnica orientada al exterior, aunque la DGED está administrativamente adscrita a la Administration de la Défense Nationale mientras que la DGST responde ante el Ministerio del Interior [26, 27]. La DGSN, la fuerza de policía civil nacional de Marruecos, tiene un linaje distinto y más antiguo, habiéndose establecido el 16 de mayo de 1956 en virtud del Dahir n.º 1-56-115 para sustituir a la Police Chérifienne de la era colonial, y su relevancia para este capítulo descansa en una única dirección constituyente y no en la fuerza en su conjunto, examinada en detalle más abajo [28].

Desde el 15 de mayo de 2015, un único responsable, Abdellatif Hammouchi, dirige simultáneamente la DGST y la DGSN, una doble función que el registro de fuentes abiertas describe de forma consistente como sin precedentes en el aparato de seguridad marroquí posterior a 1999 y que fusiona, sin equivalente europeo directo, la autoridad de contraespionaje interno y la de policía nacional [27, 29]. Es casi seguro que esta concentración de autoridad en un único responsable otorga a Hammouchi un grado de control institucional sobre la arquitectura de seguridad interna de Marruecos al que no se aproxima ningún arreglo comparable entre los principales socios europeos de Marruecos (confianza: alta), dado que ninguna fuente revisada identifica una fusión equivalente de un servicio de contraespionaje y una fuerza de policía nacional en un único responsable en ninguna otra parte de la región que examina este informe. La tabla siguiente ofrece una instantánea comparativa de los tres organismos antes de sus perfiles individuales, y la figura que sigue presenta sus líneas de dependencia jerárquica de forma simplificada.

Tabla 4. Los organismos marroquíes de inteligencia civil y policía de un vistazo.

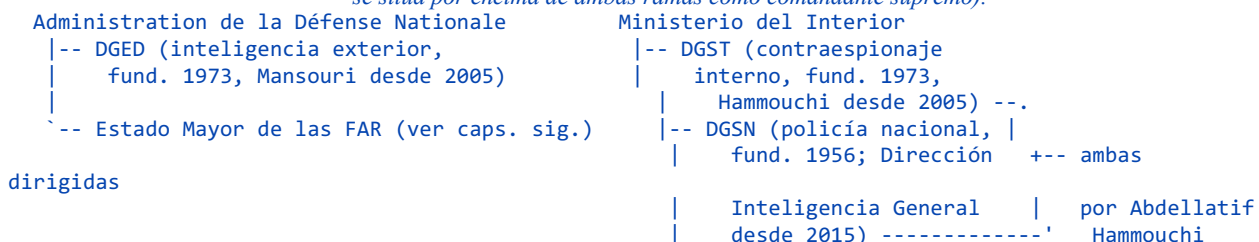
Organismo	Fundación	Depende de	Director (desde)	Mandato principal
DGED	1973 (dahir, 12 ene.)	Administration de la Défense Nationale	Mohammed Yassine Mansouri (2005)	Inteligencia exterior, contraespionaje, diplomacia de seguridad en el Sahel
DGST	1973 (dahir, 12 ene.)	Ministerio del Interior	Abdellatif Hammouchi (2005)	Contraespionaje interno, contrterrorismo, inteligencia de señales (PCR), policía judicial (BCIJ)
DGSN	1956 (dahir, 16 may.)	Ministerio del Interior	Abdellatif Hammouchi (2015)	Policía civil nacional: orden público, policía

judicial,
Inteligencia
General

Tabla 5. Sucesión en la dirección de la DGED, la DGST y la DGSN.

Organismo	Director	Mandato	Cargo previo destacado
DGED	Ahmed Dlimi	1973-1983	Antiguo jefe de CAB-1
DGED	Abdelhak El Kadiri	1983-2001	—
DGED	Ahmed El Harchi	2001-2005	—
DGED	Mohammed Yassine Mansouri	2005-presente	Antiguo director de Maghreb Arabe Presse; primer director civil
DGST	Ahmed Dlimi	1973-1983	Simultáneamente, primer director de la DGED
DGST	Driss Basri	1983-1999	Simultáneamente, ministro del Interior
DGST	Hamidou Laanigri	1999-2003	—
DGST	Ahmed Harari	2003-2005	—
DGST	Abdellatif Hammouchi	2005-presente	Se incorporó a la DGST en 1993; también director de la DGSN desde 2015
DGSN	Abdellatif Hammouchi	2015-presente (doble función con la DGST)	Simultáneamente, director de la DGST desde 2005

Figura 2. Líneas de dependencia jerárquica simplificadas de la arquitectura marroquí de inteligencia civil y policía (el rey Mohamed VI se sitúa por encima de ambas ramas como comandante supremo).



Los tres perfiles que siguen —DGED, DGST y el fragmento de la DGSN relevante para la inteligencia— dan cuenta de esencialmente todo el registro de fuentes abiertas sobre la actividad de inteligencia civil marroquí, y dos de los tres tienen historiales operativos documentados en Europa que afectan directamente a España. Cada perfil aborda el mismo punto débil evidencial desde un ángulo distinto: la división precisa del trabajo entre la DGED y la DGST en el uso por Marruecos de software espía comercial, una cuestión de atribución que este informe resuelve solo con confianza baja a moderada y aborda de forma consistente en los tres perfiles en lugar de zanjarla una vez y darla por cerrada.

DGED

La Direction Générale des Études et de la Documentation (DGED), el servicio marroquí de inteligencia exterior y contraespionaje, fue creada por el Dahir Real 1-73-8 el 12 de enero de 1973 como parte de la misma reestructuración postgolpe que produjo la DGST, y tiene su sede en Rabat,

adsrita administrativamente a la Administration de la Défense Nationale y no al Ministerio del Interior —un arreglo que la mantiene, al menos sobre el papel, fuera de la cadena ministerial de seguridad interna que rige la DGST y la DGSN examinadas más abajo [26]. Su mandato declarado abarca la recopilación de inteligencia exterior, el contraespionaje y la protección de la seguridad de las instituciones nacionales, y esta adscripción fundacional a la administración de defensa y no a Interior la sitúa, estructuralmente, en la misma cadena que en última instancia responde ante el rey como comandante supremo y no ante ningún ministro responsable ante el parlamento [26].

La dirección ha pasado por cuatro directores: Ahmed Dlimi (1973-1983), que anteriormente había dirigido CAB-1; Abdelhak El Kadiri (1983-2001); Ahmed El Harchi (2001-2005); y Mohammed Yassine Mansouri, en el cargo desde el 14 de febrero de 2005 [26]. Mansouri es el primer civil en ocupar el cargo, antiguo compañero de clase del rey Mohamed VI en el Colegio Real que anteriormente dirigió la agencia estatal de noticias Maghreb Arabe Presse, y los perfiles de fuentes abiertas lo describen de forma consistente como un discreto confidente real [26]. Es probable que el nombramiento de Mansouri reflejara una preferencia deliberada de Palacio por un director de confianza y no militar, frente a la tradición anterior del servicio de liderazgo militar (confianza: moderada), dado que no se había producido ningún nombramiento civil comparable en las tres primeras décadas del servicio y ninguna fuente localizada ofrece una explicación alternativa para el cambio.

Es muy probable que el mando y control sobre la DGED discorra directamente hacia Palacio con una intermediación solo nominal a través de la administración de defensa (confianza: moderada), un juicio que descansa en el perfil de confidente personal de Mansouri, el patrón de nombramiento real directo a la dirección, y la ausencia, en cualquier fuente revisada, de un ministro identificado que ejerza una supervisión real de las operaciones de la DGED. Las cifras de personal y presupuesto disponibles en fuentes abiertas están desfasadas y deben leerse como indicativas y no como actuales: aproximadamente 4.000 efectivos según una estimación de 2003, en torno al 60 % procedentes de las Fuerzas Armadas Reales y el resto civil, con entre 250 y 300 oficiales desplegados en el extranjero según estimaciones, y un presupuesto anual citado en 1.080 millones de MAD en 2015 [26]; ninguna fuente localizada actualiza estas cifras más allá de mediados de la década de 2010, y esto se registra como una carencia explícita y no como una suposición de continuidad.

Las disciplinas de recopilación de la DGED, según se documentan en fuentes abiertas, se centran en la inteligencia humana construida a través de relaciones de enlace exterior y no en la recopilación técnica interna, que es más consistentemente el cometido documentado de la DGST; la evidencia más clara de esta orientación es la cartera de mediación en el Sahel del servicio desde 2020, a la que se atribuye haber logrado la liberación en 2022 del rehén alemán Jörg Lange en Níger, la liberación en 2023 del ciudadano rumano Iulian Ghergut en Burkina Faso, la implicación en las negociaciones de 2024 relativas al detenido expresidente de Níger Mohamed Bazoum, la liberación en 2024 de cuatro agentes de la DGSE francesa retenidos en Burkina Faso, y la asistencia reportada en 2025 a Níger en el seguimiento de la figura de Boko Haram Bakura Doro [26]. Es probable que este papel de mediación refleje una estrategia marroquí deliberada de llenar un vacío de diplomacia de seguridad dejado por la influencia francesa menguante en el Sahel (confianza: moderada), dado que la cronología y la consistencia de estos episodios a lo largo de tres países distintos y cuatro años resultan difíciles de explicar como trabajo de enlace coincidente. El trabajo de contraterrorismo interno es un conjunto de misiones secundario y documentado con anterioridad para la DGED: se atribuye al servicio un papel en la investigación posterior a los atentados de Casablanca de mayo de 2003, que llevó a la condena de varias figuras del Partido de la Justicia y el Desarrollo y de un corresponsal de Al-Manar por presunta complicidad [26]. Este historial es en sí mismo controvertido dado el estatus de partido político de algunos de los condenados, y existe una posibilidad prácticamente equivalente (confianza: baja) de que refleje

una necesidad genuina de contraterroismo en lugar de un uso políticamente conveniente de las potestades de seguridad contra un partido islamista entonces en auge electoral, dado que ninguna fuente localizada resuelve esa cuestión en un sentido u otro.

El papel de la DGED en la recopilación cibernética y técnica es la cuestión abierta individual más trascendente abordada en este perfil, y la evidencia debe leerse en capas y no como un único hecho zanjado. La evidencia a nivel de red del estudio de 2018 de Citizen Lab identificó a un presunto operador de Pegasus, con nombre en clave interno ATLAS, geolocalizado mediante sondeo de caché DNS en redes de telecomunicaciones marroquíes desde agosto de 2017 en adelante — evidencia a nivel de infraestructura de una presencia de Pegasus con nexo marroquí, explícitamente no forense de dispositivo [30]. La confirmación forense a nivel de dispositivo llegó de forma independiente: el Security Lab de Amnistía documentó ataques de Pegasus mediante inyección de red en el teléfono del periodista Omar Radi en cuatro fechas de 2019-2020, atribuyendo la responsabilidad a las autoridades marroquíes de forma genérica sin nombrar a un organismo concreto [31], y un segundo caso, corroborado entre laboratorios, confirmó rastros de Pegasus en el teléfono de la activista saharauí Aminatou Haidar en 2018 y de nuevo en 2021, con Citizen Lab reproduciendo de forma independiente los hallazgos de 2021 a partir de registros suministrados por Amnistía [32]. Es casi seguro que los servicios estatales marroquíes han operado Pegasus contra objetivos de la sociedad civil interna desde al menos 2019 (confianza: alta), dada esta corroboración entre laboratorios a nivel de dispositivo.

Si la DGED en concreto, a diferencia de la DGST, tiene algún papel operativo en este programa Pegasus está mucho menos zanjado. La investigación del consorcio Forbidden Stories de julio de 2026, construida sobre documentos filtrados de la DGST y testimonios internos, atribuye el control operativo principal a la DGST y no a la DGED [33, 34], y un artículo distinto del consorcio sobre el objetivo de ministros franceses parece referirse a la DGSE como el organismo marroquí implicado —casi con toda certeza un error de transcripción por DGED, dado que Marruecos no tiene ningún organismo llamado DGSE y la DGSE es el propio servicio exterior de Francia, aunque esto no pudo verificarse contra el texto primario y no debe corregirse silenciosamente [10]. Un caso relacionado en Gabón, en el que Forbidden Stories atribuye a la DGST el objetivo de figuras del entorno presidencial y de la oposición gabonesas mediante unos veinte efectivos marroquíes rotando por Gabón en destinos de seis meses desde la era de Hassan II, se lee estructuralmente más como el cometido típico de enlace exterior de la DGED que como el de contraespionaje interno de la DGST, una cuestión de atribución interservicios que el propio reportaje del consorcio no resuelve [35]. Existe una posibilidad prácticamente equivalente (confianza: baja) de que la DGED tenga un papel de facilitación o de enlace exterior en la adquisición o el objetivo de Pegasus distinto del papel de operación de dispositivos de la DGST, dado que la función documentada de enlace exterior de la DGED es funcionalmente el tipo de papel que ocuparía un intermediario de adquisición orientado al exterior, aunque ninguna fuente localizada lo afirme directamente.

La huella europea de la DGED desde 2014 ha generado una serie de controversias que, en conjunto, apuntan a un conjunto de misiones de influencia exterior y interrupción de enlaces más allá de la inteligencia humana clásica: el episodio MarocLeaks de 2014, en el que se publicó correspondencia entre la DGED y consulados marroquíes y Rabat culpó a actores próximos al Polisario y a Argelia; un caso de 2017 en el que un agente de la policía fronteriza francesa fue detenido por presuntamente entregar a contactos de la DGED archivos de listas de vigilancia de seguridad de unas 200 personas; una acusación de 2021 de infiltración de la DGED en el Consejo Francés del Culto Musulmán; y un escándalo de 2022 relativo a una presunta infiltración vinculada a la DGED en el Parlamento Europeo, contemporáneo del escándalo más amplio del Qatargate [26]. Es improbable (confianza: baja) que todas ellas fueran operaciones de la DGED dirigidas de forma centralizada y no redes más difusas de actores alineados con Marruecos, dado que la fuente

subyacente para este conjunto es una única compilación terciaria que no distingue por sí misma entre ambas posibilidades.

Una carencia adicional y distinta afecta a los satélites marroquíes de reconocimiento óptico Mohammed VI-A y Mohammed VI-B, lanzados en 2017 y 2018 respectivamente por un coste combinado de aproximadamente 500-600 millones de euros y descritos en su momento por la prensa francesa como al servicio de un firme propósito militar; ninguna fuente localizada en ninguna parte de la investigación de este informe identifica qué organismo marroquí —la DGED, el Estado Mayor de las FAR u otro organismo enteramente distinto— asigna realmente las tareas a los satélites o recibe sus imágenes [36, 37]. Dada la propia orientación de la DGED hacia el enlace exterior y la inteligencia humana, este informe ni asume que la DGED tenga un papel de asignación de tareas simplemente porque la capacidad sea relevante para la inteligencia, ni lo descarta; registra la ausencia de cualquier vínculo documentado entre la DGED y el programa de satélites como una carencia explícita que amplía, en lugar de reducir, la incertidumbre ya asociada al perfil de recopilación técnica de la DGED.

El desarrollo nuevo más significativo relativo a la DGED es la aparición, en información de prensa española de septiembre de 2026, de Mehdi Hijaouy como persona de interés identificada: descrito como antiguo subdirector de la DGED y jefe de una unidad de operaciones encubiertas que la información denomina Service Action, se informa de que Hijaouy huyó de Marruecos hace aproximadamente dos años, fue detenido en España en septiembre de 2024 en virtud de una orden internacional, y posteriormente desapareció del control judicial mientras presuntamente conservaba acceso a material derivado de Pegasus procedente de los teléfonos del presidente del Gobierno de España y de dos ministros, con una afirmación adicional según la cual un contacto marroquí ofreció a un colaborador policial español entre dos y tres millones de euros para localizarlo [38, 39]. Se trata de una exclusiva de un único medio que descansa en fuentes de seguridad no identificadas, y el nombre de la unidad Service Action no está corroborado en ninguna otra parte de esta recopilación; debe tratarse como una pista seria y no como un hecho establecido, pero de confirmarse sería el primer desertor identificado de la DGED vinculado directamente a la cadena evidencial de Pegasus, examinada más adelante en establecido, pero de confirmarse sería el primer desertor identificado de la DGED vinculado directamente a la cadena evidencial de Pegasus, examinada más adelante en *DGST* a continuación.

La principal fortaleza de la DGED, según el registro de fuentes abiertas, es su capacidad demostrada de diplomacia de seguridad discreta y respaldada por Palacio en una región donde la influencia occidental convencional se ha debilitado, lo que otorga a Marruecos un nicho de mediación que genera crédito diplomático sin requerir reconocimiento público de la implicación de los servicios de inteligencia; sus principales limitaciones son el coste reputacional acumulado de las controversias de infiltración europeas y la controversia de atribución de Pegasus, ambas complicando las relaciones de la DGED con los mismos socios europeos que su papel de mediación en el Sahel presumiblemente busca cultivar, y la deserción de Hijaouy recientemente reportada, que, de confirmarse las acusaciones, representaría un fallo significativo de seguridad interna. La confianza en este perfil es mixta y no uniforme: la historia fundacional y la sucesión de dirección descansan en fuentes consistentes, aunque terciarias, y merecen confianza moderada a alta; los detalles actuales de personal y presupuesto tienen una década o más de antigüedad y constituyen una carencia explícita; y la atribución DGED frente a *DGST* para Pegasus en concreto es el juicio peor fundamentado y de mayor trascendencia de este perfil, descansando en el testimonio de un único consorcio de investigación que no se ha replicado de forma independiente.

DGST

La Direction Générale de la Surveillance du Territoire (DGST) es el servicio marroquí de contraespionaje interno y seguridad interna, creado por el mismo dahir real del 12 de enero de

1973 que creó la DGED, y renombrado a partir de su anterior denominación DST en 2005 [27]. A diferencia de la DGED, la DGST opera bajo la supervisión del Ministerio del Interior, con sede central en Temara y una rama subordinada de aplicación de la ley, el Bureau Central d'Investigations Judiciaires (BCIJ), con sede en Salé; su mandato fundacional abarca el contraespionaje, el contraterrorismo y la protección de activos económicos y científicos, formulado en su dahir original como la prevención, mediante la recopilación de inteligencia, de actividades inspiradas, emprendidas o respaldadas por movimientos subversivos o terroristas [27]. La sucesión en la dirección va de Ahmed Dlimi (1973-1983), pasando por Driss Basri (1983-1999, que ocupó el cargo simultáneamente con su largo mandato como ministro del Interior), Hamidou Laanigri (1999-2003) y Ahmed Harari (2003-2005), hasta Abdellatif Hammouchi, director desde diciembre de 2005 [27, 29]. Hammouchi se incorporó al servicio en 1993 a los 27 años, especializándose desde el principio en el análisis de redes islamistas y yihadistas, y dirigió su servicio de contraterrorismo tras los atentados de Casablanca de 2003 antes de su ascenso en 2005 al puesto máximo [29]. Desde el 15 de mayo de 2015 dirige también la DGSN, la policía nacional de Marruecos, una doble función que el registro de fuentes abiertas describe de forma consistente como sin precedentes en el aparato de seguridad marroquí posterior a 1999 [27, 29]. Es casi seguro que esta concentración de autoridad de inteligencia interna y de aplicación de la ley en un único responsable otorga a Hammouchi un grado de control institucional sobre la arquitectura de seguridad interna de Marruecos sin paralelo europeo directo (confianza: alta), tal como ya se estableció más arriba en *La comunidad de inteligencia*.

Una estructura subordinada pero institucionalmente significativa bajo el director es el BCIJ, creado en 2015 tras la legislación aprobada después del atentado de la cafetería de Marrakech de 2011, que otorgó por primera vez a los agentes de la DGST el estatus formal de policía judicial; el BCIJ funciona como el brazo de aplicación de la ley de la DGST mientras opera bajo la supervisión de la Fiscalía General para el trabajo de casos, un diseño de doble dependencia que otorga a la DGST un alcance procesal que no poseía anteriormente [27]. Su primer jefe fue Abdelhak Khiame, y hacia 2021 se atribuía al BCIJ el desmantelamiento de 86 células terroristas y 1.386 detenciones desde su creación en 2015, frente a un total a más largo plazo de 213 células desmanteladas desde 2002, cifras no actualizadas en el material revisado más allá de ese año [27].

Las disciplinas de recopilación de la DGST abarcan la inteligencia de señales, la inteligencia humana y, desde 2017 según información contestada pero convergente, la recopilación técnica ofensiva mediante software espía comercial. Su rama de inteligencia de señales, la Police des Communications Radioélectriques (PCR), se remonta a la década de 1960 bajo Hassan II y presuntamente intercepta miles de comunicaciones diarias, con una capacidad técnica que, según un punto de referencia de 2010, incluía búsqueda por palabras clave y análisis de reconocimiento de voz y de escritura manuscrita, mientras que un Groupe d'Intervention Rapide proporciona una capacidad de asalto de operaciones especiales [27]. La investigación del consorcio Forbidden Stories de julio de 2026 añade una capa de inteligencia humana y testimonio interno en gran medida ausente de las compilaciones terciarias: un antiguo agente de la DGST que usa el seudónimo Safir describió la distribución de teléfonos Samsung Galaxy S6 Edge preinfectados a través de tiendas de telefonía en la región del Rif y la infiltración de cibercafés para dirigirse a activistas, en el marco de un programa interno que los documentos filtrados del consorcio denominan Op S6_Edge, fechado en 2017 [33].

El papel cibernético de la DGST es el del servicio más directamente implicado, en el material revisado, en el programa Pegasus de Marruecos, aunque la solidez de esa implicación varía marcadamente según la fuente y la afirmación. El consorcio Forbidden Stories nombra a personal concreto de la DGST presuntamente implicado en operaciones de software espía —Abdeljalil Taki como jefe de departamento, el especialista informático jefe Amine Labbardi, el director Abdelaziz Brachmi, y Mohammed Raji, apodado el señor Escucha del rey— y sitúa el cambio operativo del

anterior software Remote Control System de Hacking Team a Pegasus en septiembre de 2017, cuando Taki y Labbardi presuntamente probaron Pegasus en sus propios teléfonos personales [33]. El reportaje del mismo consorcio sobre esa adquisición original añade una capa adicional y distinta: bajo el nombre en clave interno Morgan, la licencia se habría intermediado a través de FSSYS Morocco, descrita como filial del grupo Al Fahad/Edge-Etimad con sede en los EAU, y se dice que el cofundador de NSO Group y entonces consejero delegado Shalev Hulio viajó a Marruecos con un pasaporte diplomático israelí en relación con el acuerdo; el propio consorcio señala el elemento de financiación emiratí como poco claro y no confirmado, y este informe traslada esa salvedad en lugar de tratar el canal de adquisición como establecido [40]. Esto es sustancialmente más específico que tanto el hallazgo a nivel de infraestructura ATLAS de Citizen Lab como las confirmaciones forenses de dispositivo de Amnistía, ninguna de las cuales nombra a organismo o individuo marroquí alguno [30, 31, 32], y es probable (confianza: moderada) que el control operativo del programa Pegasus interno recaiga específicamente en la DGST y no en la DGED, dado que esa división descansa en la fuente de un único consorcio de investigación que es detallada e internamente consistente, pero aún no replicada de forma independiente por un segundo medio ni confirmada por ningún laboratorio forense o resolución judicial.

Tabla 6. Cuestiones de atribución en disputa en el registro de Pegasus y Jabaroot de Marruecos.

Cuestión de atribución	Posiciones en disputa	Respuesta mejor fundamentada	Confianza estimada
¿Qué servicio controla operativamente el programa Pegasus interno?	DGST (personal identificado, Op S6_Edge) frente a DGED (papel de enlace exterior/adquisición)	DGST, según el testimonio interno y los documentos filtrados de Forbidden Stories	Moderada (fuente de un único consorcio, no replicada de forma independiente)
¿Quién está detrás de la filtración Jabaroot/JabaROOT?	Actor argelino (autodescripción) frente a un antiguo oficial de inteligencia marroquí residente en Alemania frente a cinco antiguos miembros de la DGST exiliados en Europa (según Le Monde)	No resuelto; tres afirmaciones mutuamente excluyentes permanecen sin dirimir	Baja (cada afirmación de fuente única o no confirmada)
¿Qué solidez tiene la base evidencial del uso marroquí de Pegasus en general?	Hallazgos forenses de Amnistía/Citizen Lab a nivel de dispositivo e infraestructura (sin organismo identificado) frente a la atribución de organismo y personal por testimonio interno de Forbidden Stories	La confirmación forense del uso de Pegasus tiene alta confianza; la atribución a nivel de organismo descansa únicamente en testimonios	Alta para el uso; baja para la atribución de organismo

El objetivo exterior de la DGST con Pegasus, a diferencia de su uso interno contra periodistas y activistas, ha dañado directamente una de las relaciones de enlace europeas más importantes del propio servicio: Forbidden Stories informa de que una cuenta de Pegasus que sus fuentes vinculan a la DGST tuvo como objetivo al coronel Alberto Aguilera —agregado de Interior de España en Rabat entre 2012 y 2017 y el oficial de la Guardia Civil responsable de los planes de formación en contrterrorismo de la DGST— cinco veces a partir del 8 de marzo de 2019, con la edición en

español de la misma investigación identificando a la DGST como el servicio operador principal mientras la DGED aparece solo en un papel de coordinación [34, 41]. Es probable (confianza: moderada) que esto refleje una operación genuina de la DGST contra un socio de formación, dada la especificidad de los documentos filtrados y las fuentes identificadas, incluido un antiguo oficial de la DGST, aunque la afirmación no ha sido corroborada de forma independiente por un segundo medio de investigación ni confirmada por ninguno de los dos gobiernos.

La misma información sitúa a la DGST en el centro del objetivo de 2021 contra el presidente del Gobierno español Pedro Sánchez y miembros de su gabinete, junto con el anterior objetivo de ministros franceses cuya atribución de organismo está también enturbiada por el probable error de transcripción DGSE/DGED señalado más arriba en *DGED* [10, 41]. La Audiencia Nacional de España abrió una investigación judicial sobre estas infecciones en mayo de 2022, la archivó en julio de 2023 citando la falta de cooperación de Israel, la reabrió en abril de 2024 tras una Orden Europea de Investigación francesa, y la archivó por segunda vez el 22 de enero de 2026, de nuevo por insuficiencia de pruebas, con el fiscal jefe del tribunal presuntamente rechazando la evidencia subyacente por no concernir a Marruecos; ningún tribunal español ha atribuido formalmente nunca las intrusiones a Marruecos ni a ningún organismo marroquí concreto, y Marruecos ha negado su implicación en todo momento [42, 43]. La información española de septiembre de 2026 sobre la presunta posesión por Hijaouy del material de Pegasus subyacente sugiere que esta cuestión evidencial sigue genuinamente abierta y no cerrada, aunque cada afirmación concreta de ese hilo sigue siendo de un único medio y no verificada [38, 39].

El historial de enlace exterior de la DGST se extiende mucho más allá de la relación de formación con la Guardia Civil, e incluye advertencias en 2015, a las que se atribuye mérito, a homólogos franceses sobre Abdelhamid Abaaoud antes de los atentados de París de noviembre de 2015 [27]. Es muy probable (confianza: moderada) que esta función de aviso de enlace siga siendo un canal activo y valorado para los socios europeos pese a la controversia paralela de Pegasus, dado que los gobiernos europeos han continuado la cooperación en seguridad e incluso han condecorado personalmente a Hammouchi —el ministro del Interior de España le entregó la Gran Cruz de la Orden del Mérito de la Guardia Civil en noviembre de 2025— incluso después de que las revelaciones de Pegasus de 2021 ya fueran públicas, una yuxtaposición que en sí misma indica cómo los socios europeos han optado por compartimentar el valor del enlace en contraterrorismo frente a las preocupaciones por el abuso de software espía en lugar de dejar que estas últimas prevalezcan sobre el primero [44].

Las acusaciones de tortura y entrega extrajudicial vinculadas a las instalaciones de Temara constituyen la controversia de derechos humanos más persistente de la DGST: las autoridades judiciales francesas intentaron citar personalmente a Hammouchi en 2014 por denuncias de tortura, incluidas las de la activista saharauí Naama Asfari y el ciudadano franco-marroquí Adil Lamtalsi, y la inmunidad diplomática impidió su testimonio, lo que llevó a Marruecos a suspender la cooperación judicial con Francia antes de reanudarla en enero de 2015, tras lo cual Francia no obstante ascendió a Hammouchi a oficial de la Legión de Honor al mes siguiente, una secuencia que las fuentes abiertas no explican [29, 44]. Es probable (confianza: moderada) que la disposición de Rabat a suspender la cooperación judicial por este episodio refleje un patrón más amplio de uso de la influencia diplomática para proteger a la cúpula de seguridad de procesos legales extranjeros, coherente con las propias controversias de infiltración y de la policía fronteriza francesa de la DGED analizadas más arriba., coherente con las propias controversias de infiltración y de la policía fronteriza francesa de la DGED analizadas más arriba.

La controversia más reciente y menos resuelta relativa a la DGST es la filtración de Jabaroot de agosto de 2026 de un presunto conjunto de datos que cubre a más de 70.000 efectivos de seguridad marroquíes, que la DGSN y la DGST negaron conjunta y públicamente que representara una brecha en sus propios sistemas, atribuyéndolo en cambio a datos de seguros y cobertura social de

terceros ya antiguos [45]. La identidad de Jabaroot está sujeta a tres teorías de atribución mutuamente excluyentes examinadas en la tabla anterior, ninguna de las cuales este análisis intenta dirimir; lo que puede afirmarse con mayor confianza es que el material filtrado por Jabaroot se ha utilizado, según información de prensa española de septiembre de 2026 que cita un informe de la policía nacional española remitido a la jueza de la Audiencia Nacional María Tardón, para implicar personalmente a Hammouchi en la facilitación de un episodio de cruce fronterizo en Ceuta, junto con una valoración policial que describe el cruce como necesitado de una alta capacidad de influencia en redes y personas vinculadas a las fuerzas de seguridad de Marruecos, sin nombrar ella misma a ningún organismo o individuo [14, 15]. Existe una posibilidad prácticamente equivalente (confianza: baja) de que esto refleje una orden deliberada a nivel de la DGST en torno al cruce de Ceuta y no una facilitación incidental por contactos de nivel inferior, y debe tratarse como una acusación no verificada a la espera de corroboración.

La principal fortaleza de la DGST es el continuo integrado de seguridad, inteligencia y aplicación de la ley que ha construido el mandato de Hammouchi: un servicio de contraespionaje con un brazo formal de policía judicial y, desde 2015, una fusión directa al más alto nivel con la policía nacional, lo que otorga al aparato de seguridad interna de Marruecos una profundidad de coordinación que la mayoría de servicios homólogos solo logran mediante enlace interinstitucional y no mediante un mando unificado. Sus principales limitaciones son el coste reputacional acumulado de las acusaciones de tortura de Temara, la capacidad demostrada del programa Pegasus para dañar incluso la relación de formación europea más cercana de la propia DGST, y la filtración Jabaroot sin resolver, que, sea cual sea su origen real, señala bien un fallo genuino de seguridad de los datos de personal, bien una sofisticada operación de información contra el servicio. La confianza en este perfil debe leerse afirmación por afirmación: la historia fundacional, la subordinación al Ministerio del Interior, la creación del BCIJ y la cronología de liderazgo de Hammouchi descansan en fuentes consistentes y merecen confianza de moderada a alta; los detalles técnicos de capacidad del PCR y las estadísticas de desmantelamiento de células del BCIJ están desfasados; y el detalle del personal identificado detrás del programa Pegasus interno descansa enteramente en la fuente de testimonio interno de un único consorcio de investigación, la mayor carencia evidencial individual dado el peso analítico que carga la cuestión de atribución DGST frente a DGED.

Funciones de inteligencia relevantes de la DGSN

La DGSN es, ante todo, la fuerza de policía civil nacional de Marruecos, establecida el 16 de mayo de 1956 en virtud del Dahir n.º 1-56-115 para sustituir a la Police Chérifienne de la era colonial, y su relevancia para este capítulo descansa específicamente en una de sus siete direcciones constituyentes —Policía Judicial, Seguridad Pública, Sistemas de Información y Comunicación, Inteligencia General (Renseignements Généraux), Recursos Humanos, Equipamiento y Presupuesto, y Seguridad del Palacio Real— a saber, la Direction des Renseignements Généraux, que otorga a la DGSN su propia función de recopilación de información interna [28]. Esa función discurre junto al mandato de contraespionaje de la DGST, y desde mayo de 2015 se coordina en su cúpula con él, a través de la persona de Abdellatif Hammouchi, director de ambos servicios simultáneamente [28, 29]. Es casi seguro que esta fusión elimina una separación institucional entre la recopilación de información policial ordinaria y la inteligencia de contraespionaje o de seguridad interna que existe, al menos nominalmente, en la mayoría de los sistemas europeos, incluida la propia división de España entre el CNI y la Policía Nacional y la Guardia Civil (confianza: alta), dado que ninguna fuente localizada identifica una fusión comparable en un único responsable entre los principales socios de Marruecos.

Las cifras de personal y presupuesto de la DGSN en su conjunto —aproximadamente 78.146 efectivos en 2021 y un presupuesto anual de unos 13.000 millones de MAD en 2022— son

considerablemente más recientes que las cifras comparables de la DGED y la DGST expuestas más arriba, pero las fuentes abiertas no ofrecen un desglose específico del personal, presupuesto o dirección de la propia Dirección de Inteligencia General [28]. Esta es una carencia explícita y analíticamente significativa: la dirección cuya fusión con la DGST más contribuye a concentrar la autoridad de inteligencia interna marroquí es también aquella sobre la que las fuentes abiertas dicen menos respecto a su organización interna o sus resultados.

El punto de fusión operativa más claramente documentado entre la DGSN y la DGST más allá del nivel de dirección es que la unidad de delincuencia organizada del BCIJ opera bajo supervisión conjunta con la propia Brigada Nacional de Policía Judicial de la DGSN, junto a una unidad de contraterrorismo separada bajo dirección directa de la DGST [27]. Es probable (confianza: moderada) que este diseño de doble unidad refleje un esfuerzo deliberado por encauzar el trabajo de casos de contraterrorismo a través de la cadena más orientada a la inteligencia de la DGST, manteniendo al mismo tiempo el trabajo de casos de delincuencia organizada convencional bajo la estructura de policía judicial ordinaria de la DGSN, dado que la división sigue los respectivos mandatos centrales de ambos servicios en lugar de parecer arbitraria.

La iniciativa reciente más visible de la DGSN próxima al ámbito cibernético es la plataforma digital de denuncia ciudadana E-blagh, lanzada en octubre de 2024, que permite al público denunciar contenido en línea valorado como delictivo o violento, circunscrita explícitamente a la incitación al terrorismo, las amenazas a menores y las infracciones de protección de datos, y a la que se atribuye el procesamiento de 7.083 notificaciones a esa fecha [28]. Se trata de una herramienta de moderación de contenidos y denuncia ciudadana, no de evidencia de una capacidad ofensiva o técnica de investigación cibernética, y ninguna fuente localizada describe una unidad técnica de investigación cibernética de la DGSN comparable a la dirección de inteligencia de señales PCR de la DGST. Es probable (confianza: moderada) que esto refleje una división del trabajo genuina en la que la recopilación cibernética ofensiva y técnica recae en la DGST, y la ciberseguridad defensiva en la autoridad civil DGSSI/maCERT, y no en la DGSN, dado que la información sobre capacidad cibernética marroquí recopilada a lo largo de este proyecto se concentra de forma consistente en esos otros organismos y no en la DGSN.

El desarrollo reciente más trascendente que afecta a la dirección con relevancia de inteligencia de la DGSN es la acusación de septiembre de 2026, examinada en detalle más arriba en *DGST*, según la cual Hammouchi —en su capacidad que abarca tanto la DGSN como la DGST— desempeñó un papel personal en la facilitación del episodio de cruce fronterizo en Ceuta; la valoración policial española subyacente está redactada en términos de capacidad, describiendo el cruce como necesitado de un proceso predefinido con objetivos distintos de los migratorios, sin nombrar ella misma específicamente a Hammouchi, la DGSN o la DGST, y la atribución personal en la cobertura de la prensa española se deriva de combinar ese lenguaje con la afirmación propia, separada y no verificada de forma independiente, de Jabaroot [14]. Existe una posibilidad prácticamente equivalente (confianza: baja) de que esto refleje una dirección personal genuina de Hammouchi y no una facilitación de nivel inferior que la prensa ha asociado por relación al funcionario de seguridad más visible de Marruecos, y debe tratarse como una acusación seria pero no demostrada.

La principal fortaleza de la DGSN, para las funciones de inteligencia relevantes para este perfil, es la escala: una base de personal un orden de magnitud mayor que la de la DGED o la DGST otorga a su Dirección de Inteligencia General un alcance de recopilación interna que ninguno de los dos servicios de inteligencia dedicados puede igualar solo en números. Su principal limitación es la opacidad: a diferencia de la DGST y la DGED, que cada una genera controversias periódicas visibles en prensa que al menos iluminan parcialmente su actividad, la Dirección de Inteligencia General en concreto ha generado casi ninguna información independiente de fuentes abiertas sobre sus métodos, resultados o dirección actual, lo que deja su contribución real al panorama de

inteligencia interna de Marruecos esencialmente inevaluable a partir del material revisado. La confianza en esta sección debe leerse, por tanto, como alta para los hechos institucionales y estructurales —fundación, escala de personal, la fusión de doble función de Hammouchi, el alcance limitado de la plataforma E-blagh— y explícitamente baja a inevaluable para cualquier cosa relativa a la actividad operativa real de la Dirección de Inteligencia General, que constituye la carencia individual más clara de este perfil.

Orden público y seguridad interna

Más allá de la fusión de inteligencia DGST/DGSN perfilada en el capítulo anterior, el aparato de seguridad interna de Marruecos descansa en cuatro fuerzas distintas con mandatos solapados pero formalmente separados: la DGSN como policía civil nacional, el BCIJ como brazo de policía judicial de la DGST para el contraterrorismo, la Gendarmería Real como fuerza policial militarizada rural y de carreteras, y las Fuerzas Auxiliares como reserva de propósito general para el orden público, el socorro en catástrofes y el apoyo a las otras tres [46, 47, 48, 49]. La evidencia reciente más clara de que estos organismos funcionan como instituciones paralelas y no jerárquicamente vinculadas es operativa y no doctrinal: en el intento de cruce migratorio masivo del 15 de agosto de 2026 en la valla fronteriza de Ceuta, personal de la DGSN, la Gendarmería Real y las Fuerzas Auxiliares operó codo con codo empleando helicópteros, unidades terrestres y tácticas de contención, el ejemplo documentado más claro de despliegue conjunto de las tres instituciones de seguridad interna en un único evento [13, 50].

No se identificó en esta investigación ninguna fuente primaria que describa el protocolo de coordinación operativa que vincula las propias cadenas prefectorales de estas instituciones con los walis y gobernadores que encabezan formalmente la administración civil de cada wilaya, y esa ausencia se registra como una carencia estructural explícita y no se infiere solo de la jerarquía administrativa [51]. La tabla siguiente ofrece una instantánea institucional comparativa antes de los perfiles individuales, que prestan especial atención a cómo se relaciona cada fuerza con las FAR, el Ministerio del Interior y la fusión DGST/DGSN, dado que es precisamente en esas costuras donde la seguridad interna marroquí está menos documentada en fuentes abiertas.

Tabla 7. Las cuatro fuerzas de seguridad interna de Marruecos de un vistazo.

Organismo	Fundación	Depende de	Dirección actual	Personal / presupuesto	Mandato principal
DGSN	16 may. 1956 (Dahir n.º 1-56-115)	Ministerio del Interior	Abdellatif Hammouchi (desde 2015; también director de la DGST)	~79.830 efectivos (2023); presupuesto de 13.000 millones de MAD (2022)	Policía civil, policía judicial, control fronterizo, Inteligencia General
BCIJ	2015 (ley posterior al atentado de Marrakech)	DGST (brazo de policía judicial); Fiscalía General para el trabajo de casos	Cherkaoui Habboub / Haboub Cherkaoui (desde ~2021; continuidad hasta 2026 con baja confianza)	No identificado en fuentes abiertas (no se localizó cifra actual de personal)	Investigación de policía judicial en contraterrorismo y delincuencia organizada

Gendarmería Real	29 abr. 1957 (Dahir n.º 1-57-079)	FAR (estatus militar); Justicia (policía judicial); Interior (policía administrativa)	Ministro delegado Abdellatif Loudiyi (admin.); general Haramou (comandante de campo) — fechas de nombramiento no identificadas	Las fuentes discrepan: ~75.000 (una fuente) frente a ~25.000 (otra) — brecha triple sin resolver	Policía rural/de carreteras, interdicción marítima, seguridad fronteriza y costera
Fuerzas Auxiliares	Reorganizadas en 2018 (Dahir n.º 1.17.71); linaje anterior no documentado	Ministerio del Interior	Coronel mayor Mustapha Hdioud (Sur, desde oct. 2020); general Khaled Jabrane (Norte, desde oct. 2020)	No identificado en fuentes abiertas (no se localizó cifra de personal o presupuesto)	Apoyo al orden público, socorro en catástrofes, sin función de policía judicial

DGSN

La Direction Générale de la Sûreté Nationale, la policía civil nacional de Marruecos, se estableció el 16 de mayo de 1956 tras la independencia bajo el rey Mohamed V y sigue teniendo su sede en Rabat bajo autoridad del Ministerio del Interior [46]. La dirección ha pasado por una secuencia documentada e ininterrumpida de directores generales —Hamidou Laanigri (2003-2006), Charki Draiss (2006-2012), Bouchaib Rmail (2012-2015) y Abdellatif Hammouchi, que ocupa el cargo desde 2015 y continúa dirigiendo simultáneamente la DGST, la fusión personal que el capítulo de este informe sobre la *comunidad de inteligencia* trata como el hecho de coordinación más claro de Marruecos [46, 52]. Bajo esta dirección nacional existe al menos un puesto subnacional identificado, director de seguridad pública, ocupado hasta agosto de 2026 por El Hail Zitouni a lo largo de una carrera de cuatro décadas que incluyó el mando de una operación de 2024 en Marrakech con 1.200 agentes, 2.956 detenciones y 415 incautaciones de vehículos; la muerte de Zitouni dejó el puesto vacante, y no se identificó ningún sucesor en fuentes abiertas a fecha de esta recopilación, una carencia estructural que este informe registra explícitamente en lugar de darla por resuelta [53].

La propia descripción organizativa de la DGSN, de fuente terciaria, afirma tres divisiones especializadas —una Policía de Fronteras, un Cuerpo Móvil de Intervención y una Brigada Nacional que se ocupa de la investigación de delitos graves, incluidos el terrorismo y los delitos de cuello blanco— aunque no se localizó ninguna cita primaria única para esta estructura exacta, por lo que se mantiene con confianza moderada y no alta (confianza: moderada) [46]. Una capa más granular se corrobora de forma independiente a nivel regional: el lanzamiento en agosto de 2026 por la Dirección de Seguridad de Agadir de una octava brigada regional de desactivación de explosivos, tras equivalentes en Rabat, Casablanca, Fez, Tánger, Uchda, Marrakech y Laayoune, confirma que las unidades especializadas dependen de prefecturas regionales de seguridad y no

directamente de la sede central nacional, y que este despliegue se extiende al Sáhara Occidental a través de la unidad de Laayoune [54]. La fortaleza de personal se reportó en aproximadamente 79.830 en 2023, frente a unos 46.000 en 2007 y 70.000 en 2017, con un presupuesto anual de 13.000 millones de MAD para 2022 [46, 52]. Es probable que la DGSN esté llevando a cabo un programa genuino y dotado de recursos de modernización tecnológica y no uno meramente retórico, dado el despliegue en julio de 2026 en Casablanca de vehículos de patrulla Amane y Madar equipados con IA, con reconocimiento automático de matrículas y reconocimiento facial (confianza: moderada, dado que las cifras de rendimiento citadas proceden de la DGSN/el proveedor y no se sometieron a prueba independiente) [55].

El papel cibernético de la DGSN sigue siendo escaso en el registro de fuentes abiertas: la única función documentada de forma concreta es E-blagh, una plataforma digital orientada al ciudadano para denunciar contenido en línea delictivo o violento, sin que se localizara detalle alguno sobre una brigada interna dedicada de investigación de cibercrimen, su personal o su carga de casos, una ausencia que se interpreta como una carencia de recopilación declarada y no como evidencia de que tal capacidad no exista, especialmente dado que el propio dgsn.gov.ma resultó inaccesible en repetidos intentos a lo largo de esta ronda de recopilación y de la anterior [52]. Las asociaciones con el extranjero están mejor documentadas: la Oficina Central Nacional de INTERPOL de Marruecos en Rabat opera desde el 17 de junio de 1957, el canal multilateral más antiguo y amplio identificado en esta recopilación, y una operación conjunta de octubre de 2025 con la Policía Nacional española, desencadenada por un chivatazo de origen de la DGSN, incautó más de 22 toneladas de hachís ocultas en camiones frigoríficos de productos agrícolas en las provincias de Cádiz y Granada [56, 57]. Un conjunto adicional de afirmaciones de asociación de 2024-2026 con Francia, el Reino Unido, la aseguradora francesa ARGOS y el FBI descansa en una única fuente terciaria no cotejada con ninguna publicación primaria francesa, británica o estadounidense, y se trata como probablemente exacto a grandes rasgos pero no confirmado en detalle (confianza: baja) [52].

Las principales fortalezas documentadas de la DGSN son una trayectoria sostenida de crecimiento de personal y presupuesto, un programa activo de modernización tecnológica, y un despliegue de unidades especializadas que ahora se extiende al Sáhara Occidental, lo que indica que el alcance administrativo de la institución iguala la extensión territorial completa reivindicada por Marruecos. Su limitación más concreta es la vacante de liderazgo en el puesto subnacional de director de seguridad pública tras la muerte de Zitouni, junto con un patrón más amplio en el que varias afirmaciones estructurales descansan en fuentes terciarias únicas y no en documentación primaria de la DGSN, ella misma inaccesible a lo largo de esta recopilación. Es muy probable que las funciones centrales de policía civil y policía judicial de la DGSN estén descritas con precisión a grandes rasgos por las fuentes revisadas (confianza: alta, dados los relatos convergentes e independientes de prensa y enciclopédicos), pero su estructura divisional precisa, su capacidad cibernética y la durabilidad de sus asociaciones extranjeras más recientes deben tratarse todas con confianza baja a moderada a la espera de un acceso a fuentes primarias que esta investigación no pudo obtener.



Figura 3. El emblema de la DGSN, calcado del propio informe anual de 2021 del servicio.

El emblema es un escudo con forma de placa policial rematado por una corona real, ella misma coronada por una pequeña estrella de cinco puntas, que evoca la corona real marroquí utilizada en toda la insignia institucional del Estado para denotar la autoridad de la monarquía sobre los servicios de seguridad; el campo rojo principal porta una gran estrella verde de cinco puntas, el mismo pentagrama al estilo del Sello de Salomón que figura en la bandera nacional, con una letra árabe estilizada debajo, y el borde verde del escudo lleva un motivo de laurel blanco a cada lado [58]. No se localizó en las fuentes revisadas ningún texto oficial de la DGSN que explique el significado heráldico concreto de estos elementos; la descripción anterior es un inventario visual factual y no una glosa simbólica fundamentada en fuentes, y la letra bajo la estrella se registra como una abreviatura no confirmada y no como una declarada.

BCIJ

El Bureau Central d'Investigations Judiciaires se fundó en 2015 en virtud de una ley aprobada tras el atentado del 28 de abril de 2011 en Marrakech (cafetería Argana, en la plaza Djemaa el-Fna), que otorgó por primera vez a los agentes de la DGST estatus de policía judicial, y tiene su sede en Salé [47]. Estructuralmente, la oficina está subordinada a la DGST —el servicio de inteligencia interna de Marruecos— mientras opera bajo supervisión de la Fiscalía General a efectos de la investigación judicial; la misma fuente terciaria describe una división interna entre una división de élite de contraterrorismo supervisada directamente por la DGST y una unidad de delincuencia organizada supervisada en cambio por la propia Brigada Nacional de Policía Judicial de la DGSN, un vínculo interinstitucional que aquí se recoge con confianza moderada y no alta dada su fuente única [47]. Esto sitúa la posición legal y administrativa del BCIJ claramente dentro de la cadena de inteligencia interna y no en la jerarquía policial ordinaria, y no se identificó en ninguna fuente revisada relación operativa o de mando alguna entre el BCIJ y las FAR, coherente con su carácter explícitamente civil y de policía judicial.

La dirección ha pasado por al menos dos, y muy probablemente tres, personas identificadas desde 2015. Su jefe fundador, Abdelhak Khiame, dirigió la oficina desde su creación hasta su muerte en agosto de 2022 [47]. Una entrevista de octubre de 2021 nombra a Haboub Cherkaoui como jefe en funciones del BCIJ en esa fecha —lo que significa que ya había sucedido a Khiame antes de la muerte de este— y una instantánea de Wikipedia en francés, editada por última vez el 15 de abril de 2026, nombra a Cherkaoui Habboub, el mismo nombre reordenado, como director actual del artículo [59, 60]. Es probable que Cherkaoui/Habboub siguiera siendo jefe del BCIJ durante la primera mitad de 2026 (confianza: baja), dado que esto descansa en una única fuente terciaria sin confirmación de prensa independiente de continuidad, y la variación en el orden del nombre entre ambas fuentes se señala en lugar de resolverse silenciosamente.

En cuanto a estadísticas, la propia información de la oficina le atribuía 91 células dismanteladas y más de 1.400 personas remitidas a la justicia desde 2015 a fecha de marzo de 2023, aproximadamente el 85 % afiliadas a Dáesh, frente al total de más largo plazo de la propia DGST de 213 células dismanteladas desde 2002; ninguna de las dos cifras se ha actualizado en las fuentes revisadas más allá de esa fecha [47, 60]. Una operación de abril de 2026 con fecha directa demuestra, no obstante, un ritmo continuado: se dismanteló una célula de seis miembros entre Kenitra, Casablanca, Dar El Gueddari y Sidi Taibi, encuadrada por declaraciones del BCIJ/la DGST como dedicada al robo, el hurto con fractura y el blanqueo de capitales bajo una justificación de legitimación ideológica del botín, dirigida contra granjas ganaderas rurales para su reventa a través de mercados locales [61]. Es probable que el BCIJ siga integrando delitos ordinarios de delincuencia organizada en el trabajo de casos etiquetado como terrorismo cada vez que se alega un barniz ideológico (confianza: moderada, basada en este caso único pero detallado de 2026), un patrón que difumina la línea entre sus mandatos de contrterrorismo y delincuencia organizada incluso donde su estructura interna de unidades los separa formalmente.

Las asociaciones con el extranjero están comparativamente bien documentadas para el BCIJ. Una operación conjunta de noviembre de 2024 con la Comisaría General de Información (CNP) de España detuvo a nueve sospechosos en Tetuán, Fnideq, Madrid, Ibiza y Ceuta, descrita en la prensa marroquí como parte de una colaboración de seguridad excepcional de larga data que se apoya en acciones conjuntas previas de junio y julio de 2024 [62]. Una compilación terciaria distinta cita además el contacto de la DGST con el BND alemán respecto a Anis Amri antes del atentado de Berlín de diciembre de 2016, el intercambio de información de la DGST con las autoridades francesas sobre el paradero de Abdelhamid Abaaoud antes de los atentados de París de noviembre de 2015, una declaración de seguridad Catar-Marruecos de 2022 vinculada al Mundial de la FIFA, y un acuerdo Marruecos-Alemania de octubre de 2022 que abarca delincuencia organizada, terrorismo, trata de personas, cibercrimen y fraude [47]. No se identificó ningún instrumento formal confirmado BCIJ-Europol o BCIJ-CNI (España), y los episodios de Amri/Abaaoud se atribuyen en la propia fuente a la DGST a nivel de inteligencia y no al BCIJ como organismo ejecutor de policía judicial, una distinción que este informe preserva en lugar de difuminar.

Una declaración de la dirección del BCIJ en este registro lleva una señal específica de negación/engaño: en una entrevista de octubre de 2021 en la sede del BCIJ, Cherkaoui afirmó que el Frente Polisario es un importante proveedor de yihadistas, junto con afirmaciones sobre un complot frustrado en Tánger y la expansión de Dáesh en la región del Sahel [59]. Se trata de una afirmación de fuente única y políticamente cargada de un responsable cuya institución tiene un interés evidente en deslegitimar al principal adversario de Marruecos en el Sáhara Occidental, y debe leerse como una narrativa oficial declarada y no como un hecho corroborado de forma independiente; ninguna otra fuente de esta recopilación la corrobora ni la contradice. No se identificó ninguna capacidad cibernética interna dedicada del BCIJ más allá de una referencia de pasada al cibercrimen dentro del acuerdo de cooperación más amplio con Alemania de octubre de 2022, una ausencia que se registra como una carencia explícita y no se asume como inexistencia.

La principal fortaleza documentada del BCIJ es un historial de dismantelamiento de células de una década, con crecimiento incremental, corroborado en compilaciones independientes y al menos un caso operativo de 2026 con fecha directa, junto con la red de enlace multipaís más concretamente evidenciada —España, Alemania, Catar— de cualquier institución perfilada en este capítulo. Sus principales limitaciones son una identidad de dirección actual no confirmada que descansa en una única fuente de baja confianza, una susceptibilidad evidente al encuadre público politizado, y la ausencia de presencia web primaria accesible o de estadísticas publicadas oficialmente más allá de la cifra de marzo de 2023. Es muy probable que el BCIJ siga siendo el brazo de policía judicial operativamente activo de la DGST para el contrterrorismo hasta 2026 (confianza: alta, dada la operación con fecha de abril de 2026), pero la confianza en su dirección

precisa, la fortaleza de sus unidades internas y su capacidad cibernética sigue siendo baja. Sobre el emblema: no se identificó ningún emblema del BCIJ distinto y publicado oficialmente; el único logotipo que circula en línea es un gráfico autopublicado de Wikimedia Commons atribuido a un editor anónimo sin cita a ninguna publicación del BCIJ o la DGSN, coherente con que el BCIJ opere como una emanación de la estructura DGST/DGSN y no mantenga una identidad de marca separada [63].

Gendarmería Real

La Gendarmerie Royale se fundó el 29 de abril de 1957 bajo el rey Mohamed V (Dahir n.º 1-57-079), con un Dahir n.º 1-57-280 de marco operativo posterior, del 14 de enero de 1958, que establece su organización detallada; un intento de obtener el texto primario completo de este dahir fundacional a través de refworld.org devolvió un error HTTP 403 en esta investigación, dejando el texto en sí sin verificar y sus disposiciones conocidas solo a través de un resumen terciario [48, 64]. Ese resumen describe a la Gendarmería como explícitamente una fuerza militar en estructura, administración y mando, subordinada a las FAR y compuesta por oficiales y suboficiales, mientras que su mandato se divide entre funciones de policía judicial bajo supervisión del Ministerio de Justicia y funciones de policía administrativa —seguridad fronteriza, control de tráfico, protección de puertos y aeropuertos, aplicación de la ley contra la pesca ilegal— bajo supervisión del Ministerio del Interior, superpuestas a su cadena hacia las FAR a través del secretario general de la Administración de Defensa [48, 64]. Este carácter legal dual civil/militar la distingue claramente tanto de la policía puramente civil de la DGSN como del estatus puramente dependiente del Ministerio del Interior de las Fuerzas Auxiliares.

Su estructura territorial comprende una Comandancia General que supervisa 22 Gendarmerías Regionales, 64 compañías y 322 puestos, complementada por divisiones de Gendarmería Móvil, Aérea y Marítima y una unidad de intervención especial, el GSIGR; estas cifras concretas se afirman sin una cita primaria claramente fechada y se mantienen con confianza moderada y no alta a la espera de una verificación directa frente a un Bulletin Officiel o un documento emitido por la Gendarmería, que esta investigación no pudo obtener [48]. Las cifras de personal presentan una discrepancia genuina y sin resolver que este informe señala en lugar de resolver: una fuente da aproximadamente 75.000 efectivos, mientras que una compilación terciaria distinta da solo unos 25.000 para lo que debería ser la misma institución, una brecha triple que ninguna de las dos fuentes permite a este informe dirimir [48, 65]. La dirección actual identificada comprende al ministro delegado Abdellatif Loudiyi, responsable de los asuntos administrativos de Defensa Nacional que afectan a la Gendarmería, y a un general Haramou como comandante de campo; no se identificó en esta investigación ninguna fecha de nombramiento, duración del mandato o predecesor para ninguno de los dos puestos, y esta ausencia se registra como una carencia y no se rellena por inferencia [48].

No se identificó en esta investigación ninguna subordinación entre la Gendarmería y la DGSN o la DGST, coherente con que los tres organismos operen como instituciones paralelas y no jerárquicamente vinculadas; el ejemplo documentado más claro de coordinación interinstitucional es de nuevo la operación fronteriza de Ceuta del 15 de agosto de 2026, en la que la vigilancia por helicóptero y las unidades terrestres de la Gendarmería Real operaron junto a personal de la DGSN y las Fuerzas Auxiliares en el mismo evento [13, 50]. Una subunidad marítima identificada con un área de responsabilidad definida, la Gendarmería Marítima Real de M'diq, interceptó por separado una embarcación neumática con trece migrantes bangladesíes en octubre de 2025, lo que evidencia una granularidad de mando a nivel operativo por debajo de la capa de mando regional [66]. Una interdicción en julio de 2026 frente a Tarfaya, en la región de Laayoune-Sakia El Hamra, incautó más de tres toneladas de cocaína transferidas en el mar desde un buque a embarcaciones neumáticas antes del desembarco —la evidencia de 2026 más clara de que el papel de

contranarcóticos marítimo de la Gendarmería ahora se extiende a la cocaína en tránsito atlántico cerca del Sáhara Occidental, y no solo al comercio de cannabis/hachís más comúnmente asociado con Marruecos [67]. Esto sugiere, con confianza moderada, que la Gendarmería funciona como la institución líder de Marruecos específicamente para la interdicción de narcóticos en el mar, complementando el papel de cooperación transfronteriza más terrestre de la DGSN en materia de hachís.

Dos casos judiciales reportados de forma independiente documentan la narcocorrupción como una vulnerabilidad institucional recurrente, y no aislada, dentro de las filas de la Gendarmería. En Beni Mellal, 37 agentes de la gendarmería fueron juzgados por aceptar sobornos para proteger las operaciones de un narcotraficante, quien admitió pagos tanto directos como a través de intermediarios, aunque no se había reportado ningún veredicto a fecha de la publicación del artículo en marzo de 2025 ni se localizó en ninguna otra parte de esta recopilación [68]. Por separado, en el distrito de El Borouj/Beni Meskine, se ordenó la detención de siete gendarmes en enero de 2025 por cargos de ocultar la actividad delictiva de un capo de la droga antes de un asesinato que el capo presuntamente cometió contra un antiguo asociado [69]. Es probable que la narcocorrupción represente una limitación institucional recurrente y no aislada para la Gendarmería (confianza: moderada), dados estos dos procesos judiciales reportados de forma independiente y geográficamente distintos en un lapso de aproximadamente dos años, aunque ambos descansan únicamente en información de prensa sobre procedimientos judiciales aún sin resolver y no en un registro adjudicado definitivo.

Una limitación adicional documentada es la exposición de la Gendarmería a la agitación interna a nivel de puestos rurales individuales: en octubre de 2025, un puesto de la Gendarmería Real en Lqliaa, cerca de Agadir, fue atacado durante protestas vinculadas a Gen Z 212 por una multitud reportada en más de 200 personas, incluidos menores armados, con un resultado de tres muertos y ocho gendarmes heridos, con el fiscal Abderrazak Fattah atribuyendo el uso por los gendarmes de armas de servicio a legítima defensa tras disparos de advertencia [70]. No se localizó corroboración independiente y no oficial del encuadre de legítima defensa ni de las cifras precisas de víctimas, por lo que este incidente se traslada como de fuente única del relato de la fiscalía y no como un hecho verificado de forma independiente. En cuanto a recursos técnicos y humanos, asociaciones con el extranjero y papel cibernético, esta investigación es genuinamente escasa: no se localizó ninguna capacidad cibernética dedicada específicamente para la Gendarmería, y la única afiliación multilateral documentada es la pertenencia a FIEP, la asociación internacional de gendarmerías y fuerzas policiales con estatus militar, desde 1999 [48]. Estas se registran como carencias explícitas y no se asume que reflejen los registros de asociación más desarrollados de la DGSN o el BCII.

En conjunto, la principal fortaleza documentada de la Gendarmería es una huella territorial y marítima amplia y multidominio, evidenciada por operaciones concretas de 2025-2026 que abarcan la interdicción de cocaína, la interceptación de tráfico de migrantes y la respuesta al orden público rural, mientras que sus limitaciones más concretas son las acusaciones recurrentes de narcocorrupción y la vulnerabilidad demostrada de los puestos fijos ante la violencia de masas — ambos juicios sostenidos con confianza moderada dada la dependencia de información de prensa sobre procedimientos aún sin resolver. La discrepancia sin resolver en el recuento de personal agrava esta incertidumbre, dejando genuinamente abierta cualquier valoración de la capacidad y densidad reales de la fuerza.



Figura 4. El emblema asociado a la Gendarmerie Royale en fuentes abiertas (salvedad de procedencia más abajo).

La imagen representa un escudo hexagonal rematado por una corona real, flanqueado por dos serpientes o cordones estilizados enrollados alrededor del marco del escudo, con fragmentos de escritura árabe en el borde que se leen en parte como real y el rey, y una estrella verde de cinco puntas con un centro rojo en su corazón, rodeada de líneas doradas radiantes [71]. A diferencia de los emblemas de la DGSN, la Guardia Real y las Fuerzas Auxiliares en este informe, el propio registro de Wikimedia Commons de este archivo no cita ninguna fuente oficial gubernamental o de reclutamiento, por lo que su autenticidad como reproducción precisa de la insignia real de la Gendarmería no puede confirmarse de forma independiente solo a partir del registro de la fuente; se presenta aquí como la imagen usada desde hace tiempo con este propósito en Wikipedia y no como un archivo oficial verificado, y no se localizó ninguna explicación oficial de sus elementos heráldicos.

Fuerzas Auxiliares

Las Forces Auxiliaires se describen en fuentes secundarias abiertas como un cuerpo antiguo dentro del aparato de seguridad de Marruecos, que opera bajo autoridad del Ministerio del Interior, aunque no se corroboró ninguna fecha de fundación ni linaje institucional anterior a 2018 mediante ninguna fuente primaria o de fiabilidad clasificada localizada en esta investigación, y este informe registra esa ausencia explícitamente en lugar de ofrecer una narrativa fundacional sin fuente [49]. Lo que sí está bien documentado es una reorganización legal de 2018: el rey Mohamed VI, actuando como comandante supremo y jefe del Estado Mayor de las FAR, aprobó un plan de reestructuración en una reunión del Consejo de Ministros del 22 de enero de 2018, plasmado más tarde en forma legal como el Dahir n.º 1.17.71 del 15 de febrero de 2018, que sustituyó a textos anteriores de 1973 y 1976 [49, 72]. Dos décrets de aplicación fechados el 6 de marzo de 2018 se confirmaron de forma independiente en el portal oficial marroquí de textos legales mmisp.gov.ma —el Décret n.º 2.17.827, que reorganiza la escuela de formación de oficiales/cuadros de la fuerza, y el Décret n.º 2.17.825, que rige la organización de sus servicios administrativos centrales y regionales— la corroboración de fuente primaria más clara obtenida en todo este capítulo [73].

El mando está estructuralmente bifurcado y no es único: dos Inspecciones Generales, una Zona Norte con sede en Rabat y una Zona Sur con sede en Agadir, se sitúan por encima de tres componentes funcionales —unidades territoriales que proporcionan presencia administrativa y de seguridad local, unidades móviles de intervención para la respuesta al orden público y la seguridad fronteriza, y unidades de apoyo logístico [49]. Ambos puestos de inspector general cambiaron de manos el 22 de octubre de 2020: el coronel mayor Mustapha Hdioud asumió la Zona Sur, sustituyendo al general Lahcen Imejane, que se retiraba, mientras que el general Khaled Jabrane asumió la Zona Norte, sustituyendo al general Mostafa Mestour, con ambos oficiales entrantes procedentes directamente de destinos de mando de las FAR y no de una carrera interna del

Ministerio del Interior [74]. Una instantánea terciaria editada por última vez el 18 de agosto de 2026 sigue nombrando a los mismos dos oficiales como comandantes de zona, lo que sugiere, con confianza moderada, aproximadamente seis años de continuidad en este par de dirección, y no se identificó en ninguna fuente revisada un único comandante general nacional por encima de los dos inspectores de zona de igual rango [49].

El mandato de la fuerza se centra en el mantenimiento del orden público en apoyo de los administradores territoriales, funciones de apoyo administrativo y asistencia en socorro de catástrofes, sin función propia de policía judicial o de investigación [49]. Su posición legal la sitúa bajo el Ministerio del Interior y no en la cadena de las FAR, pese a que ambos comandantes de zona actuales son oficiales generales de origen de las FAR, y el mando y control específicamente respecto a los walis y gobernadores a los que está mandatada para apoyar no fue detallado por ninguna fuente revisada más allá de la declaración general de ese papel de apoyo —una carencia que se suma al mismo silencio de coordinación con los walis ya señalado para la DGSN [49, 51]. La única evidencia operativa de 2026 con fecha directa para las Fuerzas Auxiliares específicamente es su participación, junto a la DGSN y la Gendarmería Real, en la respuesta al intento de cruce migratorio masivo del 15 de agosto de 2026 en la frontera de Ceuta, el ejemplo documentado más claro de las tres instituciones de seguridad interna operando conjuntamente en un único evento [13]; no se localizó ninguna operación independiente distinta de este despliegue conjunto, lo cual es coherente con, aunque no demuestra, la caracterización de la fuerza como una institución de apoyo y no de iniciativa independiente.

Los recursos técnicos y humanos, el papel cibernético y las asociaciones con el extranjero son los tres puntos en los que esta investigación es más claramente escasa específicamente para las Fuerzas Auxiliares: no se localizó ninguna cifra total de personal, presupuesto ni inventario de equipamiento, no se identificó ninguna capacidad cibernética de ningún tipo, y no se identificó ninguna asociación de enlace con el extranjero identificada, en claro contraste con el registro de la DGSN orientado a INTERPOL y España y el registro del BCIJ con España/Alemania/Catar [73]. Esta asimetría se trata como un rasgo estructural genuino —una fuerza de apoyo al orden público interno no requeriría evidentemente tales asociaciones— y no como un artefacto de una búsqueda incompleta, aunque no puede distinguirse por completo de esta última con la evidencia disponible. La principal fortaleza documentada de la fuerza es una modernización de 2018 claramente fechada y dirigida por el rey, con textos legales primarios corroborados y una dirección de zona estable y continua desde octubre de 2020; su principal limitación es la ausencia casi total de detalle de fuentes abiertas sobre su tamaño, presupuesto, capacidad técnica y asociaciones exteriores, lo que limita cualquier valoración de su peso operativo relativo a la DGSN y la Gendarmería más allá del único despliegue conjunto documentado.

Es probable que las Fuerzas Auxiliares funcionen tal como se pretende —un cuerpo de apoyo al orden público controlado por el Ministerio del Interior, con oficiales de las FAR, que opera bajo administradores civiles territoriales— y no como un actor de seguridad independiente con perfil propio de investigación o de enlace exterior (confianza: moderada, basada en la ausencia consistente de evidencia en contrario), aunque este juicio descansa sustancialmente en una ausencia de evidencia y no en un registro positivo sólido, y se registra como tal.



Figura 5. El emblema de las Fuerzas Auxiliares, procedente de un anuncio oficial de reclutamiento de la Inspection Générale des Forces Auxiliaires.

La insignia es un escudo rematado por una corona real, con dos lanzas o tridentes cruzados detrás; el campo rojo del escudo porta una estrella verde de cinco puntas del mismo estilo de Sello de Salomón que aparece en la bandera nacional y otros emblemas de servicios de seguridad, y una filacteria debajo reza Dios, Patria, Rey, el lema nacional oficial de Marruecos [75]. No se localizó en las fuentes revisadas ningún documento oficial de las Forces Auxiliares que explique el significado heráldico concreto de las lanzas cruzadas; la corona, la estrella y el lema nacional son coherentes con la iconografía de seguridad estatal marroquí ampliamente utilizada, pero el significado específico de las lanzas no está documentado y no se especula sobre él aquí.

Fuerzas Armadas e inteligencia militar

Las Forces Armées Royales (FAR) son las fuerzas militares nacionales unificadas de Marruecos, y el rey Mohamed VI ostenta el título constitucional de comandante supremo y jefe del Estado Mayor General, un papel que Palacio trata como sustantivo y no ceremonial [65, 76]. La administración cotidiana discurre a través de un ministro delegado de la Administración de la Defensa Nacional —Abdellatif Loudiyi ha ocupado este puesto de forma continua desde diciembre de 2010— dado que Marruecos no mantiene un Ministerio de Defensa convencional, un arreglo que mantiene a la institución respondiendo hacia arriba ante Palacio y no ante ningún gobierno electo [65]. Es muy probable que esta estructura dual —una cúspide de mando real sobre una burocracia de defensa administrada civilmente pero leal a Palacio— siga siendo el hecho individual más importante para entender cómo se dirige realmente a las FAR, más aún que cualquier orden de batalla a nivel de rama (confianza: alta), dado que toda otra afirmación estructural recopilada es coherente con ella y ninguna la contradice. La tabla siguiente ofrece una instantánea comparativa de los organismos estructuralmente más distintivos de las FAR antes de los perfiles individuales que siguen.

Tabla 8. Comparación de cuatro organismos estructuralmente distintivos de las Fuerzas Armadas.

Organismo	Relación de mando	Personal (reportado)	Dirección clave	Papel principal
Arquitectura de mando de las FAR	Bajo el rey como comandante supremo; ministro delegado Loudiyi (administración)	Ejército ~175.000-250.000; Fuerza Aérea ~13.000-16.000; Armada ~7.800-12.000 (las fuentes divergen)	Teniente general Mohamed Berrid, inspector general desde el 22 de abril de 2023	Defensa nacional convencional y empleo de la fuerza

Oficinas 2. ^a y 5. ^a	Oficinas numeradas adscritas al Estado Mayor de las FAR (línea de dependencia no confirmada)	No identificado en fuentes abiertas	No identificado en fuentes abiertas (sin jefe actual confirmado para ninguna de las dos oficinas)	Inteligencia militar (2. ^a Oficina, afirmado); contrainteligencia interna (5. ^a Oficina, afirmado)
Guardia Real	Disputado: nominalmente una rama de las FAR; una fuente cita control directo de la Casa Real; otra describe un cuerpo autónomo interno de las FAR	~6.000 (cifra de la era de 1999; no actualizada desde entonces)	No identificado en fuentes abiertas (comandante actual no confirmado; el comandante nombrado por una fuente lleva él mismo una señal de cita necesaria)	Protección personal del rey y la familia real; funciones de escolta ceremonial
Regiones militares / postura en el Sáhara Occidental	Mando territorial de la Zone Sud (Zona Sur); no se identificó una estructura de zona completa actual	Hasta ~100.000 efectivos en el teatro del Sáhara Occidental (cifra indicativa)	Históricamente Ahmed Dlimi como «Commandant de la Zone Sud» (1975-76, 1980-83); no se identificó ninguna designación de sucesor actual	Defensa territorial del Sáhara Occidental; guarnición del Muro/Berma marroquí

Las cifras recopiladas sobre el tamaño, el presupuesto y la combinación de proveedores de las FAR divergen marcadamente entre no dos sino tres corrientes de fuentes distintas, y esta divergencia es en sí misma analíticamente significativa y no un inconveniente a suavizar. Las fuentes en inglés dan 196.000 efectivos activos y un presupuesto de defensa de 2026 de 15.700 millones de dólares (8,5 % del PIB), mientras que las fuentes en francés dan 235.000 efectivos en cinco ramas y un presupuesto de 2025 de 13.300 millones de dólares (4,28 % del PIB) [65, 77]. Una tercera cifra de personal, materialmente mayor, aparece en un relevo de una valoración de defensa centrada en España de un análisis al que esa información se refiere solo como GEOPOL 21: aproximadamente 400.000 efectivos activos más 250.000 reservistas, más del doble del recuento activo en inglés, frente a una fortaleza española reportada de aproximadamente 120.000 activos y 15.000 de reserva; el mismo relevo incluye un conjunto de afirmaciones sobre alcance de UAV, municiones merodeadoras y ataque de precisión (Bayraktar Akinci, TB2, Wing Loong, Harop/Harpy, cohetes de la familia EXTRA y ATACMS) que sus propios autores señalan como parcialmente no confirmadas y que se leen como alcances máximos publicitados y no como alcances de empleo demostrados [18]. En cuanto al presupuesto en concreto, una cifra distinta atribuida al IISS y relevada por un agregador de nivel inferior sitúa el gasto de defensa de Marruecos en 7.510 millones de dólares en 2025, elevándose a un récord reportado de 7.870 millones de dólares en 2026, con una proporción del PIB en torno al 4 %—esencialmente la mitad de la cifra en inglés de 15.700 millones de dólares/8,5 %, y, para el mismo año 2025, también muy por debajo de la cifra en francés de 13.300 millones de dólares [16]. Es probable que las cifras

reales actuales de personal y presupuesto se sitúen en algún punto dentro de este abanico ahora de tres y no de dos vías, y que las tres corrientes se basen en estimaciones desfasadas, parciales o metodológicamente distintas y no en una divulgación primaria del gobierno marroquí (confianza: baja), dado que Marruecos no publica un desglose presupuestario de defensa completamente detallado en ninguna fuente revisada; cualquier cifra de personal o presupuesto de las FAR de fuente única —en inglés, en francés o centrada en España— debe tratarse solo como indicativa hasta que se corrobore frente a una fuente autorizada de orden de batalla como el propio Military Balance del IISS, al que esta investigación no pudo acceder directamente pese a que una atribución al IISS aflora de segunda mano en una de las tres corrientes. Este conflicto de tres vías se señala aquí en lugar de resolverse, coherente con la práctica general de este informe de declarar las discrepancias explícitamente en lugar de elegir silenciosamente una cifra preferida.

En cuanto a proveedores, las fuentes en francés especifican un reparto de 2025 de Estados Unidos 60 %, Israel 24 % y Francia 10 %, ampliamente coherente con las adquisiciones recientes reportadas: helicópteros de ataque Apache AH-64E de Estados Unidos (24 encargados, 6 entregados en marzo de 2025), vehículos blindados Tata WhAP 8x8, y sistemas chinos de defensa aérea HQ-9 como diversificación de proveedor secundario [65]. Es muy probable que Marruecos siga priorizando una base de proveedores principal EE. UU.-Francia-Israel mientras añade sistemas chinos limitados para defensa aérea (confianza: moderada), un juicio que descansa en los porcentajes de proveedores de una única fuente terciaria que no pudo cotejarse con una base de datos independiente de transferencias de armamento en esta investigación —un elemento concreto de seguimiento para cualquier futura pasada de recopilación sobre este tema.

Arquitectura de mando de las FAR

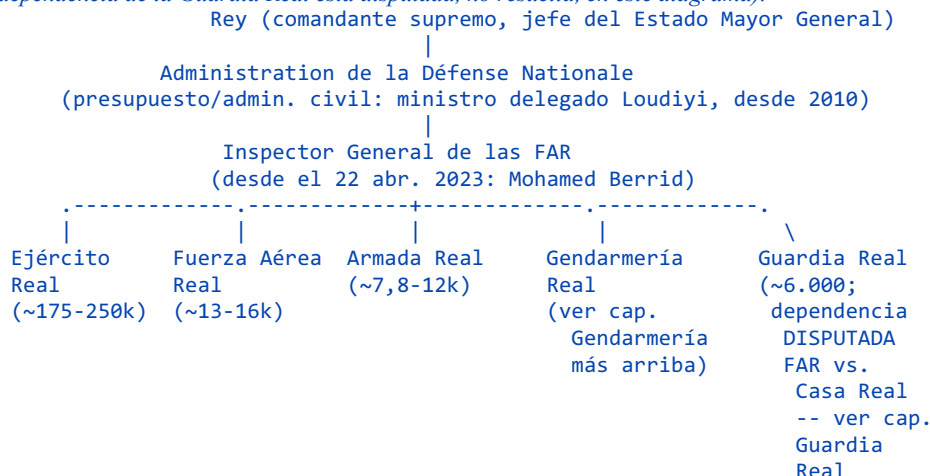
Las FAR comprenden cinco ramas bajo el rey como comandante supremo: el Ejército Real, la Fuerza Aérea Real, la Armada Real, la Gendarmería Real y la Guardia Real, con un teniente general que ejerce de inspector general —Mohamed Berrid ocupa este puesto desde el 22 de abril de 2023— actuando como el oficial uniformado de mayor rango bajo el rey [65, 77]. La sede de las FAR se sitúa en la Rue Farhat Hachad de Rabat [65]. Las estimaciones de personal a nivel de rama divergen entre las dos fuentes terciarias recopiladas —Ejército 175.000-250.000; Fuerza Aérea 13.000-16.000; Armada 7.800-12.000— y existe una posibilidad prácticamente equivalente de que las cifras más altas en francés reflejen la fortaleza nominal o sobre el papel, incluidos los reservistas, mientras que las cifras en inglés reflejen solo la fortaleza activa (confianza: baja), una reconciliación plausible pero no confirmada que una fuente de orden de batalla más autorizada necesitaría zanjar.

La Gendarmería Real, perfilada más arriba, ostenta pleno estatus militar dentro de esta arquitectura, establecida por el Dahir n.º 1-57-079 del 29 de abril de 1957 con un Dahir n.º 1-57-280 de marco operativo posterior, del 14 de enero de 1958, que presuntamente sigue siendo su base legal fundacional, y responde de forma singular ante ministerios civiles para conjuntos de misiones específicos —funciones de policía judicial ante el Ministerio de Justicia, funciones de policía administrativa ante el Ministerio del Interior— incluso manteniendo su estatus militar y su subordinación a la cadena de las FAR a través del secretario general de la Administración de Defensa [64]. En cuanto a la organización formal en regiones militares en un sentido más amplio, esta investigación no localizó ninguna lista actual de las régions militaires de las FAR en ninguna fuente revisada. El único anclaje histórico concreto identificado es el título de Ahmed Dlimi, Commandant de la Zone Sud (comandante de la Zona Sur), que ocupó dos veces —noviembre de 1975-mayo de 1976 y marzo de 1980-enero de 1983— mientras dirigía las operaciones de las FAR contra el Frente Polisario tras la Marcha Verde de 1975 [78].

Es improbable que la Zone Sud sobreviva hoy como la designación operativa para el mando de las FAR orientado al Sáhara Occidental, dadas las décadas de reorganización transcurridas (confianza:

baja), pero no se identificó en esta investigación ninguna designación de sucesor actual, y esto se registra como una carencia estructural explícita y no se resuelve por inferencia. La figura siguiente presenta la arquitectura de mando de las FAR en la forma en que puede afirmarse con confianza, dejando la línea de dependencia precisa de la Guardia Real marcada como disputada en lugar de forzar una resolución que las fuentes no respaldan; esa contradicción se examina en detalle más abajo en *Guardia Real*.

Figura 6. Arquitectura de mando de las FAR, en la medida en que las fuentes abiertas permiten afirmarla con confianza (la línea de dependencia de la Guardia Real está disputada, no resuelta, en este diagrama).



La principal fortaleza documentada de las FAR, en esta arquitectura, es una cúspide de mando clara y consistente —el rey como comandante supremo, un inspector general como oficial uniformado de mayor rango, y un ministro delegado civil que se ocupa de la administración sin un ministro de defensa electo— corroborada en todas las fuentes revisadas. Su principal limitación es la misma ya señalada para las cifras de personal y presupuesto: la ausencia casi total de un documento actual y autorizado de orden de batalla o de mando territorial de las FAR, lo que deja la estructura de regiones militares, la supervivencia institucional actual de la Zone Sud, y las cifras precisas de fortaleza por rama, todas descansando en fuentes terciarias con cifras materialmente distintas. La carencia de confianza e inteligencia más clara de esta sección es la propia estructura de mando territorial actual, sobre la que esta investigación no encontró nada más reciente que el título de Dlimi de la Zone Sud de los años setenta y ochenta. Una revisión distinta, llevada a cabo de forma independiente, de la postura naval de Marruecos, su presencia en el Estrecho de Gibraltar y su compromiso con el Diálogo Mediterráneo de la OTAN, realizada el 10 de septiembre de 2026, corrobora en lugar de cerrar esta misma carencia: tampoco localizó ningún orden de batalla naval buque por buque, ningún detalle de patrones de patrulla ni actividad de ejercicios bilaterales o por canal de la OTAN para la ventana de referencia, más allá de una mención escueta de las fragatas FREMM como línea de modernización. Esta convergencia entre dos pasadas de investigación independientes eleva la confianza (confianza: alta) en que la ausencia de detalle de fuentes abiertas sobre el dominio naval y la cooperación con la OTAN es una carencia estructural de visibilidad genuina y no un artefacto de una única ronda de recopilación.



Figura 7. La insignia de las FAR, en uso continuo en los artículos de Wikipedia sobre las FAR desde 2008.

La insignia es un pequeño escudo ovalado rematado por una corona real, que contiene una estrella de cinco puntas dentro de un campo circular bordeado por líneas radiantes, flanqueada por breves fragmentos de texto árabe [79]. El archivo ha estado en uso continuo en muchas ediciones lingüísticas de los artículos de Wikipedia sobre las FAR durante casi dos décadas, lo que respalda, sin una cita primaria explícita en el registro del archivo, que se trata de una reproducción estable y ampliamente reconocida de la insignia real de las FAR y no de una invención puntual; no obstante, se trata de una reproducción alojada en Wikipedia y no de un archivo publicado directamente por la Administration de la Défense Nationale de Marruecos. No se localizó en las fuentes revisadas ningún documento oficial de las FAR que explique los elementos heráldicos específicos de la insignia; la corona y la estrella son coherentes con el vocabulario general de insignias estatales/reales marroquíes señalado para los emblemas de las Fuerzas Auxiliares y la Guardia Real en otras partes de este informe [79].

Oficinas 2.^a y 5.^a

Esta investigación no encontró ninguna fuente, a ningún nivel de fiabilidad, que nombre, describa el mandato o perfile la dirección actual de una Deuxième Bureau (2.^a Oficina) o Cinquième Bureau (5.^a Oficina) militar marroquí. Esta ausencia se comprobó de forma deliberada y no se asumió: se verificaron específicamente los perfiles más detallados disponibles de los dos servicios de inteligencia civiles sucesores de Marruecos —la DGST, examinada en un capítulo anterior, y la DGED— para comprobar si alguno de los dos remonta su linaje a una oficina militar identificada, y ninguno lo hace en el material obtenido [80, 81]. El propio relato fundacional de la DGED afirma únicamente que se creó en 1973, en el contexto de la reorganización de los servicios de seguridad marroquíes tras los intentos de golpe de principios de los años setenta, sucediendo a estructuras anteriores no identificadas de inteligencia exterior, con Ahmed Dlimi como su primer director de 1973 a 1983 [81]. Es muy probable que este silencio refleje una característica genuina y estructural de baja visibilidad de estas oficinas en el registro de fuentes abiertas en general, y no simplemente una limitación de esta pasada de investigación en particular (confianza: moderada), dado que dos compilaciones terciarias redactadas de forma independiente y centradas en las dos instituciones sucesoras más plausibles omiten el tema por completo en lugar de discrepar sobre él.

Lo que puede afirmarse es adyacente y circunstancial, y no directo: Dlimi sirvió bajo Mohamed Oufkir en los servicios de seguridad marroquíes antes de su mando en el Sáhara Occidental de 1975, y ambos hombres están bien documentados en la literatura histórica general como figuras centrales de la represión vinculada al ejército y el trabajo de inteligencia de la era de Hassan II, sin que esta investigación localizara una fuente que vincule explícitamente a ninguno de los dos con una oficina que lleve la designación 2.^a o 5.^a [78]. Los analistas que se basen en este informe deben

tratar cualquier afirmación sobre el mandato actual, el personal o la relación con la DGST/DGED de las Oficinas 2.^a/5.^a como efectivamente carente de fuente a partir del material abierto recopilado hasta la fecha, y deben señalarlo explícitamente en lugar de rellenar la carencia con inferencias disfrazadas de hecho. Esta es una de las ilustraciones más claras, en todo este informe, de una carencia declarada y no inferida: es muy probable que la carencia en sí sea real, con independencia de cualquier juicio sobre la existencia o función actual real de las oficinas, que este informe no puede valorar (confianza: alta en que el silencio es genuino; no se ofrece confianza alguna sobre la actividad sustantiva actual de las oficinas, que sigue siendo completamente inevaluable a partir de las fuentes revisadas).

Guardia Real

La misión central de la Guardia Real es la protección del rey y los palacios reales, complementada por un papel ceremonial en el que unidades de caballería escoltan al rey y aparecen en actos de Estado y durante visitas de jefes de Estado extranjeros [82]. Su linaje se remonta, según una fuente, a la Garde Noire, un cuerpo de soldados de origen subsahariano formado a finales del siglo XVIII bajo el sultán Mulay Ismail, reorganizado en su forma actual con la independencia en 1956 y abierto desde entonces a marroquíes de todos los orígenes étnicos [82]. La fortaleza de personal reportada es de aproximadamente 6.000, referenciada a una cita de prensa de la era de 1999 incrustada en la fuente terciaria y no a un recuento actual; existe una posibilidad prácticamente equivalente de que esta cifra siga siendo exacta hoy dado el vacío de más de veinticinco años (confianza: baja), y no se localizó en esta investigación ninguna cifra más reciente.

La relación de mando exacta de la Guardia Real con las FAR es una cuestión genuinamente abierta y no un hecho zanjado, y este informe deliberadamente no elige una única versión para presentarla como cierta. Tres fuentes recopiladas ofrecen tres encuadres distintos: una enumera a la Guardia Real simplemente como una de las cinco ramas de las FAR sin más matización [77]; una segunda afirma que la Guardia permanece bajo el control directo del Ministerio de la Casa Real pese a su integración formal dentro del Ejército [65]; y una tercera la describe como un corps autonome des Forces armées royales —autónomo dentro de las FAR, y no bajo un mando de rama de las FAR sencillo ni bajo un ministerio externo [82]. Es probable que alguna versión del tercer encuadre esté más cerca de la realidad —un mando interno a las FAR pero funcionalmente separado que en la práctica responde de forma más directa a Palacio que a la cadena ordinaria del Estado Mayor de las FAR— dado el patrón en el diseño del sector de seguridad marroquí de mantener a las fuerzas próximas a Palacio bajo control real directo y no institucional (confianza: baja), pero esto es una inferencia a partir de un patrón estructural y no una fuente que resuelva directamente la contradicción, y el comandante actual nombrado en una fuente lleva él mismo la propia señal de cita necesaria de esa fuente, lo que significa que la dirección actual de la Guardia Real debe tratarse como no confirmada [82].



Figura 8. El emblema de la Guardia Real, procedente de un anuncio oficial de reclutamiento de la Garde Royale.

La insignia dorada presenta una corona real en su centro flanqueada por dos gallardetes rojos, cada uno con una estrella verde de seis puntas, distinta de la estrella de cinco puntas usada por los demás servicios perfilados en este informe; detrás de la corona hay un motivo de rayos de sol rematado por una pequeña estrella de cinco puntas, con la parte inferior bordeada por frondas de estilo espiga de trigo o laurel y una cinta en la base que reza La Guardia Real [83]. No se localizó en las fuentes revisadas ningún documento oficial de la Guardia Real que explique el significado heráldico específico de la corona, las banderas con hexagramas, los rayos de sol o las frondas; la descripción anterior es un inventario visual factual y no una explicación simbólica fundamentada en fuentes.

Regiones militares y postura en el Sáhara Occidental

La posición militar de Marruecos en el Sáhara Occidental descansa físicamente en el Muro marroquí (la Berma), un sistema de fortificación de arena y piedra construido en seis fases entre agosto de 1980 y abril de 1987 con la asistencia reportada de asesores franceses, israelíes, sudafricanos y portugueses, cuya línea principal recorre unos 2.500 km desde Guerguerat hacia el norte a través del territorio, flanqueada por lo que se describe como el campo de minas continuo más largo del mundo [84]. Es muy probable que la Berma siga siendo el ancla estructural de la postura militar marroquí en el Sáhara Occidental, esencialmente sin cambios en su concepto desde 1987 (confianza: moderada), dado que toda fuente que describe la actividad actual de la MINURSO o de Marruecos en el territorio sigue haciendo referencia a la Berma como la línea divisoria operativa, aunque las cifras concretas reportadas de densidad de tropas y alcance de radar —puestos de observación aproximadamente cada 5 km con 35-40 efectivos cada uno, cobertura de radar solapada a 60-80 km— proceden de una única fuente terciaria y no se corroboraron de forma independiente en esta investigación [84].

Figura 9. El Muro/Berma marroquí: sectores de construcción y localidades encerradas reportados (cifras de fuente única y señaladas como no corroboradas; ver texto).

ADMINISTRADO POR MARRUECOS (oeste) ESTE	LA BERMA / MURO MARROQUÍ	ZONA DE AMORTIGUACIÓN /
El Aaiún, Smara, Bu Craa yacimientos de fosfatos Tinduf	~2.500 km línea principal; construida en seis fases, ago. 1980 - abr. 1987	territorio administrado desde los campamentos de
Localidades reportadas encerradas/flanqueadas, de norte a sur (fuente terciaria única, no corroborada -- tratar solo como indicativo): El Aaiún / Smara / Bu Craa -- Amgala -- Ydiriya / Hauza -- Mahbes / Farsia -- Guelta Zemmur / Bir Anzarán / Dajla -- Auserd / Tichla / Bir Ganduz		
Puestos de observación cada ~5 km (35-40 efectivos cada uno); cobertura de radar reportada a 60-80 km más allá del muro (fuente única, no confirmado)		
Paso de Guerguerat (extremo sur) -- alto el fuego funcionalmente roto desde nov. 2020		

Políticamente, la disputa subyacente sigue formalmente viva y sin resolver en la vía negociadora que enmarca el despliegue de las FAR. La Resolución 2797 del Consejo de Seguridad de la ONU, adoptada el 31 de octubre de 2025 por 11 votos a favor con tres abstenciones (China, Pakistán, Rusia) y Argelia sin votar por ser entonces miembro del Consejo, prorrogó el mandato de la MINURSO hasta el 31 de octubre de 2026 y respaldó la propuesta de autonomía de Marruecos como base para las negociaciones, reafirmando al mismo tiempo el derecho del pueblo saharaui a la autodeterminación —manteniendo ambos elementos en tensión y no resolviéndose a favor de ninguna de las partes [85]. El embajador de Marruecos ante la ONU en Ginebra ha declarado desde entonces ante la 63.^a sesión del Consejo de Derechos Humanos que 40 países respaldan la autonomía bajo soberanía marroquí en virtud de esta resolución, una afirmación coherente con la propia resolución, ampliamente corroborada, pero reportada en esta investigación solo a través de un único medio marroquí [86]. Es probable que Rabat siga apoyándose en la Resolución 2797 como palanca diplomática hasta 2026 (confianza: moderada), dado el patrón de la declaración de

Ginebra de septiembre de 2026 apoyándose directamente en el texto de la resolución de octubre de 2025.

La propia MINURSO sigue funcionando como el mecanismo de vigilancia y acción contra minas a lo largo de esta línea, con el mayor general Jawwad Ahmed, de Pakistán, habiendo asumido como comandante de la fuerza en sustitución del general Fakhru Ahsen a finales de julio de 2026, en un contexto que el propio sitio de la misión enmarca en torno a las hostilidades reanudadas en noviembre de 2020 —es decir, el propio encuadre de la MINURSO trata el alto el fuego original de 1991 como funcionalmente roto desde esa fecha, aunque la misión persista [76]. Por separado, un diario argelino independiente informó de que la Asamblea General de la ONU adoptó una resolución Corregir el Mapa el 4 de septiembre de 2026 por 164 votos a uno, sustituyendo la proyección de Mercator por una proyección Equal Earth que representa al Sáhara Occidental como una entidad distinta de 266.000 km² con El Aaiún como capital, y afirmó que el propio Marruecos votó a favor sin reservas [87, 88]. Se trata de una afirmación de fuente única y no verificada procedente de un medio editorialmente proafiliado a la causa saharauí, no corroborada frente a ningún registro primario de la ONU ni relato de la prensa marroquí en esta investigación, y no debe tratarse como confirmada —de ser exacta, sin embargo, sería un desarrollo notable y casi con toda certeza infraanalizado que merecería seguimiento prioritario (confianza: baja a la espera de corroboración). Mapa el 4 de septiembre de 2026 por 164 votos a uno, sustituyendo la proyección de Mercator por una proyección Equal Earth que representa al Sáhara Occidental como una entidad distinta de 266.000 km² con El Aaiún como capital, y afirmó que el propio Marruecos votó a favor sin reservas [87, 88]. Se trata de una afirmación de fuente única y no verificada procedente de un medio editorialmente proafiliado a la causa saharauí, no corroborada frente a ningún registro primario de la ONU ni relato de la prensa marroquí en esta investigación, y no debe tratarse como confirmada —de ser exacta, sin embargo, sería un desarrollo notable y casi con toda certeza infraanalizado que merecería seguimiento prioritario (confianza: baja a la espera de corroboración).

Sobre el terreno, un medio marroquí informó el 8 de septiembre de 2026 de que un dron de las FAR atacó dos vehículos que transportaban a presuntos mineros de oro procedentes de los campamentos de Tinduf que habían cruzado a la zona de amortiguación, atribuyendo los detalles de víctimas y daños a fuentes mauritanas no identificadas, y se afirmó que las autoridades mauritanas habían advertido repetidamente a los ciudadanos contra entrar en la zona [89]. Es probable que esto refleje un patrón de aplicación genuino y recurrente y no un incidente aislado, dado el propio encuadre de la fuente respecto a eventos similares anteriores (confianza: baja), dado que el reportaje descansa en el relevo por un único medio marroquí de fuentes gubernamentales extranjeras no identificadas sin corroboración independiente mauritana, del Polisario o argelina localizada —pero se trata de un dato concreto y fechado que demuestra el uso actual por las FAR de drones armados para hacer cumplir la zona de amortiguación, una capacidad no evidenciada en el material más antiguo sobre el diseño original de la Berma de los años ochenta.

Otros actores relevantes

Alrededor de las cuatro instituciones perfiladas más arriba se sitúa un aparato más amplio del Ministerio del Interior y un pequeño conjunto de organismos adyacentes que dan forma a la práctica de seguridad interna marroquí sin ser, por derecho propio, servicios de orden público o de inteligencia. El Ministerio, dirigido por Abdelouafi Laftit desde 2017, alberga una Secretaría General; la DGSN y la Inspección General de las Fuerzas Auxiliares, ambas perfiladas más arriba; una Inspección General de la Administración Territorial que supervisa el sistema de walis/gobernadores; una Dirección General de Colectividades Territoriales; una Dirección General

de Protección Civil; y direcciones especializadas de recursos humanos, asuntos jurídicos, asuntos rurales y gestión de riesgos naturales [90]. Un organismo de coordinación más acotado, centrado en catástrofes y emergencias, se sitúa dentro de este mismo ministerio: el Centre de Veille et de Coordination (CVC), establecido en 2008 por directiva del rey Mohamed VI para coordinar la respuesta a catástrofes entre la DGSN, la Protección Civil y la Gendarmería Real [90]. Ninguna fuente localizada indica si el mandato del CVC se extiende a la coordinación rutinaria de inteligencia de seguridad, frente a la gestión de catástrofes específicamente; es probable (confianza: baja) que el CVC sea funcionalmente distinto de, y más acotado que, el Conseil Supérieur de Sécurité constitucional examinado más abajo en *Coordinación y supervisión*, aunque esto se infiere del propósito fundacional declarado del CVC y no de una exclusión directamente documentada.

La DGST, perfilada en un capítulo anterior como institución matriz del BCIJ, lleva consigo un historial de autoridad legal previo al BCIJ directamente relevante como trasfondo aquí: un informe de 2004 de Human Rights Watch —utilizado estrictamente como línea de base histórica previa a 2015, no como evidencia de la práctica actual— documentó que la DST/DGST no estaba autorizada por ley para detener, retener o interrogar a personas, y registró abusos sistemáticos de detención posteriores al atentado de 2003, incluidos arrestos sin orden judicial y detención incomunicada prolongada [91]. Es probable que la creación del BCIJ en 2015 tuviera por objeto, al menos en parte, situar la investigación de contraterrorismo alimentada por la DGST sobre una base de policía judicial más defendible que la que permitía el propio estatus legal previo a 2015 de la DGST (confianza: moderada), dado el vínculo temporal y legal directo entre la ley posterior al atentado de Marrakech de 2011 y la fundación de la oficina documentada más arriba [47].

Los walis y gobernadores —funcionarios del Ministerio del Interior nombrados directamente por el rey para encabezar cada wilaya— reaparecen como la contraparte civil-administrativa nominal hacia la que se orientan formalmente tanto la estructura regional de la DGSN como el mandato de las Fuerzas Auxiliares, y sin embargo ninguna fuente de esta investigación documenta el protocolo operativo específico mediante el cual los walis asignan tareas o coordinan con los directores prefectorales de la DGSN, los mandos regionales de la Gendarmería o las inspecciones de zona de las Fuerzas Auxiliares [51]. Esta es una de las carencias estructurales más trascendentes de este informe, dado que significa que la mecánica práctica del sistema de coordinación de seguridad territorial de Marruecos, a diferencia de su jerarquía administrativa formal, sigue sin verificarse.

La Fiscalía General (parquet) aparece repetidamente a lo largo de esta investigación como la autoridad de supervisión judicial tanto para el trabajo de casos de contraterrorismo del BCIJ como para las investigaciones penales de la Gendarmería Real, incluida la investigación posterior al ataque de Lqliaa y los casos de corrupción de Beni Mellal y El Borouj, lo que indica que la supervisión de la fiscalía, y no ningún organismo dedicado de supervisión del sector de seguridad, es el control más consistentemente documentado sobre la conducta operativa en las instituciones perfiladas en este capítulo [68, 69, 70].

En el lado exterior, la Policía Nacional española y su Comisaría General de Información (CNP), y el BND alemán, son los dos servicios homólogos extranjeros identificados de forma más concreta, colaborando respectivamente con la DGSN en la interdicción de delincuencia organizada y con la cadena DGST/BCIJ en el enlace de contraterrorismo [47, 57, 62], mientras que la Oficina Central Nacional de INTERPOL con sede en Rabat sigue siendo el único canal multilateral que abarca todo el sistema desde 1957 [56].

El Institut Royal des Études Stratégiques (IRES), un organismo con sede en Rabat creado por dahir real con una relación de dependencia directa ante la monarquía, completa esta sección como un actor de análisis estratégico próximo a Palacio y no como un organismo de seguridad operativo: su misión declarada es contribuir a iluminar la toma de decisiones estratégicas mediante análisis encargados por el rey y una vigilancia estratégica continua de los ámbitos críticos nacional e

internacionalmente, que abarcan la geopolítica, la defensa y las políticas públicas [92]. El IRES no otorga títulos académicos y se trata aquí como un actor adyacente a, y no un componente de, la arquitectura formal de coordinación de seguridad de Marruecos.

Empresas privadas

De esta investigación emergen tres relaciones distintas y cronológicamente solapadas con proveedores extranjeros de tecnología de vigilancia, siendo la mejor evidenciada el software espía Pegasus de NSO Group. La información de prensa atribuye el uso marroquí principal de Pegasus a la DGST, y específicamente a su departamento de internet y operaciones, desde 2017 en adelante, corroborado de forma independiente por el Security Lab de Amnistía Internacional, que documentó la infección u objetivo con Pegasus de dos figuras marroquíes identificadas de la sociedad civil —el activista Maati Monjib (noviembre de 2017-julio de 2019) y el periodista Omar Radi (febrero de 2019-enero de 2020)— mediante análisis forense de dispositivos y no mera afirmación [93, 94]. Dada esta convergencia de atribución de un medio identificado y confirmación forense independiente, es muy probable que la DGST haya operado Pegasus contra objetivos de la sociedad civil interna desde al menos 2017 (confianza: alta), un juicio que el capítulo de este informe sobre la *comunidad de inteligencia* examina más a fondo junto con la cuestión de atribución DGED frente a DGST para el uso exterior de Pegasus. Un hallazgo técnico anterior de Citizen Lab incide directamente en qué redes del sector privado transportaron esta actividad: el mismo informe *Hide and Seek* de 2018, que catalogó por primera vez la huella global de Pegasus, geolocalizó a un presunto operador marroquí de Pegasus, con etiqueta interna ATLAS, en infraestructura de las redes de Maroc Telecom y Orange Maroc mediante sondeo de caché DNS y huella digital TLS desde agosto de 2017, un método que los propios autores del informe describen como una guía para futuras investigaciones y no como evidencia irrefutable [30]. Dado que Maroc Telecom es a su vez mayoritariamente de propiedad extranjera (Etisalat, por e&, 53 %, con el Estado marroquí manteniendo aproximadamente un 22 %) y Orange Maroc está cerca de ser mayoritariamente propiedad de la francesa Orange S.A. (49 %) [95, 96], este hallazgo indica que la infraestructura del presunto operador de la DGST se asentaba en redes de telecomunicaciones privadas y parcialmente de propiedad extranjera y no en infraestructura estatal dedicada, un locus distinto tanto de la infraestructura de Circles vinculada al BCIJ/las Fuerzas Auxiliares como de cualquier sistema propiamente operado por la DGST (confianza: baja específicamente sobre el vínculo ATLAS-DGST, dado que el propio informe trata esto como una pista de investigación y no como una atribución confirmada).

Una segunda relación con un proveedor, técnicamente distinta, implica a Circles, una empresa israelí/chipriota afiliada a NSO Group por un historial de propiedad compartido, pero que vende explotación del sistema de señalización SS7 para la geolocalización telefónica y la interceptación de llamadas/SMS, en lugar de la cadena de exploits en el propio dispositivo de NSO. El informe *Running in Circles* de Citizen Lab de diciembre de 2020, basado en un escaneo de toda internet en busca de una firma de cortafuegos distintiva, sitúa la infraestructura de despliegue de Circles en Marruecos en la misma subred que varios sitios web del BCIJ y la misma subred que el sitio web de las Forces Auxiliares —ambas entidades bajo el Ministerio del Interior— con actividad documentada desde marzo de 2018 hasta la publicación del informe en diciembre de 2020 [97]. Dado que este hallazgo descansa en metodología técnica divulgada y no en una afirmación no verificada, es probable que el Ministerio del Interior, a través de infraestructura vinculada al BCIJ/las Fuerzas Auxiliares, aloje u opere el despliegue de Circles en Marruecos (confianza: moderada) —un locus institucional materialmente distinto del hallazgo centrado en la DGST sobre Pegasus más arriba, lo que sugiere que la capacidad de vigilancia con proveedores extranjeros de Marruecos no se concentra en un único organismo.

Una tercera relación con un proveedor, más antigua y no israelí, está documentada solo a un nivel de fiabilidad bajo: la filtración de correos de Hacking Team de 2015, tal como la sintetiza una fuente terciaria y no como se verificó frente al archivo primario de la filtración, enumera a un cliente marroquí codificado como CSDN, sector Inteligencia, con un primer contrato fechado en 2009, tarifas de mantenimiento anuales de 140.000 € y unos ingresos por contrato identificados de 1.936.050 € en total [98]. Esto convertiría a Marruecos en uno de los clientes de más larga trayectoria de Hacking Team en Oriente Medio/África, anterior tanto a la relación con NSO como a la de Circles, pero la confianza en las cifras concretas es baja dada la fuente terciaria única; el patrón subyacente —que los servicios de inteligencia de Marruecos han utilizado al menos tres proveedores extranjeros distintos de intrusión/vigilancia de tres orígenes nacionales desde 2009— se valora, no obstante, como probable (confianza: moderada), dado que cada afirmación sobre un proveedor descansa en un hallazgo de fuente separada y no en una única cita repetida. Esta investigación buscó específicamente, y no encontró, ninguna relación documentada de cliente marroquí con QuaDream, Candiru, Intellexa/Cytrox, Verint, Nexa Technologies/Amesys o Rayzone Group; esto se registra como un hallazgo negativo declarado para esta pasada, no como evidencia de que tal relación no exista, dado que las relaciones con proveedores de vigilancia comercial son, por diseño, difíciles de detectar en ausencia de una filtración o un episodio de infección forense.

Por separado, la propia ley de ciberseguridad de Marruecos crea una capa distinta del sector privado, regulada internamente: la Ley 05-20 exige que cualquier operador de infraestructura crítica que subcontrate servicios de ciberseguridad utilice un proveedor cualificado por la DGSSI, y el régimen de cualificación de la DGSSI exige constitución marroquí para todos los proveedores cualificados y capital y nacionalidad mayoritariamente marroquíes entre los especialistas propuestos para los sistemas más sensibles [99]. El texto de aplicación específico para proveedores en la nube, el Décret n.º 2-24-921 del 22 de octubre de 2024, establece dos niveles de cualificación: el Nivel 1, que abarca el alojamiento, la gestión o la operación de sistemas de información sensibles, no lleva restricción de propiedad, mientras que el Nivel 2, que abarca el procesamiento, la operación o el almacenamiento de los propios datos sensibles, exige propiedad mayoritariamente marroquí, procesamiento y gestión exclusivamente en territorio nacional, y personal operativo de nacionalidad marroquí, con cualificaciones válidas hasta cinco años, autoridad de auditoría de la DGSSI en todo momento, y una transición de cumplimiento de 24 meses para los proveedores existentes que expira alrededor del 22 de octubre de 2026 [100]. Dado que ningún gran hiperescalador extranjero (Microsoft Azure, Google Cloud y Cloudflare confirman todos que no tienen presencia regional marroquí) opera actualmente infraestructura en territorio marroquí, es muy probable que la cualificación de Nivel 2 se cumpla en la práctica, si acaso, a través de empresas conjuntas constituidas en Marruecos o proveedores nacionales y no de filiales directas de hiperescaladores extranjeros para esa fecha límite (confianza: moderada, dado que tanto el texto del decreto como la línea de base de infraestructura están bien evidenciados, pero la respuesta práctica del mercado ante la fecha límite que se aproxima aún no se ha observado). Esto crea un panorama bifurcado del sector privado: proveedores extranjeros de vigilancia ofensiva no regulados o usados de forma encubierta por un lado, y una industria nacional de ciberseguridad y servicios en la nube restringida por nacionalidad y con licencia estatal por otro. La tabla siguiente presenta uno junto a otro los tres proveedores de tecnología de vigilancia identificados, dado que el lector debería poder ver de un vistazo que los tres hallazgos descansan en tres bases evidenciales distintas y no en una certeza uniforme.

Tabla 9. Tres relaciones con proveedores extranjeros de tecnología de vigilancia identificadas para Marruecos.

Proveedor	País de origen	Producto / técnica	Cliente/infraestructura marroquí identificado	Ventana de actividad	Base evidencial
-----------	----------------	--------------------	---	----------------------	-----------------

NSO Group (Pegasus)	Israel	Cadena de exploits en el dispositivo (software espía)	DGST, específicamente su departamento de internet y operaciones	2017-2021 (confirmación forense de dispositivo)	Atribución de prensa de un medio identificado más confirmación forense independiente (Amnistía Internacional)
Circles	Israel / Chipre	Explotación del sistema de señalización SS7 (geolocalización, interceptación de llamadas/SMS)	Infraestructura del Ministerio del Interior (misma subred que los sitios web del BCII y las Forces Auxiliaires)	Marzo 2018-diciembre 2020	Escaneo técnico de Citizen Lab a escala de toda internet (metodología divulgada)
Hacking Team	Italia	Software de intrusión Remote Control System	Cliente codificado «CSDN», sector «Inteligencia»	2009-2015 (fecha de la filtración)	Síntesis terciaria de los correos filtrados de 2015, no reverificada de forma independiente frente al archivo primario

Universidades

De las instituciones académicas marroquíes examinadas en esta investigación, solo una ofrece un currículo claramente conducente a titulación y específico de seguridad: la École Nationale Supérieure d'Informatique et d'Analyse des Systèmes (ENSIAS), una grande école pública de ingeniería fundada en 1992 y adscrita formalmente a la Université Mohammed V de Rabat, que imparte un itinerario de especialización dedicado en Sécurité des Systèmes d'Information y un Master Recherche en Sécurité des Systèmes et Services de investigación asociado [101]. Este es el hallazgo más directamente relevante para el requisito de una institución académica marroquí relacionada con la seguridad y los estudios cibernéticos, aunque en la fuente obtenida no se documentó ninguna asociación institucional entre la ENSIAS y la DGSSI u otro organismo estatal de ciberseguridad, lo que se registra como una carencia evidencial y no como una ausencia confirmada.

Se comprobaron específicamente otras dos universidades marroquíes destacadas en busca de un vínculo con la seguridad/inteligencia/ciberespacio, con resultados negativos. La Université Mohammed VI Polytechnique (UM6P), una universidad de investigación privada financiada por la Fundación OCP con sólidos programas de inteligencia artificial e informática y una notable presencia de campus en El Aaiún, Sáhara Occidental, no mostró ningún instituto específico de ciberseguridad ni asociación con organismos de defensa/seguridad gubernamentales documentados en la fuente examinada [102]. La Université Internationale de Rabat (UIR), la

primera universidad de colaboración público-privada de Marruecos, ofrece dobles titulaciones en ingeniería aeroespacial y automotriz con socios internacionales, pero tampoco mostró ningún programa de ciberseguridad ni asociación con organismos de defensa documentados [103]. Ambos hallazgos negativos son candidatos plausibles a un vínculo genuino —la UM6P dada su fortaleza en IA/informática y su financiación vinculada al Estado, la UIR dada la proximidad de su programa aeroespacial a la creciente base industrial de drones/defensa de Marruecos— pero ninguno está fundamentado en esta investigación, y es improbable, aunque no descartado, que cualquiera de las dos instituciones tenga una asociación no divulgada con un organismo de seguridad invisible para la revisión de fuentes abiertas (confianza: baja).

El Institut Royal des Études Stratégiques, perfilado más arriba como un actor de estudios estratégicos próximo a Palacio, no es explícitamente una universidad en el sentido de conceder titulaciones y se excluye del hallazgo central de esta sección por esa razón [92]. El propio sitio de la DGSSI hace referencia a un Master spécialisé en cybersécurité con un sexto ciclo de matriculación abierto en marzo de 2013, lo que implica una relación de formación que se remonta al menos a mediados de la década de 2000, pero el contenido obtenido no nombra a la universidad socia que lo imparte [104]; dos intentos de identificar una academia militar marroquí o un colegio de Estado Mayor/de guerra con un currículo documentado de estudios de seguridad o inteligencia no devolvieron ninguna página recuperable, una carencia abierta y sin resolver para futura investigación y no un hallazgo negativo, dado que tal institución es una candidata plausible que esta investigación no pudo confirmar ni descartar.

Delincuencia

El panorama de delincuencia organizada de Marruecos, según se evidencia en esta investigación, se centra en dos corredores de tráfico geográfica e institucionalmente distintos: una ruta de hachís consolidada que se mueve hacia el norte hacia España oculta en camiones de exportación agrícola, y una ruta emergente de cocaína marítima atlántica que discurre por la costa adyacente al Sáhara Occidental. La ruta de hachís se evidencia mediante una operación conjunta de octubre de 2025 de la DGSN y la Policía Nacional española que incautó más de 22 toneladas ocultas en convoyes de camiones frigoríficos de pimientos entre Marruecos y España, desencadenada por inteligencia de origen marroquí [57], mientras que la ruta de cocaína se evidencia mediante la interdicción de la Gendarmería Real de julio de 2026 de más de tres toneladas transferidas de buque a costa frente a Tarfaya [67]. Es probable que estas dos sustancias discurren ahora por canales institucionales y geográficos sustancialmente distintos —cooperación terrestre/de exportación agrícola DGSN-España para el hachís, interdicción marítima liderada por la Gendarmería para la cocaína— en lugar de a través de una única red de tráfico indiferenciada (confianza: moderada, basada en la separación institucional y geográfica consistente en los casos concretos de 2025-2026 revisados). El tráfico de migrantes reaparece a lo largo de esta investigación tanto como un tipo de delito independiente como uno que se solapa directamente con el narcotráfico en las mismas embarcaciones y redes. Una única interdicción en Sidi Ifni acusó a la misma embarcación y tripulación tanto de narcotráfico internacional como de migración marítima organizada, lo que evidencia un solapamiento de redes entre la logística del hachís y la infraestructura de tráfico de migrantes en la costa atlántica, aunque la cantidad concreta reportada para esa incautación se señala como casi con toda certeza un error de extracción y no debe tomarse como fiable [105]. Por separado, la interceptación por la Gendarmería Marítima Real de migrantes bangladesíes frente a M'diq demuestra que la clientela del tráfico de personas en la costa mediterránea de Marruecos no se limita a nacionales regionales del África subsahariana, lo que indica un mercado de facilitación del tráfico más amplio e internacional que opera a través del territorio marroquí de lo que sugeriría un encuadre puramente migratorio regional [66]. La crisis fronteriza de Ceuta de agosto de 2026 ilustra además cómo las autoridades marroquíes distinguen a los migrantes de los facilitadores a

efectos de enjuiciamiento: junto a unos 300 migrantes detenidos, 61 personas adicionales fueron acusadas por separado de incitación a la migración ilegal, un delito distinto de tráfico/organización [50].

La corrupción institucional es una vulnerabilidad documentada y recurrente que las redes de delincuencia organizada parecen capaces de explotar en el propio nivel de las fuerzas del orden: los dos casos independientes de narcocorrupción de la Gendarmería Real en Beni Mellal y El Borouj, analizados más arriba en *Gendarmería Real*, indican que las redes de tráfico han conseguido, en al menos dos ocasiones enjuiciadas por separado, cultivar con éxito protección desde dentro de las filas de la Gendarmería, en lugar de depender únicamente de la evasión [68, 69]. Por último, el caso del BCIJ de abril de 2026 muestra un patrón distinto en la frontera entre terrorismo y delincuencia organizada: una célula afiliada a Dáesh se dedicaba al robo ordinario, el hurto con fractura y el blanqueo de capitales bajo una justificación de legitimación ideológica del botín, lo que indica que al menos algunas redes ideológicamente motivadas en Marruecos se financian mediante delitos ordinarios de delincuencia organizada y no mediante financiación terrorista externa [61]. Es probable que esta mezcla de delincuencia ideológica y ordinaria sea una estrategia deliberada de reclutamiento y autofinanciación, y no una elección de encuadre aislada por parte de los fiscales (confianza: baja, dado que esto descansa en un único caso detallado en esta investigación). Una afirmación más amplia y políticamente cargada sobre la relación del Majzén con la delincuencia organizada reaparece en esta recopilación y se registra aquí estrictamente como un encuadre en disputa y no como un hallazgo evidenciado: los medios estatales argelinos (Algérie Presse Service) han caracterizado al Majzén marroquí como fomentando un entorno que permite regenerarse a la delincuencia organizada transnacional y como dando cobijo a fugitivos buscados por la justicia europea por cargos de narcotráfico y blanqueo de capitales, una afirmación sostenida en una única pieza de agencia estatal solo parcialmente accesible procedente de un gobierno rival con un interés evidente en deslegitimar a Rabat [20]. Un comentarista marroquí alineado con el establishment, por el contrario, define al Majzén como la red tradicional de autoridad centrada en la monarquía, a la que se atribuye continuidad histórica y no ningún papel de facilitación delictiva [19]. Ninguno de los dos encuadres se verifica de forma independiente frente al trabajo de casos concreto de hachís, cocaína y tráfico de migrantes de 2025-2026 detallado más arriba, y es improbable, aunque no descartado, que la caracterización de la APS refleje un patrón institucional documentado y no una deslegitimación retórica de un Estado rival (confianza: baja, dada la fuente única, sesgada y solo parcialmente accesible sobre esta afirmación concreta). La tabla siguiente presenta las operaciones documentadas de 2025-2026 en todas las instituciones perfiladas en este capítulo, dado que se trata de una enumeración natural y no de una narrativa en prosa.

Tabla 10. Operaciones documentadas de orden público y seguridad de 2025-2026, por fecha.

Fecha	Institución(es)	Operación / incidente	Resultado
Enero 2025	Gendarmería Real	Caso de encubrimiento de un capo de la droga en El Borouj/Beni Meskine	Detención ordenada de siete gendarmes
Marzo 2025	Gendarmería Real	Juicio por narcocorrupción de Beni Mellal	37 agentes juzgados; veredicto no reportado en las fuentes revisadas
Agosto 2025	DGSN	Interdicción marítima de Sidi Ifni	Embarcación de hachís y migración irregular interceptada (cantidad de la incautación)

			señalada como error de extracción)
Octubre 2025	DGSN; Policía Nacional española	Interdicción de hachís de Cádiz/Granada	Más de 22 toneladas incautadas, ocultas en convoyes de camiones frigoríficos de pimientos
Octubre 2025	Gendarmería Real (M'diq)	Intercepción de tráfico de migrantes bangladesíes	Embarcación neumática interceptada; 13 migrantes
Octubre 2025	Gendarmería Real	Ataque al puesto de Lqiaa (disturbios vinculados a Gen Z 212)	Tres muertos, ocho gendarmes heridos
Abril 2026	BCIJ / DGST	Célula afiliada a Dáesh (Kenitra, Casablanca, Dar El Gueddari, Sidi Taibi)	Célula de seis miembros desmantelada; patrón de autofinanciación de «legitimación del botín»
Julio 2026	Gendarmería Real	Interdicción atlántica de cocaína de Tarfaya	Más de tres toneladas incautadas, transferencia de buque a costa
Agosto 2026	DGSN; Gendarmería Real; Fuerzas Auxiliares	Cruce fronterizo masivo de Ceuta (15 de agosto)	~300 migrantes detenidos; 61 adicionalmente acusados de incitación a la migración ilegal
Agosto 2026	DGSN	Lanzamiento de la octava brigada regional de desactivación de explosivos de Agadir	Despliegue regional de unidades especializadas completado, extendiéndose al Sáhara Occidental a través de El Aaiún

Coordinación y supervisión

La coordinación formal del aparato de seguridad e inteligencia de Marruecos recae constitucionalmente en el rey y no en ninguna estructura civil interinstitucional. El artículo 53 de la Constitución de 2011 convierte al rey en jefe supremo de las Fuerzas Armadas Reales con potestad para nombrar cargos militares, y el artículo 54 crea el Conseil Supérieur de Sécurité (CSS) como el organismo de coordinación constitucionalmente designado del país para la estrategia de seguridad interna y externa, la gestión de crisis y la promoción de estándares de buena gobernanza en el ámbito de la seguridad [106, 107]. El rey preside el CSS pero puede delegar la presidencia en el jefe de Gobierno para una agenda específica, y la composición del Consejo abarca al jefe de Gobierno, los presidentes de ambas cámaras parlamentarias, un representante de la autoridad

judicial, los ministros de Interior, Asuntos Exteriores, Justicia y Defensa Nacional, y altos responsables de seguridad y militares —una composición que integra formalmente la coordinación interpodere en la cúspide del sistema de seguridad, sea cual sea el ritmo de funcionamiento práctico que resulte tener el Consejo.

Ese texto constitucional guarda un silencio notorio sobre cualquier comité parlamentario dedicado de supervisión de seguridad o defensa comparable a las estructuras occidentales de supervisión de inteligencia: el único papel parlamentario próximo a la defensa especificado es el requisito del artículo 99 de que una declaración de guerra, decidida en el Consejo de Ministros, sea comunicada por el rey al Parlamento, y la reserva del artículo 49 de los proyectos de ley de declaración de guerra y del ámbito militar a la deliberación del Consejo de Ministros [106]. Es muy probable que el orden constitucional de Marruecos no proporcione al Parlamento un mecanismo permanente y con habilitación de seguridad de supervisión sobre los organismos de inteligencia y seguridad, como cuestión de diseño institucional y no como una convención no escrita pero funcionante (confianza: moderada), basándose en la ausencia de tal disposición en dos fuentes de texto constitucional obtenidas de forma independiente. La síntesis de Privacy International de la arquitectura legal de supervisión de vigilancia de Marruecos converge con ese silencio constitucional: afirma llanamente que se sabe poco sobre las leyes y reglamentos que regirían la autoridad del CSS, y documenta por separado que la Ley 85-13, que faculta a las comisiones parlamentarias de investigación, excluye del alcance de dichas comisiones los documentos de naturaleza secreta o que caigan bajo la defensa nacional [108]. Es muy probable que el Parlamento de Marruecos no posea ningún mecanismo operativo para revisar la inteligencia clasificada o la actividad de los organismos de seguridad (confianza: moderada-alta), un juicio que descansa en la convergencia del silencio constitucional y esta exclusión legal específica.

La supervisión judicial, y no parlamentaria, rige nominalmente la interceptación de comunicaciones: los artículos 108-116 del Code de Procédure Pénale exigen una orden escrita del primer presidente del Tribunal de Apelación, dirigida a un juez de instrucción o al fiscal de la Corona, limitada a cuatro meses y renovable una vez, con una excepción de ratificación judicial en 24 horas para casos de extrema urgencia [108]. El peso práctico de esta salvaguarda es dudoso por dos motivos independientes documentados en la misma fuente: Privacy International cita la falta de independencia del poder judicial como una preocupación constante entre las asociaciones profesionales de jueces marroquíes y las organizaciones de la sociedad civil, y señala por separado que un estatuto de 2011 (Ley 35-11) que otorga a los agentes de la DST/DGST el estatus de Officier de Police Judiciaire se aplica solo de forma limitada a los delitos concretos que el organismo está facultado para investigar, funcionando como una concesión de estatus de procedimiento penal y no como un mecanismo general de supervisión sobre la actividad de inteligencia más amplia del organismo [108]. Es probable que el régimen de órdenes de los artículos 108-116 del CPP limite más la interceptación ordinaria de procedimiento penal que la actividad de vigilancia propiamente de los servicios de inteligencia (confianza: moderada), dada esta distinción de alcance de estatus.

El hecho de coordinación individual más claro de toda la arquitectura de seguridad marroquí es la dirección simultánea por Abdellatif Hammouchi de la DGST, que dirige desde diciembre de 2005, y la DGSN, que dirige simultáneamente desde mayo de 2015, un arreglo que múltiples medios identificados de forma independiente tratan como un punto de fusión de facto entre el aparato de orden público y contraespionaje de Marruecos [46, 93]. Esta doble función se refuerza institucionalmente por la ubicación del BCIJ bajo la autoridad de la DGST como su brazo judicial, lo que significa que el producto de inteligencia, el trabajo de casos de policía judicial y el mando de la policía nacional convergen bajo un único titular [109]. El mecanismo constitucional que permite esta concentración es en sí mismo identificable y no meramente inferido: el artículo 49 sitúa el nombramiento de los jefes de las administraciones de seguridad interna y de los organismos

públicos estratégicos en el Consejo de Ministros presidido por el rey, a propuesta del jefe de Gobierno, lo que otorga al nombramiento y la permanencia dual continuados de Hammouchi una base constitucional textual directa y no una que descansa solo en la práctica administrativa [106, 107]. Es casi con toda certeza el mecanismo de coordinación individual más trascendente documentado en esta investigación (confianza: alta), dada la convergencia de la atribución de prensa independiente, el hallazgo estructural del BCIJ y esta potestad de nombramiento constitucional, aunque ninguna fuente localizada documenta ningún control formal sobre esta fusión más allá del informe ministerial ordinario al ministro del Interior.

El hallazgo forense de Amnistía Internacional sobre el objetivo con Pegasus de Maati Monjib y Omar Radi, analizado más arriba en *Empresas privadas*, es directamente relevante aquí porque ninguno de los dos objetivos era un sospechoso penal bajo investigación activa en el momento del objetivo, lo que significa que su vigilancia no puede explicarse como una aplicación del marco de orden judicial de los artículos 108-116 del CPP [94]. Es muy probable que esta y operaciones comparables de Pegasus contra figuras marroquíes de la sociedad civil se llevaran a cabo como actividad de los servicios de inteligencia completamente al margen del marco documentado de autorización judicial de Marruecos para la interceptación de comunicaciones (confianza: alta), dado que no se documenta ningún proceso de orden, remisión a juez de instrucción ni artefacto judicial comparable para ninguno de los dos objetivos en el informe forense obtenido ni en ninguna otra fuente revisada. Esto ilustra de forma concreta lo que significan en la práctica operativa los silencios constitucionales y legales analizados más arriba.

En cambio, la arquitectura de gobernanza específica de ciberseguridad de Marruecos está comparativamente bien codificada en texto legal primario, aunque en la práctica siga dominada por la DGSSI. La Ley 05-20 designa las infraestructuras críticas mediante lo que, en los propios términos del estatuto, es un mecanismo de doble llave establecido en el artículo 16: la propia autoridad gubernamental coordinadora de cada sector de actividad vital toma la decisión de designación, pero solo tras el dictamen consultivo obligatorio de la DGSSI, con la lista resultante mantenida en secreto y actualizada a intervalos no superiores a dos años [99]. La misma ley establece dos comités de gobernanza permanentes —un comité stratégique de la cybersécurité que fija la dirección estratégica nacional y evalúa el propio informe anual de actividad de la DGSSI, y un comité de gestion des crises et événements cybernétiques majeurs subordinado para la coordinación de crisis, facultado para obligar a los operadores de telecomunicaciones y proveedores de servicios a prestar asistencia técnica durante una crisis cibernética mayor declarada [99]. Es muy probable (confianza: alta, dado que esto descansa en texto legislativo primario) que la arquitectura de coordinación del dominio cibernético de Marruecos esté materialmente más documentada en términos de procedimiento que su arquitectura de coordinación de inteligencia humana y de señales, aunque ambas respondan nominalmente ante la misma estructura de seguridad de cúspide.

Esta asimetría no debe leerse como evidencia de que los comités de gobernanza de la DGSSI funcionen como se pretende en la práctica: ninguna fuente documenta con qué frecuencia se ha reunido realmente ninguno de los dos comités de ciberseguridad, lo que refleja la misma carencia ya señalada en torno al historial de reuniones del propio CSS. Tomado junto con el papel más acotado de coordinación de catástrofes del CVC documentado más arriba en *Otros actores relevantes*, el panorama de coordinación de Marruecos se caracteriza mejor como un conjunto de organismos paralelos y temáticamente acotados —el CSS para la estrategia de seguridad general, el CVC para la gestión de emergencias, los dos comités de la DGSSI para la ciberseguridad— y no como una única estructura de mando integrada, y existe una posibilidad prácticamente equivalente, según la evidencia de fuentes abiertas actual, de que esta fragmentación refleje una compartimentación deliberada y no una mera acumulación administrativa con el tiempo (confianza: baja). La tabla y la figura siguientes reúnen este aparato: la tabla enumera el mandato

y la línea de dependencia de cada organismo, y el diagrama distingue los vínculos constitucionales y legales de la fusión de doble función de Hammouchi, que es personal y no estructural.

Tabla 11. Los principales organismos formales de coordinación y supervisión de seguridad de Marruecos.

Organismo	Instrumento fundacional / fecha	Mandato declarado	Presidencia / línea de dependencia	Mecanismo de supervisión documentado
Conseil Supérieur de Sécurité (CSS)	Artículo 54, Constitución de 2011	Coordinación de la estrategia de seguridad interna y externa, gestión de crisis, promoción de la buena gobernanza	Rey (delegable en el jefe de Gobierno para una agenda específica)	Ninguno documentado; historial de reuniones real no confirmado
Centre de Veille et de Coordination (CVC)	2008, directiva real	Coordinación de la respuesta a catástrofes y emergencias entre la DGSN, la Protección Civil y la Gendarmería Real	Ministerio del Interior	Ninguno documentado más allá de su propósito fundacional declarado
Comité stratégique de la cybersécurité	Ley 05-20 (2020)	Fija la dirección estratégica nacional de ciberseguridad; evalúa el propio informe anual de actividad de la DGSSI	DGSSI	Frecuencia de reunión no documentada
Comité de gestion des crises et événements cybernétiques majeurs	Ley 05-20 (2020)	Coordinación de crisis; puede obligar a operadores de telecomunicaciones y proveedores de servicios a prestar asistencia técnica	DGSSI	Frecuencia de reunión no documentada
BCIJ (como punto de coordinación)	2015, ley posterior al atentado de Marrakech	Funciona como el «brazo judicial» de la DGST, convirtiendo la inteligencia en trabajo de casos de policía judicial	DGST, mediante la supervisión de la Fiscalía General del trabajo de casos	Supervisión de la fiscalía sobre el trabajo de casos; no se identificó ningún mecanismo de supervisión parlamentaria

Figura 10. El aparato de coordinación de seguridad de Marruecos, consolidado (los vínculos de fusión personal y la frecuencia de reunión no documentada se señalan explícitamente en lugar de suavizarse).

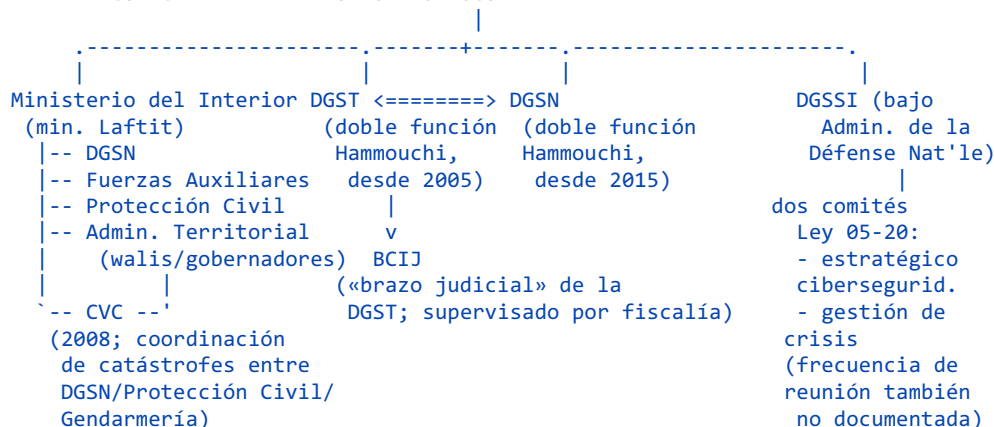
REY

(Art.53: jefe supremo de las FAR; Art.54: preside el CSS, delegable en el jefe de Gobierno para una agenda específica)

|

Conseil Supérieur de Sécurité (CSS)

miembros: jefe de Gobierno, ambos presidentes de Cámara, un representante de la autoridad judicial, los ministros de Interior/Asuntos Exteriores/Justicia/Defensa, altos cargos de seguridad y FAR --
FRECUENCIA REAL DE REUNIÓN NO DOCUMENTADA



Supervisión judicial de la interceptación: arts. 108-116 del CPP (orden del primer presidente del Tribunal de Apelación) -- peso práctico dudoso (preocupación por la independencia judicial; el estatus OPJ de la Ley 35-11 es limitado, no una supervisión general)

Esta investigación concluye declarando explícitamente, y no omitiendo silenciosamente, las carencias que quedan: la frecuencia real de reunión y el resultado práctico del CSS no están documentados en ninguna fuente localizada aquí; ninguna fuente nombra a la autoridad específica que ejecuta técnicamente una interceptación de comunicaciones autorizada judicialmente una vez emitida; no se identificó ningún órgano legislativo con habilitación de seguridad para revisar material clasificado en ningún estatuto o información marroquí; y la universidad socia que imparte el propio máster de ciberseguridad de la DGSSI sigue sin nombrarse. La arquitectura de coordinación y supervisión de seguridad de Marruecos es, según la evidencia reunida aquí, un ámbito genuinamente de baja transparencia, y estas carencias deben leerse como tales y no resolverse por inferencia.

Parte IV. El ecosistema cibernético marroquí

El ciberespacio marroquí

Los mercados marroquíes de internet y móvil están cerca de la saturación en número de suscripciones, aunque no en alcance de usuarios únicos. A finales de 2025 el Reino registraba más de 41 millones de suscripciones de internet frente a una población de unos 38 millones —una tasa de penetración nominal superior al 110 % que refleja el uso multidispositivo y multi-SIM y no una conectividad doméstica universal— junto a más de 58 millones de suscripciones móviles [110]. Es casi seguro que esto se interpreta mejor como evidencia de un mercado móvil maduro y competitivo que de un acceso doméstico uniforme (confianza: alta, dado que el propio informe del observatorio sectorial del primer trimestre de 2026 de la ANRT, una fuente regulatoria primaria, corrobora de forma independiente el mismo orden de magnitud directamente: una tasa de penetración de internet del 111,54 % y 3,22 millones de usuarios 5G atendidos por 8.400 emplazamientos 5G a fecha de ese informe [111], elevando la cifra terciaria anterior de una salvedad de fuente permanente a un dato directamente confirmado, aunque la propia página de la ANRT no desglosaba la cuota de mercado por operador). Tres operadores autorizados estructuran el mercado —Maroc Telecom, el operador histórico establecido, mayoritariamente propiedad de la emiratí e& desde 2013, examinado en su dimensión de propiedad más abajo en *Dependencias clave*; Orange Maroc, reportado ligeramente por delante de Maroc Telecom en suscripciones móviles a mediados de 2025; e Inwi— cada uno ofreciendo servicio móvil, de línea fija y de banda ancha [110]. La ANRT, el regulador sectorial, lanzó el 5G comercialmente el 7 de noviembre de 2025, alcanzando una cobertura poblacional estimada del 38 % a finales de 2025, junto a más de 1,4 millones de conexiones de fibra fija y aproximadamente el 30 % de la infraestructura fija desplegada mediante acuerdos de compartición de infraestructura entre operadores [110].

La evidencia más clara localizada de la creciente relevancia jurídica de la economía digital es indirecta y no estadística: la necesidad de la CNDP, de cara a las elecciones legislativas del 23 de septiembre de 2026, de imponer una obligación específica de etiquetado sobre el contenido político generado por IA [112], examinada en detalle más abajo en *Derecho y regulación*, es un requisito que no existiría en ausencia de un contexto de economía digital en el que las herramientas de IA generativa ya se usan en la comunicación política. Más allá de este único indicador, no se localizó ninguna fuente estadística primaria marroquí sobre la magnitud del comercio electrónico, la contribución de los servicios digitales al PIB o el tamaño de la economía de plataformas para este capítulo; esto se declara como una carencia de alcance explícita y no se disimula con una cifra inferida, y sigue siendo un objetivo natural para investigación dedicada del ámbito económico y no para el material centrado en lo cibernético del que se nutre este capítulo.

Esta base de conectividad, y la arquitectura legal e institucional que Marruecos ha construido para gobernarla y defenderla, se examinan a continuación por su orden: *Derecho y regulación* expone el marco legislativo; *Ciberseguridad defensiva y respuesta a incidentes* perfila a la DGSSI y maCERT; *Recopilación de inteligencia y vigilancia* aborda en detalle la cuestión de la vigilancia DGST/DGED; y *Ciberguerra militar, guerra electrónica y C4ISR* cierra este primer grupo de capítulos examinando —y, en gran medida, documentando la ausencia de información de fuentes abiertas sobre— una capacidad cibernética militar marroquí dedicada.

Derecho y regulación

El estatuto de ciberseguridad de Marruecos, la Ley 05-20, fue promulgado por el dahir n.º 1-20-69 del 4 de hiyya de 1441 (25 de julio de 2020), tal como confirma directamente el preámbulo de su propio decreto de aplicación [100]. Ese decreto, el n.º 2-24-921 del 22 de octubre de 2024, opera el artículo 25 de la Ley 05-20 exigiendo a las entidades de infraestructura vital (IIV) que utilicen únicamente un proveedor de nube cualificado por la DGSSI para sistemas y datos sensibles, bajo un esquema de cualificación de dos niveles: un Nivel 1, abierto a cualquier empresa registrada en Marruecos con recursos adecuados, que abarca el alojamiento o la operación de sistemas de información sensibles; y un Nivel 2 materialmente más estricto, que abarca el procesamiento o almacenamiento de los propios datos sensibles, que exige además propiedad mayoritariamente marroquí, procesamiento y gestión de servicios exclusivamente en territorio nacional, y personal operativo de nacionalidad marroquí [100]. Las decisiones de cualificación tienen una validez de hasta cinco años y se publican en el Bulletin Officiel, y la propia DGSSI audita a los proveedores cualificados en virtud del artículo 38 de la Ley 05-20 [100]; el propio artículo 18 del decreto otorga además a las entidades IIV que ya utilizaban servicios en la nube cuando entró en vigor una transición de cumplimiento de 24 meses, situando el cierre de esa transición hacia el 22 de octubre de 2026, unas seis semanas después del propio periodo de referencia de este capítulo, y su artículo 16 condiciona la salida del mercado de cualquier proveedor de Nivel 2 a garantías de recuperación de datos y borrado certificado para el cliente IIV saliente [100]. Es muy probable que la cualificación de Nivel 2 solo sea alcanzable por proveedores marroquíes nacionales y no por ningún hiperescalador global, examinado por su propia ausencia de Marruecos más abajo en *Dependencias clave* (confianza: moderada), dado que los requisitos de nacionalidad y territorialidad exclusiva en el propio texto del decreto equivalen a una exclusión categórica de las entidades bajo control extranjero de ese nivel y no meramente a un umbral de cumplimiento estricto; correspondientemente, es muy probable (WEP 80-95 %) que la cualificación de Nivel 2 se cumpla en la práctica, donde se cumpla, a través de proveedores nacionales o de empresas conjuntas y no de una filial directa de un hiperescalador extranjero (confianza: moderada, dado que tanto el texto del decreto como la línea de base de ausencia de nube están bien evidenciados, mientras que la respuesta real del mercado ante la fecha límite que se aproxima aún no se ha observado). La Ley 05-20 faculta por separado a la DGSSI, en virtud del propio artículo 28 del estatuto, para recopilar y analizar únicamente datos técnicos —el propio texto del artículo excluye «cualquier otra explotación»— de operadores de telecomunicaciones, proveedores de servicios de internet, proveedores de ciberseguridad y editores de plataformas, pero solo a efectos de prevenir y caracterizar amenazas cibernéticas [99]; se trata de una potestad de vigilancia acotada y ciberdefensiva sobre infraestructura privada, y no de una autoridad de interceptación de contenidos, y es distinta tanto en base legal como en alcance de la actividad de vigilancia a nivel de dispositivo de Pegasus examinada más abajo en *Recopilación de inteligencia y vigilancia*, que ninguna disposición legal revisada para este capítulo pretende autorizar, ya sea para la DGSSI o para la DGST/DGED.

El preámbulo del mismo decreto de 2024 confirma de forma independiente que el décret n.º 2-82-673 del 13 de enero de 1983, que organiza la Administration de la Défense Nationale, fue a su vez modificado por el décret n.º 2-11-509 del 21 de septiembre de 2011 [100]. Esto es coherente con, aunque no constituye en sí mismo una confirmación directa de fuente primaria de, la ubicación fundacional de la DGSSI bajo esa misma administración de defensa y no bajo un ministerio civil (confianza: moderada), dado que ninguna publicación de la DGSSI consultada para este capítulo declara explícitamente su propio decreto fundacional; el punto no obstante importa estructuralmente, dado que integra a la autoridad nacional de ciberseguridad de Marruecos dentro del estamento de defensa y no en un organismo regulador puramente civil, una diferencia estructural respecto a la mayoría de los modelos europeos de autoridad de ciberseguridad que merece señalarse explícitamente.

El estatuto de protección de datos de Marruecos, la Ley 09-08, rige la actividad regulatoria de la CNDP, y la evidencia más clara y actual de esa actividad es la guía de la comisión del 31 de agosto de 2026 para las elecciones legislativas del 23 de septiembre de 2026 [112, 113]. Esa guía exige a los partidos políticos notificar por adelantado a la CNDP las operaciones de tratamiento de datos en virtud del artículo 12, prohíbe la explotación de opiniones políticas sin consentimiento explícito en virtud del artículo 21, limita la conservación a la finalidad declarada en virtud del artículo 3, restringe la captación no solicitada en virtud del artículo 10 y —su elemento más novedoso respecto a la práctica anterior de la CNDP— exige que el contenido de campaña generado por IA se etiquete como tal, citando el artículo 447-2 del Código Penal de 2018 y los artículos 39, 51 y 53 de la Ley Orgánica n.º 53-25 [112]. Es muy probable que este requisito de etiquetado de IA sea una incorporación genuinamente nueva a las normas de comunicación electoral de Marruecos y no una reformulación de una guía anterior (confianza: moderada), inferido de la ausencia de cualquier comunicado electoral anterior de la CNDP de este tipo en el material revisado, y no de una comparación directa con la propia guía de un ciclo electoral anterior. Una salvedad de precisión, no de fondo: el propio comunicado de la CNDP confirma la existencia de la guía y su encuadre de «diez imperativos», pero los números de artículo concretos citados más arriba — artículo 447-2 del Código Penal, artículos 39, 51 y 53 de la Ley Orgánica 53-25— descansan en la propia caracterización de prensa de Le360/MAP de los textos subyacentes y no en una cita primaria de la CNDP o del Bulletin Officiel obtenida directamente [112], y deben leerse en consecuencia como plausibles en su validez pero no verificados de forma independiente en el texto. Dado que este es el primer ciclo electoral que opera bajo este requisito en absoluto, existe solo una posibilidad de prácticamente equivalente a probable (WEP 45-70 %) de que la aplicación por la propia CNDP durante la votación del 23 de septiembre de 2026 resulte ser ligera y reactiva ante denuncias en lugar de vigilada de forma proactiva (confianza: baja), una previsión que este informe formula explícitamente como una prueba de primera instancia genuinamente abierta sobre la independencia práctica de la CNDP, y no como una predicción que el material subyacente permita formular con mayor confianza. Esta norma electoral de etiquetado de IA no debe interpretarse como un movimiento hacia un marco general de gobernanza de la IA marroquí: no se localizó ningún estatuto o borrador específico de IA marroquí de ningún tipo para este capítulo, y el requisito de etiquetado es una norma acotada y específica del contexto electoral, vinculada a disposiciones existentes del Código Penal y del derecho electoral sobre la conducta de los candidatos, y no el primer pilar de un régimen regulatorio más amplio, una distinción declarada explícitamente y no dejada a la inferencia.

El régimen de homologación de la DGSSI, distinto del esquema de cualificación de proveedores en la nube anterior, exige que todo sistema de información sensible operado por una entidad IIV sea objeto de una homologación formal antes de su despliegue, en virtud del artículo 19 de la Ley 05-20 [114]. La homologación es un acto documentado y no meramente un control técnico: el propio responsable de la entidad IIV debe emitir una decisión que acredite haber comprendido la postura de seguridad del sistema y aceptar formalmente el riesgo residual que quede [114]. Esto sitúa la responsabilidad última de la postura de seguridad de un sistema de infraestructura vital en un responsable institucional identificado y no en la DGSSI como auditora, una decisión de diseño estructuralmente significativa que el material fuente declara con claridad pero no desarrolla más a nivel procedimental; los criterios de evaluación completos y el papel de la autoridad de homologación se limitan a una guía descargable no examinada en su totalidad para este capítulo, una carencia de contenido específica y nombrable.

El marco de declaración de incidentes de ciberseguridad de Marruecos descansa en el artículo 42 del Decreto n.º 2-21-406, el decreto de aplicación general de la Ley 05-20, que encomienda a la DGSSI la detección rápida de incidentes, la minimización del impacto, la corrección de vulnerabilidades y la restauración del servicio como sus objetivos declarados [115]. El plazo de

notificación específico o el umbral que desencadena una declaración obligatoria, y la división precisa del trabajo entre la función de auditoría de la DGSSI y el papel operativo de gestión de incidentes de maCERT, examinada más abajo en *Ciberseguridad defensiva y respuesta a incidentes*, no pudieron establecerse a partir del material revisado y se registran como carencias explícitas y no se infieren del lenguaje general del marco. La Estrategia Nacional de Ciberseguridad 2030 de la DGSSI, fechada el 22 de julio de 2024, declara su objetivo como mejorar la gobernanza nacional y reforzar el marco legal e institucional hasta 2030, respaldada por doce guías técnicas que abarcan la clasificación de datos, la gestión de incidentes, la seguridad de sistemas de control industrial, la continuidad de negocio y la auditoría [116].

Solo esta sección enumera al menos siete instrumentos legales y regulatorios distintos —la Ley 05-20 y su decreto de aplicación general 2-21-406, el Decreto 2-24-921 de nube IIV, la Ley 09-08, la disposición de etiquetado de IA del Código Penal de 2018, la Ley Orgánica n.º 53-25 y la Estrategia Nacional de Ciberseguridad 2030— además de varios référentiels técnicos propios de la DGSSI; la tabla siguiente los reúne todos para referencia rápida.

Tabla 12. Instrumentos legales y regulatorios de Marruecos sobre ciberespacio y protección de datos.

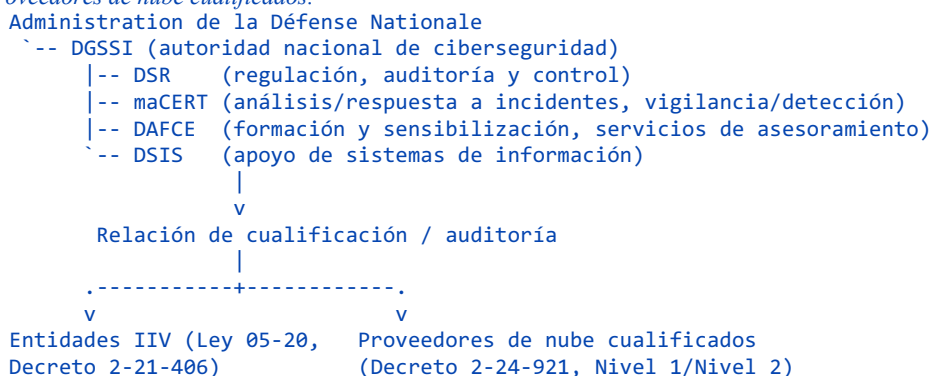
Instrumento	Cita legal	Fecha	Autoridad emisora/de aplicación	Obligación principal
Ley 05-20 (ciberseguridad)	Dahir n.º 1-20-69	25 jul. 2020	DGSSI (autoridad coordinadora nacional)	Establece la arquitectura nacional de ciberseguridad; obligaciones organizativas/técnicas para organismos estatales y operadores de infraestructura crítica
Decreto n.º 2-21-406 (decreto de aplicación general)	Aplica la Ley 05-20	2021	DGSSI	Marco de declaración de incidentes (art. 42): detección, minimización del impacto, corrección, restauración
Decreto n.º 2-24-921 (cualificación de proveedores de nube IIV)	Aplica el art. 25 de la Ley 05-20	22 oct. 2024	DGSSI (cualificación y auditoría)	Cualificación de proveedores de nube en dos niveles (Nivel 1 general; Nivel 2 de propiedad mayoritariamente marroquí, solo territorio nacional) para entidades de infraestructura vital
Ley 09-08 (protección de datos personales)	—	2009 (guía electoral 2026, 31 ago. 2026)	CNDP	Notificación/autorización previa para el tratamiento de datos personales; guía electoral 2026 (arts. 3, 10, 12, 21)
Art. 447-2 del Código Penal (etiquetado de	Enmienda al Código Penal de 2018	citado en 2026	CNDP / autoridades judiciales	Exige que el contenido de campaña generado por IA se etiquete como tal

contenido generado por IA)				
Ley Orgánica n.º 53-25 (Cámara de Representantes)	arts. 39, 51, 53	citado en 2026	Parlamento / CNDP	Normas de comunicación electoral referenciadas junto al requisito de etiquetado de IA
Guía de homologación de la DGSSI	Art. 19 de la Ley 05-20	9 nov. 2021	DGSSI	Homologación formal obligatoria de sistemas de información IIV sensibles antes del despliegue
Estrategia Nacional de Ciberseguridad 2030	—	22 jul. 2024	DGSSI	Hoja de ruta de gobernanza nacional y marco legal/institucional; doce guías técnicas de apoyo

Ciberseguridad defensiva y respuesta a incidentes

La DGSSI es la autoridad nacional de ciberseguridad de Marruecos, que organiza su propio mandato público en seis ámbitos funcionales —análisis y respuesta a incidentes, vigilancia y detección, regulación, auditoría y control, formación y sensibilización, y servicios de asesoramiento— prestados a través de cuatro direcciones internas identificadas: DSR, maCERT, DAFCE y DSIS [117]. Se trata de un mandato amplio, de todo el gobierno, que combina las funciones de regulador, auditor y respuesta operativa dentro de un único organismo, una concentración de autoridad que es eficiente para la coordinación pero que también significa que la DGSSI tiene un control externo independiente limitado sobre sus propios hallazgos de auditoría dentro del ámbito de la ciberseguridad civil (confianza: moderada, una inferencia de diseño institucional y no un hallazgo directamente documentado). La figura siguiente presenta esta estructura y la relación regulatoria de la DGSSI con las entidades de infraestructura vital y los proveedores de nube cualificados analizados más arriba en Derecho y regulación.

Figura 11. Estructura institucional de la DGSSI: direcciones, y su relación regulatoria con las entidades de infraestructura vital y los proveedores de nube cualificados.



maCERT, una de las cuatro direcciones de la DGSSI, es el CERT nacional de Marruecos, autodescrito como el centro de vigilancia, detección y respuesta a ataques informáticos, que persigue cuatro objetivos de seguridad —disponibilidad, integridad, confidencialidad y trazabilidad— a través de servicios reactivos (alerta, gestión de incidentes, análisis de incidentes, apoyo a la respuesta) y servicios proactivos (vigilancia tecnológica, evaluación de seguridad,

detección de intrusiones, difusión de información de seguridad) [118]. No se localizó ninguna fecha de fundación, cifra de personal, organigrama ni respuesta a incidentes históricos identificada en ninguna parte del material orientado al público de maCERT, una carencia explícita y operativamente relevante: no es posible, a partir de las fuentes abiertas revisadas, valorar la capacidad real o el historial de maCERT, solo su mandato declarado (confianza: alta en que esta carencia concreta existe, dado que refleja una comprobación de ausencia frente a la propia fuente primaria y no una inferencia). El único indicador cuantificado disponible, aunque indirecto, de la postura cibernética general de Marruecos es el Índice Nacional de Ciberseguridad 2026 (NCSI) de la Academia Estonia de Gobernanza Electrónica, en el que Marruecos se situó en el puesto 43 de 155 Estados con una puntuación de 79,17, en aumento en puntuación absoluta respecto a 70,13 en la edición anterior, aunque su posición cayera desde el puesto 32 al mejorar más rápido otros Estados comparables [119]. Este índice debe leerse como indicativo de la integridad de la política y el marco legal, y no de una capacidad operativa demostrada, y es un instrumento distinto del propio Índice Mundial de Ciberseguridad de la UIT, en el que Marruecos ocupó una posición de «Nivel 1» en 2024 —ambos no deben confundirse, un error que este capítulo ha visto cometido en parte de la cobertura de prensa marroquí del resultado del NCSI—; tomado junto con la carencia recién señalada, es probable (confianza: moderada) que la capacidad técnica real de respuesta a incidentes de maCERT sea más limitada de lo que sugerirían por sí solos su mandato formal de seis ámbitos y la respetable posición de Marruecos en el NCSI, dado que una puntuación sólida en el marco de políticas no es en sí misma evidencia de una función de CERT operativa madura. Las únicas afiliaciones de asociación internacional de maCERT documentadas de forma concreta, según su propia página primaria, son FIRST, el Forum of Incident Response and Security Teams, y OIC-CERT, la red de CERT de la Organización de Cooperación Islámica [118]; no se localizó ninguna corroboración de asociaciones bilaterales de ciberdefensa más amplias mediante ninguna fuente primaria de maCERT o la DGSSI, y cualquier afirmación de ese tipo debe tratarse como no confirmada y no repetirse como establecida.



Figura 12. El logotipo institucional de la DGSSI, obtenido directamente del sitio web oficial del organismo.

El logotipo combina una pequeña insignia con forma de escudo en los colores nacionales marroquíes con un logotipo textual en francés que reza «Royaume du Maroc / Administration de la Défense Nationale / Direction Générale de la Sécurité des Systèmes d'Information» [120]. El logotipo textual es en sí mismo informativo para este informe, dado que confirma públicamente la adscripción institucional de la DGSSI a la Administration de la Défense Nationale y no a un regulador de ciberseguridad puramente civil, corroborando el punto estructural ya expuesto más arriba en *Derecho y regulación* a partir del linaje del decreto y no solo del logotipo. No se localizó en el sitio de la DGSSI ninguna otra explicación oficial de los propios elementos heráldicos de la insignia —el motivo del mapa y la estrella, o los colores nacionales específicos utilizados— en el tiempo disponible para esta investigación, por lo que esta descripción es en consecuencia un inventario visual factual y no una glosa simbólica fundamentada en fuentes.

El propio maCERT ya no mantiene un sitio web público independiente: macert.ma no resuelve, y la ruta dgssi.gov.ma/macert redirige a la página principal de la DGSSI, que hace referencia a maCERT solo a través de noticias —participación en eventos de FIRST, OIC-CERT y APCERT— y una dirección de contacto funcional, sin ninguna imagen de logotipo específica de maCERT encontrada en la página; la propia página de afiliación de maCERT en FIRST.org muestra igualmente solo el propio logotipo de FIRST, sin ningún emblema específico de maCERT cargado [121]. En consecuencia, maCERT no tiene un emblema institucional propio y distinto: hoy opera como una función o equipo integrado dentro de la DGSSI y no como un organismo con marca

separada, y parece utilizar la propia identidad visual de la DGSSI, mostrada más arriba, y no un logotipo propio —un hallazgo negativo declarado explícitamente y no dejado sin abordar.

El caso de respuesta a incidentes del mundo real más claro registrado es la brecha de abril de 2025 de la Caja Nacional de Seguridad Social (CNSS) de Marruecos, confirmada de forma independiente por el propio CERT nacional de España: un actor de amenazas que usa el alias Jabaroot divulgó más de 53.000 archivos en BreachForums, que cubrían aproximadamente 500.000 empresas y dos millones de empleados, incluidos datos salariales y de contacto expuestos sin cifrar en servidores comprometidos [122]. El propio encuadre de INCIBE-CERT trata esto como una actividad orientada al mensaje político y no puramente motivada financieramente, vinculándola explícitamente a la tensión Marruecos-Argelia a través de la propia narrativa de represalia declarada por Jabaroot por un compromiso anterior de la cuenta de X de la Agencia de Prensa Argelina [122], un episodio examinado en detalle, junto con la campaña Jabaroot más amplia que inició, más abajo en *Hactivismo y confrontación de información*. Es probable que este incidente represente el incidente de ciberseguridad operativamente más significativo que el aparato defensivo de Marruecos ha tenido que gestionar en el periodo revisado (confianza: moderada), basándose en la magnitud de los registros expuestos y en la campaña sostenida y plurianual que desencadenó, aunque no se localizó ninguna declaración pública de la DGSSI o maCERT sobre su propia respuesta al incidente, en sí misma una carencia específica adicional.

No se localizó ninguna declaración pública oficial de la DGSSI o maCERT que abordara la brecha de la CNSS, las posteriores filtraciones de Jabaroot, o las afirmaciones de agosto de 2026 de una nueva brecha dirigida a los registros de personal de la DGST/DGSN —un silencio institucional que es en sí mismo analíticamente relevante. Existe una posibilidad prácticamente equivalente de que esto refleje una postura deliberada de no divulgación, coherente con la opacidad general que mantienen las instituciones de seguridad marroquíes en torno a los incidentes operativos, en lugar de una ausencia de cualquier esfuerzo de respuesta (confianza: baja, dado que no se localizó evidencia directa ni de una respuesta interna activa ni de una política deliberada de silencio); esto se declara como una carencia, no resuelta por inferencia en ningún sentido.

Recopilación de inteligencia y vigilancia

La comprensión forense y técnica de cómo se estructuran las operaciones de software espía de la clase Pegasus avanzó materialmente en el periodo revisado, aunque el indicador técnico públicamente documentado más antiguo específico de las propias redes de Marruecos lo precede considerablemente: el estudio «Hide and Seek» de Citizen Lab de 2018 identificó indicadores a nivel de red —sondeo de caché DNS y anomalías de huella digital TLS— coherentes con un presunto operador de Pegasus al que denominó en clave «ATLAS», geolocalizado en las propias redes de Maroc Telecom y Orange Maroc (números de sistema autónomo 6713 y 36925 respectivamente) desde agosto de 2017 [30]. El propio informe de Citizen Lab caracteriza explícitamente este mapeo a nivel de red como «una guía para futuras investigaciones, y no evidencia irrefutable», una limitación metodológica declarada por la propia fuente y no impuesta por este capítulo, y no establece por sí mismo qué organismo marroquí, si alguno, operaba la huella ATLAS —una cuestión a la que esta sección vuelve más abajo a través del reportaje más reciente de Forbidden Stories. El Security Lab de Amnistía Internacional publicó, en julio de 2026, su relato técnico público más detallado hasta la fecha de la evolución de Pegasus, basándose en documentos internos de NSO Group previamente inéditos divulgados a través del litigio estadounidense WhatsApp contra NSO [123]. Ese informe documenta la práctica de «White Services» de NSO, de crear cuentas y dominios específicos para cada cliente, y afirma que dos grupos dentro de la filtración original del Pegasus Project de 2021 se corresponden directamente

con despliegues que el informe etiqueta como «Sales 3» y «Sales 6», usados para demostraciones a proveedores [123]. El mismo informe hace referencia, sin nombrar directamente a Marruecos, a una línea de investigación activa de seguimiento de Forbidden Stories centrada explícitamente en «la máquina de espionaje de Marruecos» [123] —confirmación independiente, de un laboratorio forense distinto, de que la atención investigativa sería a una relación de cliente NSO específica de Marruecos seguía viva a mediados de 2026, tres años después de las revelaciones originales de 2021 (confianza: alta sobre el hecho de que tal línea de investigación exista; sus propios hallazgos son una cuestión distinta que este capítulo no valora).

El perfil de la DGST en un capítulo anterior de este informe ya rastrea en detalle el historial judicial 2021-2026 de las infecciones por Pegasus del presidente del Gobierno Pedro Sánchez, la ministra de Defensa Margarita Robles y el ministro del Interior Fernando Grande-Marlaska; este capítulo añade un dato más, directamente verificable. Una comprobación directa de fuente primaria del propio listado público de noticias judiciales de la Audiencia Nacional, que cubre del 2 de julio al 7 de septiembre de 2026, no encontró ningún elemento que hiciera referencia a esa investigación, ni ningún elemento que nombrara a Marruecos, la DGST o la DGED [124]. Esta ausencia es coherente con, aunque no confirma de forma independiente, la información de prensa según la cual el caso fue archivado por segunda vez en enero de 2026 citando la falta de cooperación judicial israelí; la brecha entre la ausencia de un elemento visible actual en el registro y una orden de archivo concreta y fechable se declara explícitamente como no resuelta y no se trata como zanjada (confianza: baja sobre la fecha y el razonamiento del archivo específicamente, moderada sobre la inactividad judicial actual del caso tal como se refleja en el listado público).

Sobre la cuestión pendiente de qué organismo marroquí, si alguno, operó realmente esta capacidad —dejada abierta inmediatamente más arriba y retomada más abajo en *Modelo de capacidades*— la atribución más específica localizada en toda esta investigación es la propia información de la edición en español del consorcio Forbidden Stories, que nombra a la DGST y no a la DGED como el servicio operador principal, con la DGED en un papel de mera coordinación [34]. Se trata de una afirmación materialmente más específica que el lenguaje genérico de atribución de Amnistía a «autoridades marroquíes», pero descansa en fuentes testimoniales de un único antiguo oficial seudónimo de la DGST relevado por un consorcio de investigación, y no en confirmación forense o judicial independiente; es muy probable (confianza: moderada) que los servicios estatales marroquíes, con mayor probabilidad la DGST, hayan operado Pegasus contra disidentes internos, periodistas y activistas saharauis desde al menos 2017, un juicio que descansa en la corroboración forense de dispositivo entre laboratorios de las infecciones subyacentes combinada con un patrón de objetivos coherente con los intereses estatales marroquíes conocidos, pero un juicio que se detiene antes de una resolución institucional firme DGST frente a DGED dada la naturaleza de fuente única de la afirmación sobre el organismo operador en concreto. El mismo hilo informativo lleva un detalle irónico de transferencia de capacidad directamente relevante para la cooperación España-Marruecos: se reporta que la Guardia Civil de España, a través de su unidad GAO, formó a personal de la DGST en tradecraft de vigilancia desde 2014 en adelante, con algunos de esos mismos oficiales formados presuntamente implicados más tarde, según fuentes testimoniales, en actividad de vigilancia que presuntamente se extendió a los propios formadores de la Guardia Civil [41]. Este detalle se declara aquí como reportado y atribuido testimonialmente, no confirmado judicialmente, coherente con la cautela evidencial más amplia que esta sección aplica en todo momento; de confirmarse, significaría que las competencias transferidas para la cooperación bilateral de seguridad se volvieron después, según este relato, contra la propia institución española que impartió la formación.

La pista nueva individual más significativa relativa a este expediente, examinada en detalle más arriba en *DGED* en un capítulo anterior, es una información de prensa española del 8 de septiembre de 2026 que nombra a Mehdi Hijaouy —descrito como antiguo subdirector de la DGED y antiguo

director de una unidad que la información denomina Service Action— como habiendo tenido acceso a documentación relacionada con Pegasus utilizada contra los tres ministros españoles nombrados más arriba, y como actualmente fugitivo viviendo entre Madrid y Cáceres tras huir de Marruecos hace aproximadamente dos años y no comparecer posteriormente en vistas judiciales españolas [125]. Esta afirmación descansa enteramente en fuentes de seguridad españolas no identificadas relevadas por un único medio y no está verificada por ninguna fuente forense, judicial o de prensa corroborante independiente localizada aquí; debe tratarse como una pista que requiere corroboración urgente de seguimiento, no como un hecho establecido (confianza: baja), aunque de confirmarse sería el primer desertor identificado de la DGED vinculado directamente a la cadena evidencial de Pegasus.

A nivel de la UE, el entorno de rendición de cuentas en torno al software espía de la clase Pegasus siguió activo a mediados de 2026 con independencia de la línea España-Marruecos específicamente. Una declaración conjunta de la sociedad civil del 6 de julio de 2026, tras la confirmación forense de Citizen Lab de que el eurodiputado griego Stelios Kouloglou fue infectado con Pegasus en octubre de 2022 y de nuevo en marzo de 2023 mientras formaba parte del comité de supervisión de software espía PEGA del Parlamento Europeo, instó a la Comisión Europea a iniciar una investigación independiente y a hacer cumplir el Reglamento de Doble Uso de la UE contra los proveedores de software espía [126]. Este elemento no hace referencia a Marruecos ni a España específicamente, pero demuestra que la presión de rendición de cuentas sobre el software espía a nivel de la UE persistió como una línea política viva más de cuatro años después de las revelaciones originales del Pegasus Project, situando las infecciones de Sánchez/Robles/Grande-Marlaska dentro de un patrón más amplio de objetivos a nivel parlamentario de la UE sin resolver, y no como un episodio español aislado (confianza: alta sobre el hecho de la actividad continuada a nivel de la UE).

Una columna de opinión española identificada, registrada aquí sin respaldo, argumenta explícitamente que la infección por Pegasus de 2021 del teléfono del presidente del Gobierno Sánchez pudo haber influido en el giro de España de abril de 2022 respecto a su posición histórica sobre el Sáhara Occidental, mediante una carta personal al rey Mohamed VI [127]. Ambos hechos subyacentes —la infección de 2021 y el cambio de política de 2022— están documentados de forma independiente en otras partes de este informe; el vínculo causal entre ellos es una inferencia propia de este columnista, no respaldada por ninguna declaración gubernamental, investigación o fuente corroborante localizada aquí, y es improbable que el material de fuentes abiertas permita actualmente un juicio responsable que confirme o descarte ese vínculo (confianza: baja, es decir, baja confianza en que actualmente sea posible un juicio más firme en cualquier sentido).

Más allá de la línea Pegasus específicamente, este mismo periodo vio una campaña de filtraciones Jabaroot en escalada contra datos del sector de seguridad marroquí, alcanzando, hacia agosto de 2026, una amenaza de exponer aproximadamente 70.000 nombres de personal afiliado a la DGST; circulan al menos seis teorías de atribución mutuamente excluyentes para esa campaña, ninguna confirmada forensemente, y este capítulo remite su comparación completa a *Hacktivismo y confrontación de información y Grupos APT* más abajo, en lugar de duplicar aquí el análisis.

Ciberguerra militar, guerra electrónica y C4ISR

El hallazgo central y más trascendente de esta sección es una carencia, declarada llanamente y no rellenada por inferencia: ninguna fuente primaria, técnica o de periodismo de investigación consultada para este capítulo documenta una unidad de ciberguerra dedicada e identificada, un mando formal de guerra electrónica, o un programa unificado de integración de red C4ISR dentro de las Fuerzas Armadas Reales de Marruecos (FAR) o su aparato de inteligencia militar [128].

Esta ausencia no debe leerse como evidencia de que tal capacidad o unidad no exista —las instituciones militares y de seguridad marroquíes son consistente y deliberadamente opacas sobre el detalle organizativo interno en fuentes abiertas, un patrón ya observado de forma independiente para la propia autodescripción pública de la DGSSI y maCERT más arriba en *Ciberseguridad defensiva y respuesta a incidentes*— pero es una carencia de información genuina, y no meramente cosmética, que limita materialmente lo que este capítulo puede valorar (confianza: alta en que la propia carencia es real, lo que significa alta confianza en que el método de investigación subyacente, y no la mera mala suerte, no logró localizar tal material).

El único material relevante para las FAR localizado de forma concreta se refiere a equipamiento táctico de guerra electrónica y reconocimiento a nivel de plataforma, y no a una unidad cibernética o un programa C4ISR: conjuntos de autoprotección y alerta de radar instalados en los F-16 (ASPIIS II, AN/ALR-93) y modernizaciones anteriores de F-5/Mirage F1 (contenedores ECM de Elettronica, sistemas de alerta de radar y enlace de datos de Thales), dos aeronaves Gulfstream G550 configuradas para alerta temprana y control aerotransportados con dos más encargadas, y, históricamente, aeronaves C-130 Hercules equipadas con radar aerotransportado de barrido lateral usado para la detección de unidades enemigas durante el conflicto del Sáhara Occidental [128]. Este material procede únicamente de una compilación terciaria cuyas propias citas internas no pudieron resolverse de forma independiente aquí, y debe leerse estrictamente como una pista para verificación de seguimiento en fuentes primarias, y no como detalle de capacidad confirmado (confianza: baja en cualquier cifra específica); el punto cualitativo más amplio de que las FAR operan cierto equipamiento táctico de guerra electrónica/ISR es en sí mismo incontrovertido y coherente con las relaciones documentadas de Marruecos con proveedores extranjeros analizadas en otras partes de este informe, pero este capítulo no puede ir más allá de eso sin sobreinterpretar una fuente escasa.

No se localizó ninguna evidencia de una unidad cibernética identificada específicamente dentro del aparato de inteligencia militar de Marruecos, a diferencia de los servicios civiles DGST y DGED examinados en un capítulo anterior y de la ubicación institucional de la DGSSI bajo la Administration de la Défense Nationale, que es un canal próximo a la defensa pero no específico de inteligencia militar. Dada la ausencia casi total de material de fuentes abiertas sobre esta cuestión específica, sería analíticamente irresponsable ofrecer un juicio con banda WEP sobre si tal unidad existe en absoluto; este capítulo, en cambio, declara la carencia y la señala como el objetivo de seguimiento de máxima prioridad individual para cualquier pasada de investigación posterior, consultando idealmente fuentes especializadas de inteligencia de defensa como Janes o el IISS, a las que esta investigación no pudo acceder.

Ciberdelito y análisis forense digital

El entorno de ciberamenazas de Marruecos, según se documenta aquí, se separa claramente en cuatro capas analíticamente distintas que este capítulo trata por separado en todo momento: el ciberdelito con motivación financiera investigado por las fuerzas del orden convencionales, examinado más abajo en *Las fuerzas del orden en el ciberespacio y Ciberdelito*; un fenómeno amplio, controvertido y abrumadoramente de fuente única de hacktivismo y filtraciones tras intrusión, centrado en el actor conocido como Jabaroot o JabaROOT DZ, examinado más abajo en *Hactivismo y confrontación de información*; un ecosistema de apoyo de proveedores comerciales privados y extranjeros más una capa académica de investigación notablemente escasa, examinada más abajo en *Otros actores*; y un pequeño número de operaciones técnicamente documentadas de grado APT, examinadas más abajo en *Grupos APT*. Es probable que esta asimetría evidencial —una corroboración sólida, identificada y multipartita para los casos ordinarios de ciberdelito

financiero frente a afirmaciones escasas, de fuente única y dirigidas por el propio actor para el material de hacktivismo— refleje una diferencia genuina en cómo se vigilan y reportan estos dos tipos de actividad, y no un artefacto de la propia estrategia de búsqueda de esta investigación (confianza: moderada, dado que el patrón se mantuvo de forma consistente en todas las fuentes examinadas). Ninguna de las dos líneas debe confundirse con la línea de vigilancia de inteligencia DGST/DGED perfilada más arriba en *Recopilación de inteligencia y vigilancia*.

Las fuerzas del orden en el ciberespacio

La DGSN, la policía nacional de Marruecos, construyó su capacidad de investigación de cibercrimen de forma incremental a lo largo de más de una década: se creó una célula dedicada a combatir el cibercrimen en 2007, siguió un servicio central especializado en 2013 dentro de la dirección de Rabat de la Policía Judicial, y se estableció en 2018 una Oficina Nacional de lucha contra la delincuencia relacionada con la tecnología en la Brigade Nationale de la Police Judiciaire (BNPJ), con sede en Casablanca, dotada de aproximadamente una docena de agentes de policía judicial y un número similar de técnicos e ingenieros de informática y telecomunicaciones [129]. Esta capacidad central está respaldada, según la misma fuente, por 29 brigadas regionales de cibercrimen que cubren prácticamente todas las prefecturas y provincias de Marruecos, y por siete laboratorios de análisis forense digital identificados, en Rabat, Casablanca (dos), El Aaiún, Fez, Marrakech y Tetuán [129]. Este relato nombra a un funcionario identificado —el comisario divisionario Marouane Hejjouji, jefe del laboratorio de análisis forense digital de la BNPJ— una mejora genuina de fiabilidad respecto al material de fuente anónima que domina el material de hacktivismo examinado más abajo, aunque sigue siendo una autodescripción del organismo relevada por prensa y no una publicación primaria de la DGSN auditada de forma independiente. Es muy probable que las unidades de investigación de cibercrimen y análisis forense digital de la DGSN posean una capacidad operativa genuina, y no meramente sobre el papel (confianza: moderada), un juicio que no descansa solo en el relato de historia institucional, sino en resultados operativos identificados y fechados de forma independiente —específicamente la detención de la Operación Lyrebird y la detención de octubre de 2022 en el aeropuerto de Casablanca por notificación de INTERPOL detalladas más abajo en *Cibercrimen*, ambas de las cuales requirieron una capacidad funcional de evidencia digital y de enlace internacional para llegar a un sospechoso identificado. En cambio, no se localizó ningún relato público comparablemente detallado de una capacidad de análisis forense cibernético dedicada dentro del BCIJ, el brazo de policía judicial de la DGST para el trabajo de casos de terrorismo —una carencia explícita y declarada, y no evidencia de que la capacidad no exista, y una que este capítulo deliberadamente no disimula por inferencia a partir de la fortaleza documentada por separado de la DGSN. La arquitectura de regulador civil de ciberseguridad DGSSI/maCERT, cubierta en profundidad más arriba, es institucional y funcionalmente distinta de esta capacidad de investigación y análisis forense de las fuerzas del orden y no se repite aquí.

Cibercrimen

El caso notable más claro y más verificable de forma independiente registrado es la Operación Lyrebird, una investigación conjunta de dos años de la DGSN, INTERPOL y la firma comercial identificada de ciberinteligencia de amenazas Group-IB, que culminó en la detención de un sospechoso que usaba el alias Dr Hex, al que Group-IB atribuye aproximadamente 134 ataques de desfiguración de sitios web y fraude de pagos entre 2009 y 2018, dirigidos predominantemente contra empresas e instituciones financieras francófonas [130]. Se trata de un caso evidencialmente mucho más sólido que cualquier elemento del registro de hacktivismo que sigue más abajo: nombra a las tres partes cooperantes, un alias específico, un recuento de ataques con una metodología declarada —el propio seguimiento por Group-IB de una firma digital consistente

dejada en páginas comprometidas— y cita a un funcionario de INTERPOL identificado [130]. Un segundo caso, fechado de forma independiente, un sospechoso de 24 años interceptado en el Aeropuerto Internacional Mohamed V de Casablanca el 18 de octubre de 2022 mientras intentaba embarcar en un vuelo con destino a Turquía después de que el control fronterizo lo señalara frente a una notificación de personas buscadas de INTERPOL por fraude de tarjetas robadas y pirateo de cuentas bancarias internacionales, corrobora además que los sistemas marroquíes de control fronterizo y policía judicial interoperan funcionalmente con el sistema de notificaciones de INTERPOL en la práctica fechada e individualmente verificable, y no solo en principio [131].

A nivel de cooperación regional, la prensa marroquí informó de la participación de Marruecos en una operación multinacional realizada entre octubre de 2025 y el 28 de febrero de 2026 —descrita por el medio informante como la primera acción regional de esta magnitud— que facilitó el intercambio de aproximadamente 8.000 elementos de inteligencia entre los Estados participantes, condujo a la incautación de 53 servidores, y resultó en procedimientos judiciales contra tres personas en Marruecos, dirigida contra infraestructura de phishing y distribución de malware [132]. El nombre en clave específico de esta operación, reportado en otra parte como Ramz pero fuera de las fuentes directamente consultadas para este capítulo, no pudo confirmarse de forma independiente frente a una publicación primaria de INTERPOL; la existencia de la operación y sus estadísticas principales se tratan como probablemente exactas (confianza: moderada, descansando en un único relato de prensa comercial marroquí) a la espera de la confirmación primaria de INTERPOL que esta investigación no pudo obtener. La tabla siguiente reúne estos casos para referencia rápida.

Tabla 13. Casos notables de cibercrimen con motivación financiera y operaciones de cooperación.

Caso/operación	Fecha	Organismos cooperantes	Resultado declarado	Solidez evidencial
Operación Lyrebird («Dr Hex»)	Ventana de comisión 2009-2018; detención reportada en 2026	DGSN, INTERPOL, Group-IB	Detención de un sospechoso al que se atribuyen aproximadamente 134 ataques de desfiguración/fraude de pagos	Fuerte: partes identificadas, alias, recuento de ataques, funcionario de INTERPOL identificado
Detención en el aeropuerto de Casablanca	18 oct. 2022	Control fronterizo de la DGSN, sistema de notificaciones de INTERPOL	Sospechoso interceptado por una notificación de personas buscadas de INTERPOL por fraude de tarjetas robadas y pirateo de cuentas bancarias	Moderada: fechado, individualmente verificable
Operación regional octubre 2025-febrero 2026	Oct. 2025-28 feb. 2026	Marruecos, INTERPOL, socios regionales	~8.000 elementos de inteligencia intercambiados; 53 servidores incautados; procedimientos judiciales contra 3 personas	Moderada: fuente única de prensa comercial marroquí; confirmación primaria de INTERPOL no obtenida

Por separado, una investigación con fuente en Kaspersky reportó que el 49,3 % de los casos de fraude basado en mensajería contra víctimas marroquíes concluyó en los 30 minutos siguientes al primer contacto, con pérdidas financieras medias de 733 dólares por víctima, superando los 1.350 dólares en algunos casos, predominantemente a través de la suplantación de contactos o marcas de confianza en WhatsApp, Facebook y Telegram [133]. Es probable que este patrón de fraude de ingeniería social de rápido desarrollo represente una amenaza distinta y de mayor volumen para los consumidores marroquíes ordinarios que la narrativa de brechas vinculadas al Estado que domina el resto de este capítulo (confianza: moderada, basada en la propia metodología declarada por Kaspersky, aunque esta cifra es investigación derivada de una empresa y no una estadística nacional auditada de forma independiente).

Hactivismo y confrontación de información

El actor de hactivismo dominante documentado en esta investigación opera bajo el nombre Jabaroot, también estilizado como JabaROOT o JabaROOT DZ, identificado por primera vez en abril de 2025 con la brecha de la Caja Nacional de Seguridad Social (CNSS) de Marruecos, examinada más arriba en *Ciberseguridad defensiva y respuesta a incidentes*, y escalando a través de una cadena de filtraciones reivindicadas —el Ministerio de Inclusión Económica, el Ministerio de Justicia, la agencia nacional de seguridad vial NARSA, el registro de la propiedad ANCFCC, la caja de cobertura social CNOPS, una brecha reivindicada de 17 millones de registros de la base de datos de asistencia médica RAMED el 20 de agosto de 2026, y, desde agosto de 2026, un conjunto de datos reivindicado de 70.000 registros que nombra a personal de la DGST/DGSN— encuadrada explícitamente por el actor como represalia por un compromiso anterior favorable a Marruecos de la cuenta de X de la Agencia de Prensa Argelina y, desde agosto de 2026, vinculada explícitamente a la crisis migratoria de Ceuta bajo el lema de campaña «#OP_CEUTA» [122]. La afirmación sobre RAMED lleva su propia discrepancia interna, señalada por la propia fuente: los 17 millones de registros reivindicados superan los 10,83 millones de registros realmente migrados de RAMED a su régimen sucesor de diciembre de 2022, AMO-Tadamon, una discrepancia que el propio medio informante señala pero no resuelve, y que este capítulo trata como una única afirmación de fuente no identificada y no como una brecha confirmada de ninguna magnitud concreta [134]. Es casi seguro que esto representa una campaña sostenida y plurianual, y no una serie de incidentes no relacionados, dado el etiquetado consistente, el patrón de distribución por Telegram y la escalada autorreferencial a lo largo de más de una docena de tramos reportados de forma independiente (confianza: alta, dado que esta cronología está corroborada por la prensa española, marroquí y argelina y por al menos dos comprobaciones técnicas independientes detalladas más abajo).

Si Jabaroot denota a un único actor, a un pequeño grupo coordinado o a una marca compartida de forma laxa usada por más de una parte sigue siendo explícitamente no resuelto en todas las fuentes revisadas, incluida una compilación terciaria dedicada cuya propia conclusión es que el origen del actor sigue sin resolverse [135]. Circulan al menos cinco teorías de atribución mutuamente excluyentes, y ninguna está confirmada forensemente: la propia posición del gobierno marroquí de que Jabaroot es un instrumento del Estado argelino; una lectura de hactivista independiente; la hipótesis de una consultora especializada, Navakintelligence, de que un único antiguo operativo de inteligencia marroquí, actuando en solitario, es el responsable [136]; una afirmación, atribuida a una firma llamada Zecurion solo a través de una compilación terciaria y no localizable de forma independiente en ningún informe primario consultado aquí, según la cual indicadores técnicos apuntan a un ingeniero de origen tunecino residente en Alemania [135]; y la posibilidad, planteada por la pista de Hijaouy examinada más arriba en *Recopilación de inteligencia y vigilancia*, de que

un antiguo oficial identificado de la DGED esté conectado a las filtraciones [125, 137]. La tabla siguiente presenta las cinco una junto a otra.

Una sexta teoría, reportada por Le Monde y relevada a través del medio argelino TSA (Tout sur l'Algérie), sostiene que las filtraciones son obra de cinco antiguos agentes de la DGST identificados en cuanto al fondo —cuatro oficiales y un comisario— que rompieron con el servicio y se exiliaron en Europa, y que presuntamente actúan por agravio institucional y personal, exigiendo cambios de dirección y citando el abuso de datos personales en escuchas e investigaciones [138]. Esta teoría tiene cierta coherencia interna con el propio contenido de la filtración —su objetivo específico de datos de personal de seguridad, su exculpación del rey mientras culpa personalmente a la cúpula identificada de los servicios de seguridad, y sus amenazas de nuevas revelaciones vinculadas a Ceuta encajan todas mejor con una narrativa de agravio interno que con una operación puramente externa y oportunista de hacktivismo o de inteligencia extranjera— pero sigue siendo información de fuente única del propio Le Monde, relevada de segunda mano por un medio argelino con un interés evidente en desacreditar el propio encuadre del gobierno marroquí de patrocinio estatal argelino, y no está confirmada de forma independiente por ningún indicador técnico localizado en toda esta investigación (confianza: baja, exactamente como cada una de las otras cinco teorías individualmente). Es muy improbable que las seis teorías puedan ser correctas simultáneamente (confianza: alta), y la propia narrativa preferida de Marruecos —patrocinio estatal argelino— es a su vez dudada de forma independiente por fuentes del sector de la ciberseguridad y de inteligencia citadas dentro de la misma información de prensa marroquí y española que la difunde, un punto que este capítulo pondera en lugar de tratar como más establecido evidencialmente de lo que su fuente real respalda, dado que esa narrativa también sirve al propio interés institucional de Rabat de externalizar la culpa.

Tabla 14. Teorías de atribución en disputa para la campaña Jabaroot/JabaROOT DZ.

Teoría	Proponente	Base evidencial	Confianza de este informe
Dirigida por el Estado argelino	Gobierno marroquí / posición oficial marroquí	Encuadre público consistente de Rabat; sin corroboración forense independiente	Baja
Colectivo hacktivista independiente	Comentario general de fuentes abiertas	Coherente con las tácticas observadas; no fundamentada por separado	Baja
Antiguo operativo de inteligencia marroquí en solitario	Navakintelligence (consultora española)	Valoración de consultora especializada relevada en prensa regional	Baja
Ingeniero de origen tunecino residente en Alemania	Firma llamada «Zecurion» (no localizada)	Citada solo a través de una compilación terciaria; no localizable de forma independiente en ningún informe primario	Baja (no localizada)
Antiguo oficial de la DGED identificado (vinculado a Hijaouy)	Prensa española de un único medio, fuentes de seguridad no identificadas	Acceso reportado a material de Pegasus; no verificado por	Baja

fuerza forense o
judicial independiente

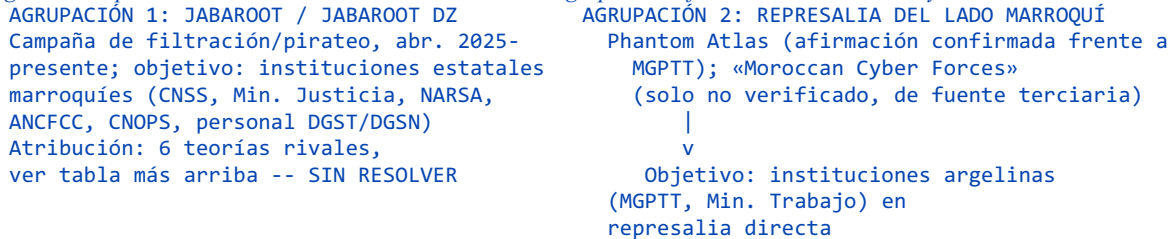
Existe una posibilidad prácticamente equivalente de que cualquiera de estas seis teorías sea correcta de forma aislada (confianza: baja, individualmente, para cada una), y solo es defendible un juicio de orden superior de confianza moderada: que el acceso de la campaña a datos personales específicos, sensibles y, en al menos un caso, previamente inéditos es más coherente con un acceso próximo a un informante interno que con una operación puramente externa y oportunista de hacktivismo (confianza: baja a moderada) —una lectura que la sexta teoría, la del exilio de la DGST, explicaría directamente de ser exacta, aunque por ello no queda más confirmada que las otras cinco. Cuál, si alguna, de las seis es exacta sigue genuinamente sin resolverse en el registro de fuentes abiertas tal como se reúne aquí, y ninguna hipótesis debe adoptarse por encima de una posición de confianza baja y prácticamente equivalente; se trata de un problema de atribución genuinamente sin resolver, no de un caso en el que una explicación simplemente espera confirmación.

Los propios servicios de seguridad de Marruecos no han permanecido en silencio: la DGSN y la DGST negaron pública y categóricamente cualquier intrusión en sus sistemas tras la afirmación de filtración de personal de la DGST/DGSN de agosto de 2026, declarando que los datos proceden en cambio de registros antiguos de seguros y cobertura social y que sus redes operativas no están conectadas a redes abiertas a internet, con analistas independientes citados en la misma información considerando implausiblemente grande la cifra reivindicada de 70.000 registros, dado que muchas de las personas identificadas eran agentes de policía ordinarios, personas fallecidas, o tenían fechas de reclutamiento no posteriores a 2020 [139]. Esta contranarrativa oficial es en sí misma no verificada e interesada, exactamente como las afirmaciones de la filtración que disputa son no verificadas e interesadas por parte del actor, y este informe las pondera a ambas de forma simétrica en lugar de decantarse por defecto por ninguna. Una comprobación técnica independiente distinta, realizada por el proveedor comercial de ciberinteligencia de amenazas CybelAngel sobre la anterior filtración del registro de la propiedad de la ANCFCC, llegó a un veredicto genuinamente mixto: el archivo muestreado de 4,8 GB, de unos 20.000 documentos, que obtuvo, no contenía malware de alerta alta en su subconjunto de «VIP», pero Jabaroot nunca entregó el conjunto de datos completo reivindicado de 10 millones de registros y cuatro terabytes, y el propio análisis de CybelAngel no encontró vínculos directos entre Jabaroot y otros grupos como Keymous+ [140]. El hacktivismo alineado con Marruecos discurre en la dirección opuesta como una imagen especular documentada, aunque más tenue: un grupo autoidentificado como Phantom Atlas afirmó, dentro de las 24 horas siguientes a la brecha original de la CNSS de abril de 2025, haber exfiltrado más de 13 GB de datos del fondo mutual de trabajadores postales y de telecomunicaciones de Argelia (MGPTT) y documentos internos del Ministerio de Trabajo argelino, encuadrado explícitamente como represalia [141]. Un segundo nombre atribuido a Marruecos, «Moroccan Cyber Forces», se cita en una compilación terciaria como habiendo llevado a cabo una afirmación de represalia similar el 10 de abril de 2025, pero no pudo localizarse de forma independiente en ninguna fuente primaria o de prensa consultada aquí, y se registra únicamente como una afirmación no verificada de fuente terciaria [135]. Por separado, la fuente técnica independiente más clara de esta investigación establece que un tercer actor, Keymous+, asociado en otras partes con actividad DDoS motivada por la causa propalestina contra objetivos gubernamentales marroquíes, se valora como operativamente distinto de Jabaroot y no como una identidad compartida, pese al solapamiento temporal y regional [140].

Es probable que el panorama de hacktivismo de Marruecos en el periodo revisado comprendiera al menos tres agrupaciones de amenaza funcionalmente separadas —la campaña de filtraciones Jabaroot/JabaROOT DZ, una agrupación de represalia más pequeña del lado marroquí, y una

agrupación distinta de DDoS propalestina— y no una única campaña unificada ni una rivalidad binaria de dos bandos (confianza: moderada, basada en el hallazgo explícito de no vinculación de CybelAngel y las tácticas distintas —filtraciones masivas de datos frente a DDoS— que emplea cada agrupación). La figura siguiente presenta esta estructura de tres agrupaciones.

Figura 13. El panorama de hacktivismo de Marruecos: tres agrupaciones funcionalmente distintas y no una única rivalidad de dos bandos.



AGRUPACIÓN 3: DDoS PROPALESTINO (Keymous+)
 Actividad DDoS contra objetivos del gobierno marroquí;
 CybelAngel: técnicamente DISTINTO de Jabaroot pese al solapamiento temporal/regional -- no se halló infraestructura compartida

La dimensión de confrontación informativa de esta campaña se extiende más allá de la divulgación de datos hacia exigencias políticas explícitas y afirmaciones no verificadas sobre terceros países: Jabaroot ha exigido una disculpa oficial marroquí, una declaración de duelo nacional y el aplazamiento de las elecciones legislativas del 23 de septiembre de 2026, y ha afirmado por separado, mediante mensajes de Telegram relevados por un medio con una orientación de incidencia proafiliada a la causa saharauí reconocida, que un presunto plan marroquí de presión migratoria implicaba conocimiento estadounidense e israelí, una afirmación tratada aquí como no verificada y de fuente del propio actor, y no como establecida [142]. La propia síntesis de agosto de 2026 de un medio español especializado en ciberseguridad advierte explícitamente contra la atribución prematura tanto en la línea de Pegasus como en la de JabaROOT simultáneamente, encuadrando el riesgo central como la proliferación de actores de atribución incierta operando en una zona gris entre el hacktivismo, los intereses estatales y la desinformación [143].

Es probable que este patrón —filtraciones de datos emparejadas con exigencias políticas explícitas y afirmaciones geopolíticas no verificables— deba leerse en sí mismo como evidencia de que los mensajes de Jabaroot funcionan como una operación de información, no solo como un mecanismo de divulgación de una brecha de datos, con independencia de cómo se resuelva finalmente la cuestión subyacente de acceso a los datos (confianza: moderada). Un efecto posterior adicional señalado en el análisis de prensa es el daño potencial a las relaciones de cooperación de seguridad africana de Marruecos, dado que la filtración de datos de personal podría en principio permitir a adversarios cotejar identidades frente a los registros de formación y enlace de unos veinte Estados socios africanos [144], aunque este juicio concreto es una inferencia analítica propia del medio citado y no un efecto confirmado de forma independiente.

Otros actores

Más allá de las capas estatales de orden público y de hacktivismo/APT ya cubiertas, el ecosistema cibernético de Marruecos incluye un sector de proveedores comerciales privados, al menos una estructura documentada de asociación con proveedores extranjeros, y una huella de investigación académica de fuentes abiertas notablemente escasa —tres subcapas que este capítulo trata por su orden más abajo, cada una fundamentada en lo que las comprobaciones directas de fuentes primarias pudieron y no pudieron establecer, y no en conocimiento general del sector.

Proveedores privados

FIRST, el Forum of Incident Response and Security Teams, un organismo internacional oficial de coordinación de CSIRT, enumera siete equipos de respuesta a incidentes registrados en Marruecos en su directorio público de miembros: maCERT, el CERT estatal ya perfilado más arriba en *Ciberseguridad defensiva y respuesta a incidentes*; Dataprotect-CSIRT; Cires Technologies CyberSOC; DXC-CDG Cyber Defense, examinado por su dimensión de proveedor extranjero más abajo en *Proveedores extranjeros*; SEKERA CSIRT; LMPS CERT; y CERT-BAM, el propio equipo de respuesta a incidentes de Bank Al-Maghrib [145]. Esto evidencia directamente un ecosistema marroquí de CSIRT en maduración y multiactor que se extiende mucho más allá del CERT nacional hacia la banca y al menos cuatro CSIRT y CyberSOC de operación privada, un indicador genuinamente positivo de capacidad institucional independiente del material de hacktivismo más controvertido examinado más arriba. La tabla siguiente reúne los siete para referencia rápida.

Tabla 15. Equipos CERT/CSIRT registrados en Marruecos listados en el directorio de miembros de FIRST.

Nombre	Carácter	Institución matriz/propietario
maCERT	CERT estatal	DGSSI (Administration de la Défense Nationale)
Dataprotect-CSIRT	Privado	DataProtect
Cires Technologies CyberSOC	Privado	Cires Technologies
DXC-CDG Cyber Defense	Empresa conjunta (extranjera/vinculada al Estado)	DXC Technology (EE. UU.) + Caisse de Dépôt et de Gestion (Marruecos)
SEKERA CSIRT	Privado	SEKERA
LMPS CERT	Privado	LMPS
CERT-BAM	Banca/banco central	Bank Al-Maghrib

DataProtect, cuyo propio sitio corporativo se consultó directamente para esta investigación, describe un catálogo de servicios que abarca vigilancia CyberSOC y CSIRT 24/7, servicios de seguridad gestionados, pruebas de penetración de seguridad ofensiva, apoyo a la gobernanza y el cumplimiento, seguridad en la nube, protección de infraestructuras críticas y una oferta de formación dedicada Cyber Skills Lab, prestando servicio a clientes de banca, seguros, gobierno e industria en una huella panafricana declarada desde su sede en Casablanca [146]. Es probable que DataProtect y Cires Technologies representen los proveedores privados de ciberseguridad de Marruecos más reconocidos internacionalmente, dada su confirmación independiente en el propio directorio de FIRST y no la mera dependencia de la autodescripción de marketing (confianza: moderada); un acceso directo al propio sitio corporativo de Cires Technologies falló para esta investigación, dejando su catálogo específico de servicios conocido solo a través del listado de FIRST, una carencia explícita y nombrable.

Proveedores extranjeros

La relación con proveedor extranjero documentada de forma más clara dentro del alcance de este capítulo es DXC-CDG Cyber Defense, una estructura conjunta de CSIRT que combina a DXC Technology, una firma global de servicios de TI con sede en EE. UU., con CDG, la Caisse de Dépôt et de Gestion, una gran institución financiera pública marroquí, confirmada de forma independiente a través del propio directorio de miembros de FIRST [145]. Se trata de una asociación legítima con un proveedor extranjero del lado defensivo, estructuralmente distinta de —y considerablemente menos controvertida que— las relaciones con proveedores de vigilancia abordadas más abajo respecto a NSO Group y Pegasus, examinadas en detalle más arriba en *Recopilación de inteligencia y vigilancia* y *DGST* y *DGED* en un capítulo anterior; el propio Pegasus, según ese registro más completo, es un producto israelí enteramente comercial que se ha

utilizado contra periodistas y activistas internos, jefes de gobierno extranjeros, incluidos Macron de Francia y Sánchez de España, y más de 6.000 números de teléfono argelinos, este último presuntamente un factor contribuyente en la ruptura de relaciones de Argelia con Marruecos de agosto de 2021 [147].

En el lado de los proveedores de vigilancia específicamente, una comprobación directa y dirigida del propio informe técnico de julio de 2026 del Security Lab de Amnistía Internacional sobre la evolución de Pegasus en busca de cualquier vínculo marroquí documentado con un proveedor distinto de NSO Group —Circles, Candiru, Intellexa/Predator, Cytrox, DarkMatter— no encontró ninguno: Intellexa/Predator aparece en ese informe solo como una referencia cruzada no relacionada, sin que se declare ningún nexo con Marruecos [123]. Es improbable que la información de fuentes abiertas documente actualmente ninguna relación con proveedor de vigilancia vinculada a Marruecos más allá de NSO/Pegasus (confianza: moderada, dado que se trata de una ausencia comprobada activamente frente a una fuente forense actual y creíble, y no de una suposición a partir del silencio, aunque no puede descartar una relación no divulgada). Esta carencia específica ha resultado consistente a lo largo de sucesivas pasadas de investigación sobre el dominio cibernético de Marruecos y se declara aquí como una limitación permanente, y no meramente puntual, del registro de fuentes abiertas disponible. Frente a esa ausencia consistente, un único medio español, Merca2, afirma por separado que Marruecos gasta más de 50 millones de euros anuales en herramientas occidentales adicionales de vigilancia e interceptación más allá de NSO/Pegasus —nombrando el producto de vigilancia masiva de tráfico de internet «Evident» de BAE Systems, el captador de IMSI «Hailstorm» de L3Harris, las herramientas de extracción de dispositivos de Cellebrite, y «RCS», de la firma italiana Memento Labs, una línea de producto sucesora de la de Hacking Team— financiadas, según el mismo informe, a través de un intermediario con sede en Abu Dabi, y alega además que Maroc Telecom y Orange Maroc mantienen conexiones directas de servidor con la DGST que permiten la interceptación fuera de la supervisión judicial [148]. Esta afirmación se comprobó directamente frente al propio informe de Amnistía de julio de 2026 sobre Pegasus, examinado más arriba, y no se encontró allí corroboración alguna para ninguna de estas herramientas nombradas ni para las presuntas conexiones de servidor con operadores de telecomunicaciones; descansa en la propia información de investigación de un único medio y no en confirmación forense o judicial independiente, y debe tratarse como una pista no confirmada y no como una capacidad establecida (confianza: baja).

Tabla 16. Proveedores comerciales extranjeros nombrados en esta recopilación, confirmados y comprobados-y-ausentes.

Proveedor	País	Producto/servicio	Vínculo con Marruecos	Base evidencial
NSO Group	Israel	Pegasus (intrusión en dispositivos móviles)	Confirmado	Información forense del Security Lab de Amnistía Internacional; confirmaciones de gobiernos extranjeros (ver *Recopilación de inteligencia y vigilancia* y los perfiles de la DGST/DGED en un capítulo anterior)

DXC Technology	Estados Unidos	CSIRT conjunto defensivo (DXC-CDG Cyber Defense)	Confirmado (asociación legítima del lado defensivo)	Directorio de miembros de FIRST
Circles, Candiru, Intellexa/Predator, Cytrox, DarkMatter	Varios	Herramientas comerciales de intrusión/vigilancia	Comprobado, no encontrado	La comprobación directa del informe técnico de Amnistía de julio de 2026 no encontró nexo con Marruecos para ninguno de estos proveedores

El ámbito académico

No se identificó ningún centro, cátedra o laboratorio de investigación académica marroquí dedicado y específico de ciberseguridad en el material revisado para este capítulo. Las comprobaciones directas de actividad de investigación específica de ciberseguridad en la ENSIAS, la École Nationale Supérieure d'Informatique et d'Analyse des Systèmes, y en el INPT, el Institut National des Postes et Télécommunications, solo revelaron contenido general de ingeniería y un listado de programa Master Data & IA, sin identificarse ninguna cátedra, laboratorio o registro de publicaciones específico de ciberseguridad, y una comprobación de la página principal de la UM6P tampoco reveló contenido específico de ciberseguridad dentro de la profundidad de página alcanzada. Esto se declara explícitamente como una carencia de investigación y no como evidencia de que tal capacidad académica no exista en Marruecos —las páginas de investigación universitaria a menudo no están indexadas a la profundidad que alcanza un único acceso de página, y una búsqueda más específica de páginas individuales de publicaciones del profesorado o un archivo dedicado de actas de conferencias académicas marroquíes no fue posible dentro del alcance de esta investigación.

Existe una posibilidad prácticamente equivalente de que el canal de formación en competencias de ciberseguridad de Marruecos discorra actualmente predominantemente a través de ofertas de formación de proveedores privados, como el propio Cyber Skills Lab de DataProtect examinado más arriba en *Proveedores privados*, en lugar de a través de un centro de investigación académica identificado e internacionalmente visible (confianza: baja, una inferencia a partir de la visibilidad relativa del material de proveedores privados y no de ningún dato comparativo de matriculación o resultados, que no se localizó para ninguno de los dos canales).

Grupos APT

El actor de amenazas técnicamente mejor fundamentado dentro del alcance de este capítulo es Starry Addax, documentado públicamente por Cisco Talos en abril de 2024: una campaña de spear-phishing contra defensores de derechos humanos asociados con la República Árabe Saharaui Democrática (RASD) y la causa del Sáhara Occidental, que emplea una familia de malware Android a medida, FlexStarling, que se hace pasar por la aplicación móvil de la Sahara Press Service, junto con infraestructura de captura de credenciales dirigida a Windows y un canal de mando y control basado en Firebase [149]. Es probable que Starry Addax represente una operación dotada de recursos y diseñada a medida con interés específico en el conflicto político del Sáhara Occidental, dados los propios indicadores divulgados por Talos —desarrollo de malware a medida, dominios dedicados controlados por el atacante, y la propia valoración de Talos de que los plazos

vinculados a diversos artefactos indican que la campaña apenas está comenzando (confianza: moderada); es improbable que el registro técnico de fuentes abiertas disponible permita atribuir Starry Addax a ningún gobierno concreto, dado que el propio informe de Talos no formula ninguna atribución a un Estado-nación y no se localizó ningún informe posterior que resolviera esa cuestión (confianza: baja, es decir, baja confianza en que actualmente sea responsable un juicio más firme). Si el propio Jabaroot debe caracterizarse como próximo a APT —una operación dotada de recursos, posiblemente vinculada a un informante interno de los servicios de seguridad del Estado, que emplea una fachada hacktivista— o como un actor genuinamente independiente de hacktivismo y filtración sigue siendo la cuestión de atribución individual sin resolver más importante de este capítulo, y no se resuelve aquí; las teorías rivales, y el juicio de confianza baja a moderada de que la campaña muestra características próximas a un informante interno sin confirmar ningún patrocinador concreto, se exponen en detalle más arriba en *Hacktivismo y confrontación de información* y no se repiten. Combinando ambos casos, es probable que el ciberespacio de Marruecos adyacente al Sáhara Occidental en el periodo revisado contuviera al menos dos hilos técnicamente relevantes y analíticamente separados —una herramienta de espionaje confirmada pero no atribuida, diseñada a medida, dirigida específicamente contra la sociedad civil saharauí, y una campaña de filtración y hacktivismo mucho más amplia, ruidosa y controvertida dirigida contra instituciones estatales marroquíes cuyo patrocinador, si lo hay, sigue sin confirmar por ninguna fuente forense o judicial localizada en toda esta investigación hasta la fecha (confianza: moderada sobre la separación analítica de ambos hilos, dados sus objetivos, herramientas y bases evidenciales completamente distintos).

No se localizó ninguna información dedicada de fuentes abiertas sobre una unidad cibernética ofensiva identificada de las FAR o la DGSSI que llevara a cabo operaciones atribuidas contra objetivos vinculados al Polisario o a Argelia, coherente con la carencia más amplia ya documentada más arriba en *Ciberguerra militar, guerra electrónica y C4ISR*; esta ausencia se registra como una carencia declarada y no se infiere ni como una afirmación de capacidad ni como una negación de capacidad, y es probable, según el balance de lo documentado en este capítulo, que el modelo cibernético ofensivo de Marruecos en general esté impulsado por la adquisición y no por el desarrollo propio (confianza: moderada), coherente con el patrón de adquisición de proveedores documentado más arriba en *Proveedores extranjeros*.

Dependencias clave

Este capítulo examina las dependencias digitales y de infraestructura crítica de Marruecos —los puntos de estrangulamiento físicos y lógicos a través de los cuales discurren las estructuras de conectividad, nube y propiedad de telecomunicaciones del Reino, y el grado en que cada una descansa en propiedad extranjera o suministro de proveedores extranjeros. Varios subtemas más abajo llevan carencias evidenciales genuinas en la información de fuentes abiertas, una consecuencia directa de una investigación realizada sin capacidad de búsqueda web; estas carencias se declaran explícitamente y no se rellenan con inferencias.

La conectividad de datos internacional de Marruecos se ancla en un conjunto pequeño y geográficamente concentrado de sistemas de cable submarino, y no en una malla global redundante. El cable Medusa —aproximadamente 8.700 km, 24 pares de fibra a 20 Tbit/s cada uno, liderado por el consorcio AFR-IX Telecom— toma tierra en Tetuán y Nador, con una finalización del tramo terrestre en Nador declarada para diciembre de 2025 [150], mientras que sistemas más antiguos, ACE, el cruce directo Estepona-Tetuán, Atlas Offshore (Marruecos-Francia) y EURAFRICA (Portugal-Marruecos-Francia), proporcionan los restantes enlaces directos hacia Europa y África Occidental [151]. Es probable que este conjunto de cables otorgue

a Marruecos capacidad agregada adecuada para la demanda actual (confianza: moderada), pero la concentración física de las tomas de tierra en torno al estrecho corredor del Estrecho de Gibraltar —Tetuán y Nador en el lado marroquí, la zona de Estepona/Tarifa en el lado español— es un punto de estrangulamiento estructural: una fracción significativa del ancho de banda internacional de Marruecos transita por un único segmento de estrecho históricamente propenso al arrastre de anclas, y no pudieron establecerse la propiedad del consorcio, la capacidad exacta ni las fechas de puesta en servicio de ACE, Estepona-Tetuán y Atlas Offshore más allá de los nombres de sus puntos de toma de tierra, lo que deja el panorama preciso de redundancia solo parcialmente documentado [151].

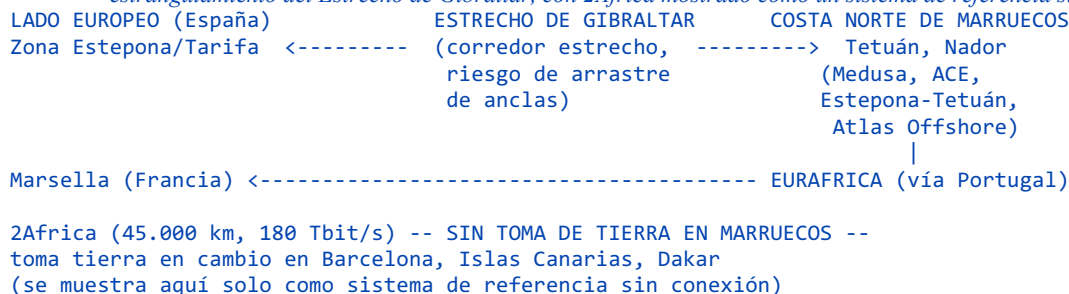
Marruecos queda, según la evidencia actual, al margen de la mayor inversión en cable transcontinental de la década: el sistema 2Africa, de 45.000 km y 180 Tbit/s, respaldado por Meta, MTN, Orange, Vodafone, China Mobile, STC, Telecom Egypt y WIOCC y declarado completo por Meta en noviembre de 2025, toma tierra en Barcelona, las Islas Canarias y Dakar, pero en ningún punto marroquí [152]. Es probable que esta ausencia de toma de tierra refleje decisiones deliberadas de enrutamiento del consorcio 2Africa y no una decisión de política marroquí (confianza: baja, dado que no se localizó ninguna declaración del consorcio sobre el motivo), pero el efecto práctico es que Marruecos no se beneficia directamente de la capacidad mayorista de acceso abierto de 2Africa y sigue dependiendo de su conjunto de cables más pequeño y antiguo para la redundancia de enrutamiento hacia África Occidental y adyacente al Atlántico —una carencia documentada de capacidad y redundancia, y no una vulnerabilidad confirmada, dado que no se halló evidencia de que el ancho de banda internacional agregado actual de Marruecos sea realmente insuficiente. La tabla y la figura siguientes reúnen este conjunto de cables para referencia.

Tabla 17. Sistemas de cable submarino que dan servicio a Marruecos, y el contraste de no toma de tierra de 2Africa.

Cable	Punto(s) de toma de tierra en Marruecos	Otras tomas de tierra	Capacidad	Consorcio/propietario	Notas/estado
Medusa	Tetuán, Nador	19 emplazamientos en el Mediterráneo/sur de Europa	~8.700 km; 24 pares de fibra a 20 Tbit/s cada uno	Consorcio liderado por AFR-IX Telecom	Tramo terrestre de Nador completado en diciembre de 2025
ACE (Africa Coast to Europe)	Nombrado como sistema con toma de tierra en Marruecos	África occidental/austral, Europa	No establecido	No establecido	La propiedad/capacidad/fecha de puesta en servicio no pudo obtenerse más allá del nombre del punto de toma de tierra
Estepona-Tetuán (cruce directo)	Tetuán	Estepona, España	No establecido	No establecido	La propiedad/capacidad/fecha de puesta en servicio no pudo obtenerse más allá del

					nombre del punto de toma de tierra
Atlas Offshore	Marruecos	Francia	No establecido	No establecido	La propiedad/capacidad/fecha de puesta en servicio no pudo obtenerse más allá del nombre del punto de toma de tierra
EURAFRICA	Marruecos	Portugal, Francia	No establecido	No establecido	La propiedad/capacidad/fecha de puesta en servicio no pudo obtenerse más allá del nombre del punto de toma de tierra
2Africa (fila de contraste — sin toma de tierra en Marruecos)	Ninguno	Barcelona, Islas Canarias, Dakar	~45.000 km; 180 Tbit/s	Meta, MTN, Orange, Vodafone, China Mobile, STC, Telecom Egypt, WIOCC	Declarado completo por Meta, noviembre de 2025; rodea a Marruecos

Figura 14. Topología de cables submarinos de Marruecos: tomas de tierra agrupadas en la costa norte frente al punto de estrangulamiento del Estrecho de Gibraltar, con 2Africa mostrado como un sistema de referencia sin conexión.



Maroc Telecom, el mayor operador fijo y móvil de Marruecos, es mayoritariamente propiedad de Etisalat by e& de los EAU desde que Vivendi vendió su participación del 53 % por aproximadamente 4.200 millones de dólares en julio de 2013, con el Estado marroquí conservando aproximadamente el 22 % y el resto en libre flotación entre las bolsas de Casablanca y París [95]. Esto sitúa al operador con la mayor huella de filiales en el continente africano —Mauritania, Gabón, Malí, Chad, Costa de Marfil y otros— bajo el control último de una entidad vinculada al Estado emiratí, casi con toda certeza un hecho y no un juicio dado el valor de la transacción de 2013, bien documentado, aunque el desglose específico del porcentaje de propiedad en sí descansa en fuentes terciarias que no pudieron confirmarse frente a una presentación primaria de la AMMC o de relaciones con inversores, habiendo devuelto ambos intentos de obtención errores de acceso [95]. Esta estructura de propiedad es analíticamente significativa menos por la operación cotidiana de la red que por la posibilidad permanente de una influencia estratégica vinculada a los EAU sobre el operador dominante de infraestructura de telecomunicaciones de Marruecos.

Orange Maroc, antiguamente Méditel y segundo operador principal de Marruecos, se reparte de forma aproximadamente equitativa entre Orange S.A. de Francia, que aumentó su participación del 40 % en 2010 (640 millones de euros) al 49 % hacia 2015, y los grupos inversores marroquíes

Finance Com y la Caisse de Dépôt et de Gestion (CDG), un inversor institucional vinculado al Estado [96]. Existe una posibilidad prácticamente equivalente de que la participación de Orange haya superado desde entonces el 49 %, dado el patrón general de consolidación de socios extranjeros observado en Maroc Telecom (confianza: baja, no se localizó ninguna actualización de 2024-2026), pero, tal como está documentado, esto deja a Orange Maroc formalmente de propiedad mayoritariamente marroquí, aunque dependiente operativa y técnicamente de la matriz corporativa francesa del Grupo Orange para los estándares de equipamiento de red, las relaciones con proveedores y el soporte técnico —una dependencia más suave y menos cuantificable que la participación mayoritaria de Etisalat en Maroc Telecom, pero real. El tercer operador de Marruecos, Inwi, antiguamente Wana Corporate, es propiedad conjunta de Al Mada, el holding vinculado a la familia real marroquí perfilado más arriba en *El Majzén* en un capítulo anterior, y del grupo kuwaití Zain Group, que adquirió una participación del 31 % en febrero de 2009 [153]; si la participación de Zain ha cambiado desde 2009 no pudo establecerse, dado que un acceso a las relaciones con inversores de Zain Group devolvió una redirección no resuelta, por lo que el porcentaje actual de propiedad del Golfo en el tercer mayor operador de Marruecos es un elemento explícitamente señalado como abierto y no un hecho zanjado.

En conjunto, los tres operadores de telecomunicaciones autorizados de Marruecos llevan un componente sustancial de propiedad no marroquí —de los EAU, Francia y Kuwait respectivamente—, lo que significa que todo el sector comercial de telecomunicaciones de Marruecos se sitúa bajo control corporativo extranjero parcial, una condición estructural distinta de, y adicional a, cualquier influencia regulatoria de un gobierno extranjero. La tabla y la figura siguientes reúnen esta estructura de propiedad para referencia rápida.

Tabla 18. Estructura de propiedad de los tres operadores de red móvil autorizados de Marruecos.

Operador	Accionista mayoritario/principal	Participación	País	Notas
Maroc Telecom (IAM)	Etisalat by e&	53 % (desde julio de 2013, transacción de ~4.200 millones de USD)	EAU	El Estado marroquí conserva ~22 %; el resto en libre flotación (bolsas de Casablanca/París)
Orange Maroc	Orange S.A.	40 % (2010), en aumento hasta el 49 % (2015)	Francia	El resto en manos de Finance Com y la Caisse de Dépôt et de Gestion (Marruecos); participación posterior a 2015 no confirmada
Inwi (Wana Corporate)	Al Mada + Zain Group	Al Mada mayoritario; Zain 31 % (desde feb. 2009)	Marruecos (Al Mada) / Kuwait (Zain)	No pudo establecerse si la participación de Zain ha cambiado desde 2009

Figura 15. Estructura de propiedad de los tres operadores de red móvil de Marruecos.

Etisalat/e& (EAU) --53%--> MAROC TELECOM <--22%-- Estado marroquí
(resto: libre flotación, bolsas de Casablanca/París)

Orange S.A. (Francia) --40-49%--> ORANGE MAROC <--resto-- Finance Com,

CDG (Marruecos)

Al Mada (Marruecos, INWI (Wana Corporate) <--31% (2009, no confirmado desde)-- Zain Group (Kuwait)

Marruecos no tiene presencia doméstica de computación en la nube a hiperescala: comprobaciones directas de las propias páginas de infraestructura de Microsoft y Google confirman que ni Azure ni Google Cloud operan una región en Marruecos, con las regiones africanas más cercanas en Sudáfrica para ambos proveedores y regiones del Golfo en los EAU, Catar y Arabia Saudí para Azure, o Arabia Saudí para Google Cloud, en su lugar [154, 155]. El mapa de red publicado de Cloudflare corrobora el mismo patrón desde el ángulo de la entrega de contenidos y la mitigación de DDoS: enumera 33 ciudades africanas pero ninguna en Marruecos ni en ningún otro lugar del norte de África [156]. Es casi seguro que cualquier carga de trabajo gubernamental, del sector financiero o empresarial marroquí alojada en un gran hiperescalador occidental reside físicamente fuera de la jurisdicción marroquí, con mayor probabilidad en un centro de datos europeo o del Golfo (confianza: alta, dado que tres fuentes corporativas oficiales independientes coinciden en la ausencia). Se trata de una dependencia fundamental de soberanía digital: la residencia de datos, la latencia del servicio en la nube y la continuidad del servicio para cualquier organización marroquí que use estos proveedores están todas condicionadas por infraestructura y jurisdicción legal fuera de Marruecos. La tabla siguiente reúne esta presencia de nube y CDN para referencia.

Tabla 19. Presencia internacional de nube a hiperescala y CDN relevante para Marruecos.

Proveedor	Región/PoP más cercana a Marruecos	Región/PoP dentro de Marruecos (S/N)	Notas
Microsoft Azure	Sudáfrica; regiones del Golfo (EAU, Catar, Arabia Saudí)	N	Ausencia confirmada mediante la propia página de infraestructura de Microsoft
Google Cloud	Sudáfrica; Arabia Saudí	N	Ausencia confirmada mediante la propia página de infraestructura de Google
Cloudflare	33 ciudades africanas enumeradas, ninguna en Marruecos/norte de África	N	Confirmado mediante el propio mapa de red publicado de Cloudflare
AWS	No establecido	No verificado	Señalado como no verificado en esta pasada de investigación

La base de proveedores de equipamiento de red móvil y fija de Marruecos —si predomina Huawei, Nokia, Ericsson, ZTE u otro proveedor— no pudo establecerse: una comprobación dirigida del propio perfil de Huawei no encontró ningún contenido específico de Marruecos en absoluto, dejando la identidad del proveedor como una carencia explícita y sin resolver, y no como un hallazgo documentado [157]. Esto importa directamente para el tema central de este informe, dado que una red dominada por Huawei plantearía consideraciones de influencia extranjera e interoperabilidad con aliados materialmente distintas, dado el escrutinio sostenido de EE. UU./la UE sobre Huawei en infraestructura crítica, que una red dominada por Nokia o Ericsson; esta

carencia debe tratarse como un elemento prioritario para investigación futura y no asumirse en ningún sentido.

La infraestructura digital de Marruecos descansa sobre una base energética que es en sí misma dependiente de las importaciones: el país se caracteriza como el mayor importador de energía del norte de África, con una producción doméstica de hidrocarburos insignificante y una combinación de generación históricamente dependiente del carbón —grandes plantas en Mohammedia y Jorf Lasfar que queman carbón importado sudafricano y polaco— aunque los objetivos de renovables aumentan hacia un 52 % declarado de la capacidad instalada para 2030 [158]. Es probable que esta dependencia de importaciones se extienda a la electricidad que en última instancia alimenta las redes de telecomunicaciones de Marruecos y cualquier futuro despliegue de centros de datos, dado que la infraestructura digital se nutre de la misma red nacional y no de un suministro acotado (confianza: moderada, una inferencia a partir de los datos de la combinación de generación y no una fuente que trate explícitamente la seguridad energética del sector de telecomunicaciones, una carencia que no pudo cerrarse aquí). La interconexión eléctrica de Marruecos a través del Estrecho con España es una dependencia relacionada y con carga propia que no pudo obtenerse en detalle para este capítulo, y debe tratarse como un requisito firme de seguimiento y no asumirse a partir de conocimiento general.

La huella de fabricación de semiconductores y hardware de Marruecos se limita al ensamblaje y las pruebas de back-end: la instalación de STMicroelectronics en Bouskoura realiza el encapsulado y las pruebas de chips, además, desde 2022, de una línea de producción de carburo de silicio para aplicaciones de vehículos eléctricos, pero no existe fabricación de obleas front-end en el país [159]. Esto casi con toda certeza se interpreta mejor como un eslabón descendente en la propia cadena de suministro de STMicroelectronics, anclada en Europa y Asia, y no como una capacidad indígena de semiconductores (confianza: alta, dado que la caracterización de solo back-end es inequívoca en la fuente), lo que significa que los sectores de telecomunicaciones y electrónica de Marruecos siguen dependiendo por completo de circuitos integrados y hardware de red importados para todo lo que exceda este estrecho nicho de ensamblaje y pruebas. Más allá de los semiconductores, no se identificó en ninguna parte del material revisado para este capítulo ningún programa nacional específico de capacidad de IA, ninguna capacidad de diseño de semiconductores (a diferencia del ensamblaje y pruebas), ningún programa de investigación en computación cuántica ni ninguna iniciativa de migración a criptografía poscuántica; esto se declara como una carencia de investigación explícita y no como evidencia de ausencia genuina, dado que la recopilación subyacente se orientó hacia fuentes de prensa y documentos regulatorios y no hacia un estudio dedicado del sector técnico, pero es no obstante un dato adicional y acumulativo dentro del mismo patrón de dependencia que esta sección documenta en todo momento.

La capacidad de reconocimiento por satélite de Marruecos —los satélites de imagen óptica Mohammed VI-A (2017) y Mohammed VI-B (2018)— fue construida enteramente por la base industrial francesa y europea, Airbus Defence and Space y Thales Alenia Space, sobre la plataforma Astrosat-1000, y lanzada en el cohete europeo Vega, con un coste total de programa reportado en torno a 500-600 millones de euros [36, 37]. Es muy probable que Marruecos no pueda mantener, reparar o sustituir esta capacidad de forma independiente sin una nueva contratación extranjera (confianza: moderada, basada en la dependencia del fabricante y del lanzador y en la ausencia de cualquier detalle fundamentado sobre el segmento terrestre o la autonomía de explotación), y la vida de diseño comparativamente corta de los satélites, de unos cinco años, significa que Marruecos se enfrenta a corto plazo a una decisión de renovación que casi con toda certeza reproducirá la misma dependencia industrial extranjera [36]. Qué institución marroquí, la DGST o la DGED, posee realmente la autoridad de asignación de tareas del satélite no pudo determinarse, una carencia señalada explícitamente y no asumida, y a la que *Modelo de capacidades* más abajo regresa directamente.

Marruecos no tiene documentada ninguna infraestructura indígena de segmento terrestre para posicionamiento, navegación y sincronización por satélite: una comprobación dirigida de los listados de segmento de control y estaciones de monitorización del GPS encontró estaciones en América, el Atlántico, Oriente Medio y Australasia, pero ninguna en Marruecos ni en el norte de África, y tampoco ninguna referencia a presencia de segmento terrestre de EGNOS o Galileo en el país [160]. Se trata de un hallazgo genuino de ausencia y no de una afirmación confirmada de inexistencia (confianza: baja sobre la ausencia absoluta, dado que no encontrar no es prueba de no existencia, aunque el hallazgo es consistente en todas las fuentes comprobadas), y significa que los servicios civiles y militares de posicionamiento, navegación y sincronización de Marruecos — usados en la sincronización de redes de telecomunicaciones, la sincronización de transacciones financieras y cualquier capacidad militar de precisión guiada— descansan enteramente en constelaciones de satélites operadas por el extranjero, sin ninguna palanca ni respaldo de segmento terrestre indígena.

Parte V. Valoración

Modelo de capacidades

La línea ofensiva y de recopilación de Marruecos combina una capacidad indígena de larga data de procesamiento de inteligencia de señales con una herramienta de intrusión enteramente de origen extranjero. La unidad Police des Communications Radioélectriques (PCR) de la DGST presuntamente intercepta miles de comunicaciones diarias y, según una descripción de la era de 2010, ejecuta búsqueda automatizada por palabras clave, análisis de llamadas por reconocimiento de voz y análisis de documentos por reconocimiento de escritura manuscrita —una capacidad indígena de procesamiento SIGINT distinta de cualquier cosa suministrada por un proveedor [161]. Superpuesta a esto, la capacidad de intrusión más trascendente documentada de Marruecos, el compromiso de dispositivos móviles mediante Pegasus, es un producto israelí enteramente comercial usado contra periodistas y activistas internos, jefes de gobierno extranjeros, incluidos Macron de Francia y Sánchez de España, y más de 6.000 números de teléfono argelinos, este último presuntamente un factor contribuyente en la ruptura de relaciones de Argelia de agosto de 2021 [147]. El organismo operador específico detrás de esta capacidad está mejor evidenciado, aunque todavía no de forma concluyente, que una carencia absoluta: la propia información de la edición en español del consorcio Forbidden Stories, examinada en detalle más arriba en *Recopilación de inteligencia y vigilancia*, nombra a la DGST y no a la DGED como el operador principal, con la DGED en un papel de mera coordinación, sobre la base de fuentes testimoniales de un único antiguo oficial de la DGST [34]. Es muy probable que la capacidad de recopilación estratégicamente más trascendente de Marruecos dependa de un proveedor y no sea indígena, y probable, con confianza de moderada a baja dada la naturaleza de fuente única de la afirmación sobre el organismo concreto, que la DGST y no la DGED sea el servicio operador (confianza: moderada sobre la dependencia de proveedor, de moderada a baja sobre la atribución específica a la DGST), lo que sitúa las propias decisiones de concesión de licencias de exportación de NSO Group y la política del gobierno israelí como una limitación externa sobre la postura cibernética ofensiva de Marruecos, con independencia de qué servicio la opere en última instancia.

La misma línea ofensiva y de recopilación se extiende al espacio: los satélites de reconocimiento óptico Mohammed VI-A/B, examinados por su dimensión de dependencia más arriba en *Dependencias clave*, otorgan a Marruecos una capacidad de imágenes que supera la de cualquier otro Estado africano en el registro de fuentes abiertas revisado [37], pero la capacidad está construida por Francia/Europa, tiene una vida de diseño corta, y su operador institucional o autoridad de asignación de tareas, la DGST frente a la DGED, no queda establecido por ninguna fuente consultada [162]. La propia DGED, el servicio de inteligencia exterior de Marruecos perfilado en detalle en un capítulo anterior —aproximadamente 4.000 efectivos según una estimación de 2003, el 60 % procedente de las Fuerzas Armadas Reales y el resto civil, con entre 250 y 300 agentes estimados en el extranjero y asociaciones orientadas hacia la DGSE francesa y el África francófona— parece, según fuentes abiertas, funcionar como una red de enlace y recopilación y no como una organización de desarrollo tecnológico [162]. En conjunto, es probable que la línea ofensiva y de recopilación de Marruecos se caracterice mejor como amplia en ambición y alcance, pero estructuralmente dependiente de hardware extranjero, proveedores extranjeros y socios industriales extranjeros en casi todas las capas técnicas (confianza: moderada). La línea defensiva de Marruecos está institucionalmente formalizada más recientemente que su aparato de recopilación: la DGSSI, examinada en detalle más arriba, publicó una Estrategia Nacional de Ciberseguridad con horizonte 2030 el 22 de julio de 2024, opera bajo la Ley 05-20 y la Ley 43-20 sobre servicios de confianza electrónicos, y gestiona maCERT como su brazo

operativo de respuesta a incidentes, que participa en ejercicios internacionales de simulación cibernética [163]. Se trata de un hallazgo directamente de fuente primaria y de alta fiabilidad sobre el mandato y la base legal de la DGSSI, pero también es limitado: la propia página principal de la DGSSI no divulga estadísticas de incidentes, ninguna cifra de presupuesto ni ningún nivel de personal, y el texto completo de la propia estrategia 2030 no pudo localizarse. Existe una posibilidad prácticamente equivalente de que la capacidad cibernética defensiva de Marruecos sea proporcional a la escala de dependencia digital documentada más arriba en *Dependencias clave* (confianza: baja, dada la ausencia casi total de datos cuantitativos de capacidad defensiva en las fuentes abiertas alcanzadas) —una carencia evidencial genuina y explícitamente señalada, y no un juicio negativo sobre la competencia real de la DGSSI.

No se localizó evidencia dedicada de fuentes abiertas sobre una línea de operaciones de información o influencia específicamente para esta sección: ninguna fuente consultada abordó campañas de desinformación vinculadas al Estado, actividad coordinada e inauténtica en redes sociales, o una doctrina de operaciones de información atribuible a una institución marroquí identificada. Esto se declara como una carencia explícita y no como una valoración de ausencia —la agencia de noticias estatal de Marruecos y el aparato mediático más amplio, y la actividad de influencia proafiliada a Rabat y proafiliada a Argelia analizada más arriba en *Hacktivismo y confrontación de información*, inciden en esta cuestión pero no se duplican aquí. La confianza en cualquier juicio sobre la escala o sofisticación de una capacidad marroquí de influencia y operaciones de información es en consecuencia baja, y debe cotejarse con el material de inteligencia y diplomático presentado en otras partes de este informe, y no afirmarse aquí sin una cita de respaldo.

Valoración de conjunto: el modelo de capacidades de tres líneas de Marruecos es asimétrico. La línea ofensiva y de recopilación es la más visible y más documentada externamente, pero es muy probable que sea estructuralmente dependiente de proveedores y socios en sus capas más trascendentes —Pegasus a través de Israel/NSO, los satélites de reconocimiento a través de Airbus y Thales de Francia, y las relaciones de enlace exterior de la DGED (confianza: moderada). La línea defensiva tiene un fundamento legal e institucional creíble y recientemente reforzado, pero su capacidad operativa real no es cuantificable a partir de las fuentes alcanzadas (confianza: baja). La línea de influencia y operaciones de información está efectivamente indocumentada dentro de esta investigación y no debe asumirse ni fuerte ni débil sin una recopilación de seguimiento dedicada (confianza: muy baja, es decir, una carencia genuina). Es probable que esta asimetría —una ofensiva visible y habilitada por el extranjero; una defensa infradocumentada e institucionalmente joven; y una capacidad de influencia no valorada— refleje un perfil de capacidad genuino y no meramente un artefacto de la investigación, dado que la visibilidad de la línea ofensiva procede sustancialmente de la exposición forense externa y no de la autodivulgación marroquí, mientras que las líneas defensiva y de operaciones de información no tienen una función de fuerza externa equivalente que impulse la divulgación (confianza: moderada). La figura siguiente presenta las tres líneas una junto a otra.

Figura 16. El modelo de capacidad cibernética de tres líneas de Marruecos: ofensiva/recopilación, defensiva, e influencia/operaciones de información, cada una anotada con su vector de dependencia extranjera dominante y su confianza evidencial.

OFENSIVA/RECOPIACIÓN	DEFENSIVA	INFLUENCIA/OI
PCR de la DGST (SIGINT indígena)	DGSSI/maCERT	Sin fuentes dedicadas localizadas en esta pasada --
+ Pegasus/NSO (Israel)	Ley 05-20/43-20,	mostrada como nodo
+ satélites Mohammed VI-A/B (Francia: Airbus/Thales)	Estrategia 2030 (fundamento	de CARENCIA DE
Autoridad de asignación de tareas (DGST vs DGED) SIN RESOLVER	institucional/legal creíble; capacidad no cuantificable)	DATOS, no una afirmación de capacidad
Dependencia dominante: Israel (Pegasus), Francia (satélites)	Dependencia dominante: ninguna identificada	Dependencia dominante:

Confianza: moderada

indígena)
Confianza: baja

Confianza: muy baja/carencia

Limitaciones y vulnerabilidades

Las instituciones de inteligencia y ciberseguridad de Marruecos están legal y organizativamente fragmentadas en al menos tres organismos con mecanismos de coordinación solo parcialmente documentados: la DGST, orientada al interior/la seguridad doméstica y sede de la unidad SIGINT PCR y del brazo de contraterrorismo BCIJ; la DGED, próxima al ministerio de defensa y orientada al exterior; y la DGSSI, un regulador nacional de ciberseguridad distinto con su propia base legal en virtud de la Ley 05-20 [161, 162, 163]. Es probable que esta división institucional tripartita genere sobrecarga de coordinación y posibles carencias de autoridad —por ejemplo, ninguna fuente establece qué organismo, si alguno, tiene autoridad de asignación de tareas sobre los satélites Mohammed VI-A/B, y el mandato defensivo de la DGSSI no se extiende evidentemente a las capacidades ofensivas documentadas más arriba en *Modelo de capacidades* (confianza: baja, dado que se trata de una inferencia a partir del silencio institucional y no de un relato directamente fundamentado en fuentes sobre fallos de coordinación).

Los presupuestos declarados de los dos servicios de inteligencia de Marruecos están ambos en el rango bajo de miles de millones de dirhams de un solo dígito y están desfasados: el presupuesto anual de la DGST se reportó en 1.100 millones de dirhams en 2016, y el de la DGED en 1.080 millones de dirhams en 2015 [161, 162]. Incluso permitiendo un probable crecimiento nominal desde que se reportaron estas cifras, es probable que el presupuesto declarado de los servicios de inteligencia de Marruecos siga siendo modesto en términos absolutos en relación con el alcance de la actividad atribuida a estos servicios —recopilación regional de SIGINT, un programa de reconocimiento por satélite, una red de enlace internacional y, a través de Pegasus, operaciones de vigilancia transnacional (confianza: baja, dado que no se localizó ninguna cifra presupuestaria consolidada actual y el panorama real de recursos puede incluir costes fuera de presupuesto o integrados en el ministerio de defensa no reflejados en estas cifras desfasadas).

La exposición de propiedad extranjera de Marruecos en su sector de telecomunicaciones, ya documentada más arriba en *Dependencias clave*, es una vulnerabilidad permanente de influencia externa por derecho propio: Etisalat mantiene una participación mayoritaria en Maroc Telecom, Orange S.A. mantiene una participación casi mayoritaria en Orange Maroc, y Zain mantiene una participación sustancial, aunque actualmente no confirmada, en Inwi [95, 96, 153]. Es probable que esta estructura de propiedad otorgue a los EAU, Francia y, en menor medida y con menor confirmación, Kuwait, cierto grado de influencia comercial permanente sobre los operadores de infraestructura de telecomunicaciones de Marruecos, con independencia de cualquier palanca regulatoria del gobierno marroquí (confianza: baja, dado que no se halló evidencia directa de que ninguno de estos Estados ejerza realmente tal influencia sobre la política de red —la vulnerabilidad es estructural y potencial, y no demostrada).

La ausencia de Marruecos de la huella global de hiperescaladores y CDN agrava esta exposición basada en la propiedad: significa que los servicios digitales marroquíes de todo tipo — gubernamentales, financieros y privados— dependen, para las cargas de trabajo alojadas en la nube, de infraestructura y jurisdicción legal fuera de Marruecos, con mayor probabilidad en Europa, el Golfo o Sudáfrica [154, 155, 156]. Es casi seguro que esto crea una exposición latente de soberanía de datos y continuidad de servicio a las decisiones políticas y legales de cualquier jurisdicción extranjera que aloje realmente la carga de trabajo en la nube de una organización marroquí determinada (confianza: moderada), aunque no pudo determinarse qué jurisdicciones concretas están realmente en uso por entidades marroquíes identificadas, lo que requeriría una

investigación a nivel de cuenta o técnica más allá de lo que puede establecer la investigación documental de fuentes abiertas.

La geografía de cables submarinos de Marruecos concentra una parte desproporcionada de la conectividad internacional del país a través del estrecho corredor del Estrecho de Gibraltar —el cruce directo Estepona-Tetuán y las tomas de tierra de Medusa en Nador/Tetuán—, un entorno físicamente limitado y de alto tráfico de buques donde el daño a cables por arrastre de anclas es una categoría de riesgo regional recurrente [150, 151]. Es probable que un incidente grave que afectara a varios cables en este corredor, accidental o deliberado, degradara materialmente la conectividad internacional de Marruecos dada la concentración documentada de puntos de toma de tierra (confianza: baja, dado que ninguna fuente cuantifica exactamente qué fracción del ancho de banda internacional marroquí transita por este corredor específico frente a las rutas de ACE, Atlas Offshore y EURAFRICA), y esto sigue siendo una carencia de cuantificación genuinamente abierta y no una suposición que este informe esté dispuesto a formular con confianza.

Ninguna fuente consultada abordó en absoluto el canal de talento de Marruecos en ciberseguridad o ingeniería de telecomunicaciones —producción universitaria, personal de la DGSSI/maCERT, o el tamaño de la fuerza de trabajo técnica del sector privado. Cualquier juicio sobre una carencia de talento marroquí en este ámbito sería pura inferencia a partir de la observación más amplia de que los propios materiales públicos de la DGSSI no divulgan cifras de personal, y este informe se abstiene de afirmar un juicio de carencia de talento sin una cita de respaldo; esto se registra como una carencia explícita y sin resolver para investigación de seguimiento dedicada, idealmente dirigida a la Agencia de Desarrollo Digital de Marruecos, datos de matriculación en programas universitarios de ciberseguridad, o informes de la ANRT sobre competencias digitales. La tabla siguiente reúne las seis limitaciones analizadas en esta sección junto con su confianza estimada, para referencia rápida.

Tabla 20. Principales limitaciones y vulnerabilidades del dominio cibernético de Marruecos, con confianza estimada.

Limitación	Naturaleza	Confianza estimada
Fragmentación institucional (DGST/DGED/DGSSI)	Sobrecarga de coordinación; autoridad de asignación de tareas satelitales poco clara	Baja
Presupuestos de inteligencia declarados, desfasados/modestos	DGST ~1.100 M MAD (2016); DGED ~1.080 M MAD (2015)	Baja
Propiedad extranjera de las telecomunicaciones	Participaciones de los EAU/Francia/Kuwait en los tres operadores	Baja
Ausencia de presencia de hiperescaladores/CDN	Exposición de soberanía de datos y continuidad de servicio	Moderada
Concentración del corredor de cables submarinos	Punto de estrangulamiento del Estrecho de Gibraltar; riesgo de arrastre de anclas	Baja
Canal de talento de ciberseguridad/telecomunicaciones indocumentado	Ninguna fuente aborda la escala de la fuerza de trabajo	Carencia (sin juicio ofrecido)

Conclusiones

Reuniendo el material sobre ciberespacio, cibercrimen, hacktivismo y dependencias examinado a lo largo de este capítulo, reaparecen cuatro hallazgos estructurales que merece la pena reafirmar

en conjunto. Primero, la postura ofensiva de Marruecos en el ciberespacio está impulsada por la adquisición y no por el desarrollo propio: no se identificó ningún APT marroquí atribuido al Estado en ningún catálogo de ciberinteligencia de amenazas monitorizado, examinado más arriba en *Grupos APT*, y sin embargo una capacidad de Pegasus confirmada forensemente y de origen comercial ha alcanzado demostrablemente a periodistas y activistas internos y, según la evidencia valorada en un capítulo anterior, a altos cargos españoles. Segundo, la arquitectura institucional defensiva de Marruecos, la DGSSI y maCERT, es integral sobre el papel —un estatuto dedicado, una estrategia 2030 publicada, la afiliación a FIRST y OIC-CERT— pero su capacidad operativa real sigue siendo no cuantificable a partir de fuentes abiertas, una carencia que este capítulo ha señalado de forma consistente en lugar de resolverla por inferencia. Tercero, el fenómeno Jabaroot ejemplifica un entorno de atribución genuinamente sin resolver en el que las explicaciones estatal, hacktivista y de informante interno permanecen todas vivas simultáneamente, y este capítulo se ha negado deliberadamente a adoptar ninguna teoría única como juicio propio. Cuarto, la infraestructura digital crítica de Marruecos —propiedad de telecomunicaciones, alojamiento en la nube, cables submarinos, satélites— está sustancialmente anclada en el extranjero, un patrón de dependencia examinado en detalle más abajo.

La infraestructura digital crítica de Marruecos está, según el balance de la evidencia reunida aquí, anclada en el extranjero en casi todas las capas de carga estructural: las tomas de tierra de cables se agrupan en un único punto de estrangulamiento físico con varios sistemas constituyentes documentados solo por nombre y no por capacidad o propiedad; los tres operadores de telecomunicaciones autorizados llevan una participación accionarial mayoritaria o casi mayoritaria extranjera, de los EAU, Francia y Kuwait respectivamente; ningún gran hiperescalador o CDN occidental opera dentro del territorio marroquí; la fabricación de semiconductores se limita al ensamblaje de back-end; el reconocimiento por satélite y su renovación a corto plazo discurren ambos a través de la base industrial francesa/europea; y los servicios de posicionamiento, navegación y sincronización no tienen segmento terrestre doméstico evidente. Es muy probable que este patrón refleje una política marroquí deliberada y de larga data de importar en lugar de nacionalizar la capacidad de infraestructura crítica y tecnología estratégica, a cambio de entradas de capital, asociación industrial y transferencia de tecnología integrada en alianzas (confianza: moderada) —pero no se encontró ningún documento de estrategia explícito del gobierno marroquí que articule esta disyuntiva como una elección consciente, por lo que el juicio descansa en la consistencia del patrón y no en una política declarada.

El modelo de capacidades que se asienta sobre esta base de dependencia está en sí mismo documentado de forma desigual, y no es desigualmente real: la línea ofensiva y de recopilación es la mejor evidenciada de las tres líneas examinadas más arriba en *Modelo de capacidades* precisamente porque su herramienta más trascendente, Pegasus, ha sido expuesta por laboratorios forenses extranjeros independientes y confirmada por gobiernos extranjeros que reportan a sus propios funcionarios como objetivos, y no porque Marruecos haya sido más transparente sobre esta línea que sobre las otras dos. Es probable que las capacidades defensivas y de operaciones de información de Marruecos sean comparablemente reales pero estructuralmente infradivulgadas, dado que la DGSSI opera bajo legislación real y una estrategia real publicada en 2024 sin una exposición forense externa equivalente frente a la que dimensionarla, y que no se localizó ninguna fuente dedicada de operaciones de influencia en absoluto (confianza: baja específicamente sobre la línea de operaciones de información, moderada sobre la premisa de infradivulgación de la línea defensiva). Este informe no debe interpretar la riqueza evidencial de la línea ofensiva como prueba de que sea la capacidad más desarrollada de Marruecos, sino solo de que es la más expuesta externamente.

El seguimiento de mayor valor individual para investigación futura, a juicio de este analista, es cerrar la carencia de verificación de propiedad y cuota de mercado —los porcentajes exactos de

accionistas de Maroc Telecom, la participación actual de Orange Maroc, el reparto actual Zain/Al Mada de Inwi, y la cuota de mercado actual por operador de la ANRT— frente a fuentes primarias de la AMMC, de relaciones con inversores o de la ANRT, y no frente a la fuente terciaria de Wikipedia a la que este capítulo se vio obligado a recurrir; una segunda carencia, de importancia comparable, es establecer la identidad del proveedor de equipamiento, Huawei frente a alternativas occidentales, en las redes móviles de Marruecos, que no pudo resolverse en absoluto aquí y que incide directamente en cualquier valoración de la exposición a influencia externa a través de las cadenas de suministro de hardware. Hasta que ambas carencias se cierren, los juicios de este capítulo que descansan en las fuentes de calificación más débil deben tratarse como supuestos de trabajo probablemente ciertos y no como hallazgos zanjados.

Referencias

Las referencias se presentan en formato ACM Reference Format, numeradas por orden de aparición en este documento. Cada entrada cierra con su clasificación OTAN/Almirantazgo: una letra (A-F) para la fiabilidad de la fuente y un dígito (1-6) para la credibilidad de la información, asignados durante la recopilación y trasladados sin alterar a este informe.

[1] Haut-Commissariat au Plan. 2024. Recensement Général de la Population et de l'Habitat 2024 (population and demographic indicators). HCP official website (2024). Recuperado el 10 de septiembre de 2026 de <https://www.hcp.ma/> [Almirantazgo: A1]

[2] Kingdom of Morocco. 2011. Constitution of the Kingdom of Morocco (English translation). Comparative Constitutions Project (constituteproject.org) (1 de julio de 2011). Recuperado el 10 de septiembre de 2026 de https://www.constituteproject.org/constitution/Morocco_2011.pdf [Almirantazgo: A1]

[3] Mohamed Chtatou. 2026. From A Morocco Of Centers To A Morocco Of Territories: The 2026 Legislative Elections And The Urgency Of A New Territorial Convergence Policy — Analysis. Eurasia Review (23 de agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.eurasiareview.com/23082026-from-a-morocco-of-centers-to-a-morocco-of-territories-the-2026-legislative-elections-and-the-urgency-of-a-new-territorial-convergence-policy-analysis/> [Almirantazgo: B2]

[4] Hespress EN. 2026. PJD's 2026 Election Platform: Key Tax and Economic Proposals. Hespress (English edition) (7 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://en.hespress.com/145034-pjd-targets-dominant-companies-with-top-corporate-tax-rate-in-election-plan.html> [Almirantazgo: B2]

[5] Oubachir (wire copy). 2025. Morocco's Gen Z protests escalate: deaths, arrests and calls for reform. BusinessMirror (3 de octubre de 2025). Recuperado el 10 de septiembre de 2026 de <https://businessmirror.com.ph/2025/10/03/moroccos-gen-z-protests-escalate-deaths-arrests-and-calls-for-reform/> [Almirantazgo: B2]

[6] Gavin Blackburn. 2025. Morocco pledges reforms as death toll from anti-government protests rises to three. Euronews (2 de octubre de 2025). Recuperado el 10 de septiembre de 2026 de <https://www.euronews.com/2025/10/02/two-killed-in-anti-government-protests-rocking-morocco> [Almirantazgo: B2]

[7] Shola Lawal. 2026. Trump says Morocco named Tiznit-Dakhla highway after him: Why it matters. Al Jazeera English (31 de julio de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.aljazeera.com/news/2026/7/31/morocco-names-tiznit-dakhla-highway-after-trump-why-it-matters> [Almirantazgo: B2]

[8] Hespress EN. 2026. US Awards \$42 Million Contract for Morocco F-16 Training Systems. Hespress (English edition) (1 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de

<https://en.hespress.com/144724-us-awards-42-million-contract-for-morocco-f-16-training-systems.html> [Almirantazgo: B2]

[9] Khadija Tachfine. 2026. Morocco and France Sign 12 Cooperation Agreements at High-Level Meeting in Rabat. Hespress (English edition) (16 de julio de 2026). Recuperado el 10 de septiembre de 2026 de <https://en.hespress.com/142030-morocco-and-france-sign-12-cooperation-agreements-at-high-level-meeting-in-rabat.html> [Almirantazgo: B2]

[10] Layan, Eloïse; Mansouri, Hicham; Vénétitay, Guillaume. 2026. While France was considering buying Pegasus, Morocco was spying on its ministers. Forbidden Stories (16 de julio de 2026). Recuperado el 10 de septiembre de 2026 de <https://forbiddenstories.org/while-france-was-considering-buying-pegasus-morocco-was-spying-on-its-ministers/> [Almirantazgo: B3]

[11] Christina Thykjaer. 2026. Crisis en Ceuta: así han evolucionado las relaciones entre España y Marruecos desde la llegada de Sánchez. Euronews (Spanish edition) (31 de julio de 2026). Recuperado el 10 de septiembre de 2026 de <https://es.euronews.com/my-europe/2026/07/31/crisis-ceuta-relaciones-entre-espana-y-marruecos-llegada-sanchez> [Almirantazgo: B2]

[12] Khadija Tachfine. 2026. Albares: There Will Never Be Any Discussion With Morocco Over Ceuta and Melilla. Hespress (English edition) (7 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://en.hespress.com/145001-albares-there-will-never-be-any-discussion-with-morocco-over-ceuta-and-melilla.html> [Almirantazgo: B2]

[13] Echarri, Carmen. 2026. Así intentan el cruce Marruecos-Ceuta cientos de subsaharianos. El Faro de Ceuta (agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://elfarodeceuta.es/asi-intentan-cruce-marruecos-ceuta-cientos-subsaharianos/> [Almirantazgo: B2]

[14] Naranjo, Antonio R.. 2026. El jefe de la Inteligencia marroquí condecorado por Marlaska irrumpe como uno de los cabecillas de la invasión a Ceuta. El Debate (9 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://www.eldebate.com/espana/20260909/jefe-inteligencia-marroqui-condecorado-marlaska-irrumpe-como-cabecillas-invasion-ceuta_456488.html [Almirantazgo: C3]

[15] unknown. 2026. La Audiencia Nacional acuerda investigar la invasión de Ceuta y alerta de una «indudable gestión favorecedora desde Marruecos». ABC (7 de septiembre de 2026 (discrepancia de fecha señalada — la marca de fecha de la URL indica 2025)). Recuperado el 10 de septiembre de 2026 de <https://www.abc.es/espana/audiencia-nacional-acuerda-investigar-invasion-ceuta-alerta-20250907144350-nt.html> [Almirantazgo: D4]

[16] Betty de G. (citing IISS and Intissar Fakir/Middle East Institute). 2026. Maroc-Algérie: «Aucun ne veut la guerre, mais les deux se préparent au pire». Bladi.net (30 de agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.bladi.net/maroc-algerie-veut-guerre-deux-preparent-pire,123454.html> [Almirantazgo: B2]

[17] unknown (wire copy). 2026. Nigeria-Morocco Gas Pipeline Approved by Ecowas. Yahoo News (26 de julio de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.yahoo.com/news/articles/ecowas-greenlights-25bn-nigeria-morocco-085428111.html> [Almirantazgo: B2]

[18] Walter Finch. 2026. Morocco 'closing military gap with Spain' with new missile arsenal. The Olive Press (7 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.theolivepress.es/spain-news/2026/09/07/morocco-military-gap-spain/> [Almirantazgo: C4]

[19] Lahcen Haddad. 2025. The Makhzen Complex: A Psychoanalytical Decoding of Algeria's Obsession with Morocco. Morocco World News (2 de julio de 2025). Recuperado el 10 de septiembre de 2026 de <https://www.moroccoworldnews.com/2025/07/223272/the-makhzen-complex-a-psychoanalytical-decoding-of-algerias-obsession-with-morocco/> [Almirantazgo: C3]

- [20] unknown (agency copy). 2026. Morocco's Makhzen shelters fugitives wanted by European justice on drug, money laundering charges. Algérie Presse Service (APS) (11 de agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.aps.dz/en/world/world/msoshb8g-morocco-s-makhzen-shelters-fugitives-wanted-by-european-justice-on-drug-money-laundering-charges> [Almirantazgo: D4]
- [21] unknown (profile page). 2026. Al Mada (company profile). Arabian Gulf Business Insight (consultado 8 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.agbi.com/industry/finance/al-mada/> [Almirantazgo: B2]
- [22] Moroccan Institute for Policy Analysis. 2026. MIPA homepage (recent publications listing, including reference to UN Security Council Resolution 2797). MIPA (consultado 8 de septiembre de 2026, listado de elementos Feb-junio de 2026). Recuperado el 10 de septiembre de 2026 de <https://mipa.institute/> [Almirantazgo: B3]
- [23] Hespress EN (with MAP). 2026. Greece's Support for Morocco's Autonomy Proposal. Hespress (English edition) (7 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://en.hespress.com/145039-greece-believes-moroccan-proposal-for-autonomy-could-be-most-feasible-solution-for-definitive-resolution-of-this-regional-conflict.html> [Almirantazgo: B2]
- [24] Mohamed Ait Elmouden. 2026. Algeria's Changing Language Signals Possible Path to Sahara Settlement. Hespress (English edition) (6 de mayo de 2026). Recuperado el 10 de septiembre de 2026 de <https://en.hespress.com/137302-algerias-changing-language-signals-possible-path-to-sahara-settlement.html> [Almirantazgo: C3]
- [25] Hespress EN (with MAP). 2026. Danish FM: Denmark and Europe Need Reliable Friend Like Morocco. Hespress (English edition) (5 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://en.hespress.com/144933-danish-fm-denemark-and-europe-need-reliable-friend-like-morocco.html> [Almirantazgo: B2]
- [26] Wikipedia contributors. 2026. General Directorate of Studies and Documentation. Wikipedia (English) (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/General_Directorate_of_Studies_and_Documentation [Almirantazgo: C3]
- [27] Wikipedia contributors. 2026. General Directorate for Territorial Surveillance. Wikipedia (English) (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/General_Directorate_for_Territorial_Surveillance [Almirantazgo: C3]
- [28] Wikipedia contributors. 2026. Direction générale de la Sûreté nationale (Maroc). Wikipedia (French) (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de [https://fr.wikipedia.org/wiki/Direction_g%C3%A9n%C3%A9rale_de_la_S%C3%BBret%C3%A9_nationale_\(Maroc\)](https://fr.wikipedia.org/wiki/Direction_g%C3%A9n%C3%A9rale_de_la_S%C3%BBret%C3%A9_nationale_(Maroc)) [Almirantazgo: C3]
- [29] Wikipedia contributors. 2026. Abdellatif Hammouchi. Wikipedia (English) (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/Abdellatif_Hammouchi [Almirantazgo: C3]
- [30] Marczak, Bill; Scott-Railton, John; McKune, Sarah; Abdul Razzak, Bahr; Deibert, Ron. 2018. Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. Citizen Lab, Munk School of Global Affairs, University of Toronto (18 de septiembre de 2018). Recuperado el 10 de septiembre de 2026 de <https://citizenlab.ca/2018/09/hide-and-peek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/> [Almirantazgo: A2]
- [31] Amnesty International Security Lab. 2020. Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools. Amnesty International (22 de junio de 2020). Recuperado el 10 de septiembre de 2026 de <https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/> [Almirantazgo: A1]

- [32] Amnesty International (Amnesty Tech / Security Lab). 2022. Morocco/Western Sahara: Activist targeted with Pegasus spyware in recent months – new evidence. Amnesty International (9 de marzo de 2022). Recuperado el 10 de septiembre de 2026 de <https://www.amnesty.org/en/latest/news/2022/03/morocco-western-sahara-activist-nso-pegasus/> [Almirantazgo: A1]
- [33] Bautista, José; Layan, Eloïse; Mansouri, Hicham; Vénétitay, Guillaume. 2026. How did Morocco become addicted to tracking down its opponents with spyware?. Forbidden Stories (16 de julio de 2026). Recuperado el 10 de septiembre de 2026 de <https://forbiddenstories.org/how-did-morocco-become-addicted-to-tracking-down-its-opponents-with-spyware/> [Almirantazgo: B2]
- [34] Bautista, José; Mansouri, Hicham. 2026. Cómo los servicios de inteligencia marroquíes habrían espiado a los agentes españoles que los formaban. Forbidden Stories (Spanish edition) (17 de julio de 2026). Recuperado el 10 de septiembre de 2026 de <https://forbiddenstories.org/es/como-los-servicios-de-inteligencia-marroquies-habrian-espiado-a-los-agentes-espanoles-que-los-formaban/> [Almirantazgo: B2]
- [35] Bautista, José; Layan, Eloïse; Mansouri, Hicham; Rueckert, Phineas; Vénétitay, Guillaume. 2026. How Morocco allegedly spies on an African ally. Forbidden Stories (16 de julio de 2026). Recuperado el 10 de septiembre de 2026 de <https://forbiddenstories.org/how-morocco-allegedly-spies-on-an-african-ally/> [Almirantazgo: B3]
- [36] Wikipedia contributors. 2026. Mohammed VI-A. Wikipedia (consultado 9 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/Mohammed_VI-A [Almirantazgo: D2]
- [37] Clark, Stephen. 2018. Moroccan spy satellite launched aboard Vega rocket. Spaceflight Now (21 de noviembre de 2018). Recuperado el 10 de septiembre de 2026 de <https://spaceflightnow.com/2018/11/21/moroccan-spy-satellite-launched-aboard-vega-rocket/> [Almirantazgo: B2]
- [38] Entrambasaguas, Alejandro. 2026. El ex 'dos' del espionaje de Marruecos que accedió a las pruebas de Pegasus vive escondido entre un piso en Madrid y una finca en Cáceres. El Debate (8 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://www.eldebate.com/espana/20260908/ex-dos-espionaje-marruecos-accedio-pruebas-pegasus-vive-escondido-entre-piso-madrid-finca-caceres_456302.html [Almirantazgo: C3]
- [39] Entrambasaguas, Alejandro. 2026. Un colaborador de la Policía pidió 2 millones a Marruecos a cambio de entregar al espía que guarda las pruebas de Pegasus. El Debate (9 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://www.eldebate.com/espana/20260909/colaborador-policia-pidio-2-millones-marruecos-cambio-entregar-espia-guarda-pruebas-pegasus_456615.html [Almirantazgo: C3]
- [40] Forbidden Stories consortium. 2026. Codename Morgan: a look back at Morocco's acquisition of Pegasus involving Israel and the United Arab Emirates. Forbidden Stories (16 de julio de 2026). Recuperado el 10 de septiembre de 2026 de <https://forbiddenstories.org/codename-morgan-a-look-back-at-moroccos-acquisition-of-pegasus-involving-israel-and-the-united-arab-emirates/> [Almirantazgo: C3]
- [41] Bautista, José; Mansouri, Hicham. 2026. Moroccan intelligence is believed to have spied on Spanish agents who were training them. Forbidden Stories (17 de julio de 2026). Recuperado el 10 de septiembre de 2026 de <https://forbiddenstories.org/moroccan-intelligence-is-believed-to-have-spied-on-spanish-agents-who-were-training-them/> [Almirantazgo: B3]
- [42] Wikipedia contributors. 2026. Espionaje con Pegasus al Gobierno de España. Wikipedia (Spanish) (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://es.wikipedia.org/wiki/Espionaje_con_Pegasus_al_Gobierno_de_Espa%C3%B1a [Almirantazgo: C3]

- [43] unknown. 2026. El fiscal jefe de la Audiencia Nacional rechazó las «pruebas» sobre el móvil de Sánchez hackeado: «No interesa por Marruecos». ABC (8 de septiembre de 2026 (discrepancia de fecha señalada — la marca de fecha de la URL indica 2025)). Recuperado el 10 de septiembre de 2026 de <https://www.abc.es/espana/fiscal-jefe-audiencia-nacional-rechazo-pruebas-sobre-20250908215738-nt.html> [Almirantazgo: D4]
- [44] Moreno Mena, Miguel. 2026. Abdellatif Hammouchi, el líder de la seguridad de Marruecos señalado por los hackers de Jabaroot y acusado de torturas al que Marlaska le dio una medalla. Infobae España (27 de agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.infobae.com/espana/2026/08/27/abdellatif-hammouchi-el-lider-de-la-seguridad-de-marruecos-senalado-por-los-hackers-de-jabaroot-y-acusado-de-torturas-al-que-marlaska-le-dio-una-medalla/> [Almirantazgo: B3]
- [45] Faouzi, Adil. 2026. Morocco's Security Pole Denies Any Database Breach, Points to Old Insurance Data. Morocco World News (27 de agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.moroccoworldnews.com/2026/08/336320/moroccos-security-pole-denies-any-database-breach-points-to-old-insurance-data/> [Almirantazgo: C3]
- [46] Wikipedia contributors. 2026. Sûreté Nationale (Morocco). Wikipedia (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de [https://en.wikipedia.org/wiki/Sûreté_Nationale_\(Morocco\)](https://en.wikipedia.org/wiki/Sûreté_Nationale_(Morocco)) [Almirantazgo: C3]
- [47] Wikipedia contributors. 2026. Bureau Central d'Investigations Judiciaires. Wikipedia (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/Bureau_Central_d%27Investigations_Judiciaires [Almirantazgo: C3]
- [48] Wikipedia contributors. 2026. Royal Moroccan Gendarmerie. Wikipedia (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/Royal_Moroccan_Gendarmerie [Almirantazgo: C3]
- [49] Wikipedia contributors. 2026. Forces auxiliaires marocaines. Wikipédia (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://fr.wikipedia.org/wiki/Forces_auxiliaires_marocaines [Almirantazgo: C3]
- [50] Echarri, Carmen. 2026. Imágenes de las detenciones a subsaharianos en Marruecos. El Faro de Ceuta (agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://elfarodeceuta.es/imagenes-detenciones-subsaharianos-marruecos/> [Almirantazgo: B2]
- [51] Wikipedia contributors. 2026. Wali (arabe). Wikipédia (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de [https://fr.wikipedia.org/wiki/Wali_\(arabe\)](https://fr.wikipedia.org/wiki/Wali_(arabe)) [Almirantazgo: C3]
- [52] Wikipedia contributors. 2026. Direction générale de la sûreté nationale. Wikipédia (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://fr.wikipedia.org/wiki/Direction_g%C3%A9n%C3%A9rale_de_la_s%C3%BBret%C3%A9_nationale [Almirantazgo: C3]
- [53] Moho Amer, Oumaima. 2026. Morocco's Public Security Director El Hail Zitouni Dies After Four-Decade Career. Morocco World News (agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.moroccoworldnews.com/2026/08/335634/moroccos-public-security-director-el-hail-zitouni-dies-after-four-decade-career/> [Almirantazgo: B2]
- [54] Afeznaoui, Hanane. 2026. Agadir Security Directorate Launches Morocco's Eighth Regional Explosives Unit. Morocco World News (agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.moroccoworldnews.com/2026/08/336307/agadir-security-directorate-launches-moroccos-eighth-regional-explosives-unit/> [Almirantazgo: B3]
- [55] Afeznaoui, Hanane. 2026. DGSN Deploys AI-Powered 'Amane' and 'Madar' Smart Patrols in Casablanca. Morocco World News (julio de 2026). Recuperado el 10 de septiembre de 2026 de

- <https://www.moroccoworldnews.com/2026/07/331326/dgsn-deploys-ai-powered-amane-and-madar-smart-patrols-in-casablanca/> [Almirantazgo: B3]
- [56] INTERPOL. 2026. Morocco — Member Countries. INTERPOL (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.interpol.int/en/Who-we-are/Member-countries/Africa/MOROCCO> [Almirantazgo: A1]
- [57] Naim, Firdaus. 2025. Morocco-Spain Operation Seizes 22 Tons of Hashish Hidden in Pepper Trucks. Morocco World News (octubre de 2025). Recuperado el 10 de septiembre de 2026 de <https://www.moroccoworldnews.com/2025/10/265741/> [Almirantazgo: B2]
- [58] Direction Générale de la Sûreté Nationale (traced by Wikimedia Commons uploader). 2022. File:Emblem of the Moroccan DGSN.svg. Wikimedia Commons (10 de noviembre de 2022). Recuperado el 10 de septiembre de 2026 de https://commons.wikimedia.org/wiki/File:Emblem_of_the_Moroccan_DGSN.svg [Almirantazgo: B3]
- [59] Machloukh, Anass. 2021. Haboub Cherkaoui, patron du BCIJ: 'Le Polisario est un important pourvoyeur de Djihadistes'. L'Opinion (Maroc) (octubre de 2021). Recuperado el 10 de septiembre de 2026 de https://www.lopinion.ma/Haboub-Cherkaoui-patron-du-BCIJ-Le-polisario-est-un-important-pourvoyeur-de-Djihadistes_a35872.html [Almirantazgo: C4]
- [60] Wikipedia contributors. 2026. Bureau central d'investigations judiciaires. Wikipédia (abril de 2026). Recuperado el 10 de septiembre de 2026 de https://fr.wikipedia.org/wiki/Bureau_central_d%E2%80%99investigations_judiciaires [Almirantazgo: C3]
- [61] MWN Staff. 2026. BCIJ Dismantles ISIS-Affiliated Cell Involved in Criminal Operations Across Morocco. Morocco World News (abril de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.moroccoworldnews.com/2026/04/286037/bcij-dismantles-isis-affiliated-cell-involved-in-criminal-operations-across-morocco/> [Almirantazgo: B3]
- [62] Kasraoui, Safaa. 2024. Morocco-Spain Dismantle ISIS-Affiliated Terror Cell Spanning Two Continents. Morocco World News (noviembre de 2024). Recuperado el 10 de septiembre de 2026 de <https://www.moroccoworldnews.com/2024/11/168105/morocco-spain-dismantle-isis-affiliated-terror-cell-spanning-two-continents/> [Almirantazgo: B3]
- [63] NorthAfricanArmsDealer (Wikimedia Commons uploader). 2022. File:Blazon du BCIJ.svg. Wikimedia Commons (19 de noviembre de 2022 (created); 29 de noviembre de 2022 (uploaded)). Recuperado el 10 de septiembre de 2026 de https://commons.wikimedia.org/wiki/File:Blazon_du_BCIJ.svg [Almirantazgo: D4]
- [64] Wikipedia contributors. 2026. Gendarmerie royale marocaine. Wikipedia (French) (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://fr.wikipedia.org/wiki/Gendarmerie_royale_marocaine [Almirantazgo: F3]
- [65] Wikipedia contributors. 2026. Forces armées royales (Maroc). Wikipedia (French) (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de [https://fr.wikipedia.org/wiki/Forces_arm%C3%A9es_royales_\(Maroc\)](https://fr.wikipedia.org/wiki/Forces_arm%C3%A9es_royales_(Maroc)) [Almirantazgo: F3]
- [66] Jiménez, Isabel. 2025. Interceptada una lancha con inmigrantes de Bangladesh que cruzaba a Ceuta. El Faro de Ceuta (octubre de 2025). Recuperado el 10 de septiembre de 2026 de <https://elfarodeceuta.es/interceptada-lancha-inmigrantes-bangladesh-cruzaba-ceuta/> [Almirantazgo: B2]
- [67] Hespress EN. 2026. Moroccan Gendarmes Seize Over Three Tonnes of Cocaine off Tarfaya. Hespress (English edition) (julio de 2026). Recuperado el 10 de septiembre de 2026 de <https://en.hespress.com/142551-moroccan-gendarmes-seize-over-three-tonnes-of-cocaine-off-tarfaya.html> [Almirantazgo: B3]
- [68] Hespress EN. 2025. Casablanca Court Deliberates Verdict in Case of 37 Gendarmerie Officers Accused of Collusion with Drug Trafficker. Hespress (English edition) (marzo de 2025).

Recuperado el 10 de septiembre de 2026 de <https://en.hespress.com/105477-casablanca-court-deliberates-verdict-in-case-of-37-gendarmerie-officers-accused-of-collusion-with-drug-trafficker.html> [Almirantazgo: C3]

[69] Hespress EN. 2025. Seven Gendarmes Jailed in Morocco Over Alleged Cover-Up for Drug Baron Linked to Murder. Hespress (English edition) (enero de 2025). Recuperado el 10 de septiembre de 2026 de <https://en.hespress.com/100511-seven-gendarmes-jailed-in-morocco-over-alleged-cover-up-for-drug-baron-linked-to-murder.html> [Almirantazgo: C3]

[70] Daoudi, Asmae. 2025. Agadir Authorities Launch Investigation into Lqliaa Gendarmerie Post Incident. Morocco World News (octubre de 2025). Recuperado el 10 de septiembre de 2026 de <https://www.moroccoworldnews.com/2025/10/261422/agadir-authorities-launch-investigation-lqliaa-gendarmerie-post-incident/> [Almirantazgo: C4]

[71] Testomania (Wikimedia Commons uploader). 2025. File:Royal Moroccan gendarmery.png. Wikimedia Commons (10 de mayo de 2025). Recuperado el 10 de septiembre de 2026 de https://commons.wikimedia.org/wiki/File:Royal_Moroccan_gendarmery.png [Almirantazgo: D4]

[72] Mesfioui, Khalid. 2018. Voici les détails du plan royal pour moderniser les Forces auxiliaires. Le360 (French edition) (enero de 2018). Recuperado el 10 de septiembre de 2026 de <https://fr.le360.ma/politique/voici-les-detaills-du-plan-royal-pour-moderniser-les-forces-auxiliaires-152697/> [Almirantazgo: B2]

[73] Ministère de la Transformation Numérique et de la Réforme de l'Administration. 2018. Textes juridiques — Décrets n° 2.17.827 et 2.17.825 du 6 mars 2018. mmsp.gov.ma (marzo de 2018). Recuperado el 10 de septiembre de 2026 de https://www.mmsp.gov.ma/fr/textes-juridiques?field_type_textes_juridiques_target_id=All&page=21 [Almirantazgo: A1]

[74] Boudarham, Mohammed. 2020. Info360. Voici les deux nouveaux patrons des Forces auxiliaires. Le360 (French edition) (octubre de 2020). Recuperado el 10 de septiembre de 2026 de <https://fr.le360.ma/politique/info360-voici-les-deux-nouveaux-patrons-des-forces-auxiliaires-225667/> [Almirantazgo: B2]

[75] Inspection Générale des Forces Auxiliaires (via mobaraty.com). 2023. File:Forces Auxiliaires.png. Wikimedia Commons (19 de junio de 2023). Recuperado el 10 de septiembre de 2026 de https://commons.wikimedia.org/wiki/File:Forces_Auxiliaires.png [Almirantazgo: B3]

[76] MINURSO. 2026. MINURSO home page. United Nations Mission for the Referendum in Western Sahara (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://minurso.unmissions.org/> [Almirantazgo: A1]

[77] Wikipedia contributors. 2026. Royal Moroccan Armed Forces. Wikipedia (English) (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/Royal_Moroccan_Armed_Forces [Almirantazgo: F3]

[78] Wikipedia contributors. 2026. Ahmed Dlimi. Wikipedia (French) (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://fr.wikipedia.org/wiki/Ahmed_Dlimi [Almirantazgo: F3]

[79] Aminovich (Wikimedia Commons uploader). 2008. File:Moroccan Armed Force.png. Wikimedia Commons (29 de enero de 2008). Recuperado el 10 de septiembre de 2026 de https://commons.wikimedia.org/wiki/File:Moroccan_Armed_Force.png [Almirantazgo: C3]

[80] Wikipedia contributors. 2026. Direction générale de la surveillance du territoire. Wikipedia (French) (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://fr.wikipedia.org/wiki/Direction_g%C3%A9n%C3%A9rale_de_la_surveillance_du_territoire [Almirantazgo: F3]

[81] Wikipedia contributors. 2026. Direction générale des études et de la documentation. Wikipedia (French) (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://fr.wikipedia.org/wiki/Direction_g%C3%A9n%C3%A9rale_des_%C3%A9tudes_et_de_la_documentation [Almirantazgo: F3]

- [82] Wikipedia contributors. 2026. Garde royale marocaine. Wikipedia (French) (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://fr.wikipedia.org/wiki/Garde_royale_marocaine [Almirantazgo: F3]
- [83] Garde Royale (via vuseen.com). 2023. File:Moroccan Royal Guard.png. Wikimedia Commons (19 de junio de 2023). Recuperado el 10 de septiembre de 2026 de https://commons.wikimedia.org/wiki/File:Moroccan_Royal_Guard.png [Almirantazgo: B3]
- [84] Wikipedia contributors. 2026. Berm (Western Sahara). Wikipedia (English) (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de [https://en.wikipedia.org/wiki/Berm_\(Western_Sahara\)](https://en.wikipedia.org/wiki/Berm_(Western_Sahara)) [Almirantazgo: F3]
- [85] Security Council Report. 2025. Western Sahara Monthly Forecast, octubre de 2025. Security Council Report (octubre de 2025). Recuperado el 10 de septiembre de 2026 de <https://www.securitycouncilreport.org/monthly-forecast/2025-10/western-sahara-16.php> [Almirantazgo: B1]
- [86] Hespress. 2026. المغرب يحشد دعم 40 دولة للحكم الذاتي. Hespress (8 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.hespress.com/%d8%a7%d9%84%d9%85%d8%ba%d8%b1%d8%a8-%d9%8a%d8%ad%d8%b4%d8%af-%d8%af%d8%b9%d9%85-40-%d8%af%d9%88%d9%84%d8%a9-%d9%84%d9%84%d8%ad%d9%83%d9%85-%d8%a7%d9%84%d8%b0%d8%a7%d8%aa%d9%8a-1803928.html> [Almirantazgo: B2]
- [87] R. N.. 2026. Equal Earth de l'ONU : une victoire cartographique historique pour le peuple sahraoui. El Watan (7 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://elwatan.dz/equal-earth-de-lonu-une-victoire-cartographique-historique-pour-le-peuple-sahraoui/> [Almirantazgo: B3]
- [88] Hammouche, Sid Ahmed. 2026. Grande victoire du peuple sahraoui. El Watan (8 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://elwatan.dz/grande-victoire-du-peuple-sahraoui/> [Almirantazgo: B3]
- [89] Boufertih, Toufiq. 2026. مسيرة مغربية تقصف منقبين بالصحراء. Hespress (8 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.hespress.com/%d9%85%d8%b3%d9%8a%d8%b1%d8%a9-%d9%85%d8%ba%d8%b1%d8%a8%d9%8a%d8%a9-%d8%aa%d9%82%d8%b5%d9%81-%d9%85%d9%86%d9%82%d8%a8%d9%8a%d9%86-%d8%a8%d8%a7%d9%84%d8%b5%d8%ad%d8%b1%d8%a7%d8%a1-1804049.html> [Almirantazgo: B4]
- [90] Wikipedia contributors. 2026. Ministry of Interior (Morocco). Wikipedia (consultado septiembre de 2026 (artículo actualizado 6 de julio de 2026)). Recuperado el 10 de septiembre de 2026 de [https://en.wikipedia.org/wiki/Ministry_of_Interior_\(Morocco\)](https://en.wikipedia.org/wiki/Ministry_of_Interior_(Morocco)) [Almirantazgo: C3]
- [91] Human Rights Watch. 2004. Morocco: Human Rights at a Crossroads. Human Rights Watch (octubre de 2004). Recuperado el 10 de septiembre de 2026 de <https://www.hrw.org/report/2004/10/20/morocco-human-rights-crossroads> [Almirantazgo: B2]
- [92] Institut Royal des Études Stratégiques (IRES). 2026. IRES — official institutional site. IRES (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.ires.ma/> [Almirantazgo: A2]
- [93] Wikipedia contributors. 2026. Abdellatif Hammouchi. Wikipedia (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/Abdellatif_Hammouchi [Almirantazgo: C3]
- [94] Amnesty International Security Lab. 2021. Forensic Methodology Report: How to Catch NSO Group's Pegasus. Amnesty International (1 de julio de 2021). Recuperado el 10 de septiembre de 2026 de <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/> [Almirantazgo: B2]

- [95] Wikipedia contributors. 2026. Maroc Telecom. Wikipedia (consultado 9 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/Maroc_Telecom [Almirantazgo: D3]
- [96] Wikipedia contributors. 2026. Orange Maroc. Wikipedia (consultado 9 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/Orange_Maroc [Almirantazgo: D3]
- [97] Marczak, Bill; Scott-Railton, John; Berdan, Kristin; Abdul Razzak, Bahr; Deibert, Ron. 2020. Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles. Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto (1 de diciembre de 2020). Recuperado el 10 de septiembre de 2026 de <https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/> [Almirantazgo: B2]
- [98] Wikipedia contributors. 2026. Hacking Team. Wikipedia (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/Hacking_Team [Almirantazgo: C3]
- [99] Royaume du Maroc. 2020. Dahir n° 1-20-69 du 4 hija 1441 (25 juillet 2020) portant promulgation de la loi n° 05-20 relative à la cybersécurité. Bulletin Officiel n° 6906 (hosted by DGSSI) (6 de agosto de 2020). Recuperado el 10 de septiembre de 2026 de <http://www.dgssi.gov.ma/sites/default/files/legislative/brochure/2023-03/loi%2005-20.pdf> [Almirantazgo: A1]
- [100] Aziz Akhannouch (Chef du Gouvernement, signatory). 2024. Décret n° 2-24-921 du 18 rabii II 1446 (22 octobre 2024) relatif au recours aux prestataires de services Cloud par les entités et les infrastructures d'importance vitale. Bulletin Officiel du Royaume du Maroc (hosted via dgssi.gov.ma) (22 de octubre de 2024 (BO N°7380, 20 de febrero de 2025)). Recuperado el 10 de septiembre de 2026 de <https://www.dgssi.gov.ma/sites/default/files/legislative/brochure/2025-04/DECREE%202.24.921%20FR%20.pdf> [Almirantazgo: A1]
- [101] Wikipedia contributors. 2026. École nationale supérieure d'informatique et d'analyse des systèmes. Wikipédia (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://fr.wikipedia.org/wiki/%C3%89cole_nationale_sup%C3%A9rieure_d%27informatique_et_d%27analyse_des_syst%C3%A8mes [Almirantazgo: C3]
- [102] Wikipedia contributors. 2026. University Mohammed VI Polytechnic. Wikipedia (consultado septiembre de 2026 (artículo actualizado 11 de agosto de 2026)). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/University_Mohammed_VI_Polytechnic [Almirantazgo: C3]
- [103] Wikipedia contributors. 2026. International University of Rabat. Wikipedia (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/International_University_of_Rabat [Almirantazgo: C3]
- [104] Direction Générale de la Sécurité des Systèmes d'Information (DGSSI). 2026. DGSSI — official institutional site (training and education section). DGSSI (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <http://www.dgssi.gov.ma/fr/> [Almirantazgo: A2]
- [105] Naim, Firdaus. 2025. Sidi Ifni Maritime Interdiction: Hashish and Irregular-Migration Boat Intercepted. Morocco World News (agosto de 2025). Recuperado el 10 de septiembre de 2026 de <https://www.moroccoworldnews.com/2025/08/249194/> [Almirantazgo: C3]
- [106] Constitute Project. 2011. Morocco's Constitution of 2011. Constitute Project (29 de julio de 2011 (consultado septiembre de 2026)). Recuperado el 10 de septiembre de 2026 de https://www.constituteproject.org/constitution/Morocco_2011 [Almirantazgo: A1]
- [107] Wikisource contributors. 2011. Constitution marocaine de 2011/Titre III : De la Royauté. Wikisource (29 de julio de 2011 (consultado septiembre de 2026)). Recuperado el 10 de septiembre de 2026 de

- https://fr.wikisource.org/wiki/Constitution_marocaine_de_2011/Titre_III:_De_la_Royaut%C3%A9 [Almirantazgo: A1]
- [108] Privacy International. 2019. State of Privacy: Morocco. Privacy International (enero de 2019). Recuperado el 10 de septiembre de 2026 de <https://www.privacyinternational.org/state-privacy/1007/state-privacy-morocco> [Almirantazgo: B2]
- [109] Wikipedia contributors. 2026. Bureau central d'investigation judiciaire. Wikipédia (consultado septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://fr.wikipedia.org/wiki/Bureau_central_d%27investigation_judiciaire [Almirantazgo: C3]
- [110] Wikipedia contributors. 2026. Telecommunications in Morocco. Wikipedia (English) (consultado 8-9 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/Telecommunications_in_Morocco [Almirantazgo: F3]
- [111] Agence Nationale de Réglementation des Télécommunications (ANRT). 2026. Observatoires du secteur au titre du T1 2026. anrt.ma (26 de junio de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.anrt.ma/> [Almirantazgo: A1]
- [112] Le360 (avec MAP). 2026. Législatives 2026: la CNDP fixe les règles sur l'usage des données personnelles. Le360 (29 de agosto de 2026). Recuperado el 10 de septiembre de 2026 de https://fr.le360.ma/politique/legislatives-2026-la-cndp-fixe-les-regles-sur-lusage-des-donnees-personnelles_6ROWMYG5TRC7FCNJVDY6PNLXA4/ [Almirantazgo: B2]
- [113] CNDP (institutional). 2026. Les dix impératifs à respecter durant les opérations et les consultations électorales (communiqué). cndp.ma (31 de agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.cndp.ma/> [Almirantazgo: A1]
- [114] DGSSI (institutional). 2021. Guide d'homologation des systèmes d'information sensibles des infrastructures d'importance vitale. dgssi.gov.ma (9 de noviembre de 2021). Recuperado el 10 de septiembre de 2026 de <https://www.dgssi.gov.ma/fr/publications/guide-dhomologation-des-systemes-dinformation-sensibles-des-infrastructures> [Almirantazgo: A1]
- [115] DGSSI (institutional). 2023. Référentiel de gestion des incidents de cybersécurité. dgssi.gov.ma (5 de mayo de 2023). Recuperado el 10 de septiembre de 2026 de <https://www.dgssi.gov.ma/fr/publications/referentiel-de-gestion-des-incidents-de-cybersecurite> [Almirantazgo: A1]
- [116] DGSSI (institutional). 2024. Stratégie Nationale de Cybersécurité 2030. dgssi.gov.ma (22 de julio de 2024). Recuperado el 10 de septiembre de 2026 de <https://www.dgssi.gov.ma/fr/publications/strategie-nationale-de-cybersecurite> [Almirantazgo: A2]
- [117] DGSSI (institutional). 2026. DGSSI homepage (mission, structure, legal basis). dgssi.gov.ma (consultado 8 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <http://www.dgssi.gov.ma/fr/> [Almirantazgo: A1]
- [118] DGSSI / maCERT (institutional). 2026. maCERT — mandate and service catalogue. dgssi.gov.ma (consultado 8 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <http://www.dgssi.gov.ma/fr/macert/> [Almirantazgo: A1]
- [119] Hespress (French edition). 2026. Cybersécurité: le Maroc classé 43e mondial sur 155 pays en 2026. Hespress (French edition) (18 de agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://fr.hespress.com/485544-cybersecurite-le-maroc-classe-43e-mondial-sur-155-pays-en-2026.html> [Almirantazgo: B2]
- [120] Direction Générale de la Sécurité des Systèmes d'Information. 2026. DGSSI — site officiel (page d'accueil et logo institutionnel). dgssi.gov.ma (8 de septiembre de 2026 (consultado)). Recuperado el 10 de septiembre de 2026 de <https://www.dgssi.gov.ma/> [Almirantazgo: A1]
- [121] Forum of Incident Response and Security Teams (FIRST). 2026. maCERT — Member Team Page. first.org (8 de septiembre de 2026 (consultado)). Recuperado el 10 de septiembre de 2026 de <https://www.first.org/members/teams/macert> [Almirantazgo: B2]

[122] INCIBE-CERT (institutional). 2025. Data Leak on Moroccan Institutions Increases Political Tensions with Algeria. INCIBE-CERT Cybersecurity Highlights (9 de abril de 2025). Recuperado el 10 de septiembre de 2026 de <https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/data-leak-moroccan-institutions-increases-political-tensions-algeria> [Almirantazgo: A1]

[123] Amnesty International Security Lab. 2026. Inside Pegasus: The evolution of the world's most notorious spyware. Amnesty International Security Lab (julio de 2026). Recuperado el 10 de septiembre de 2026 de <https://securitylab.amnesty.org/latest/2026/07/inside-pegasus-the-evolution-of-the-worlds-most-notorious-spyware/> [Almirantazgo: A1]

[124] Consejo General del Poder Judicial (institutional). 2026. Audiencia Nacional — Noticias Judiciales (rolling listing). poderjudicial.es (consultado 8 de septiembre de 2026 (elementos 2 July-7 de septiembre de 2026)). Recuperado el 10 de septiembre de 2026 de <https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Audiencia-Nacional/Noticias-Judiciales/> [Almirantazgo: A1]

[125] Alejandro Entrambasaguas. 2026. El ex 'dos' del espionaje de Marruecos que accedió a las pruebas de Pegasus vive escondido entre un piso en Madrid y una finca en Cáceres. El Debate (8 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://www.eldebate.com/espana/20260908/ex-dos-espionaje-marruecos-accedio-pruebas-pegasus-vive-escondido-entre-piso-madrid-finca-caceres_456302.html [Almirantazgo: C3]

[126] Amnesty International et al. (joint statement). 2026. Joint Statement: Pegasus in the Parliament — the EU Must Act Now. Amnesty International Security Lab (6 de julio de 2026). Recuperado el 10 de septiembre de 2026 de <https://securitylab.amnesty.org/latest/2026/07/joint-statement-pegasus-in-the-parliament-the-eu-must-act-now/> [Almirantazgo: B2]

[127] Manuel García Castellón. 2026. La sombra de Pegasus sobre Ceuta (Opinion). El Independiente (3 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.elindependiente.com/opinion/2026/09/03/la-sombra-de-pegasus-sobre-ceuta/> [Almirantazgo: D4]

[128] Wikipedia contributors. 2026. Royal Moroccan Air Force. Wikipedia (English) (consultado 8 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/Royal_Moroccan_Air_Force [Almirantazgo: F3]

[129] Hespess (institutional). 2021. La cybercriminalité: Un phénomène menaçant que la DGSN prend très au sérieux. Hespess (French edition) (25 de diciembre de 2021). Recuperado el 10 de septiembre de 2026 de <https://fr.hespess.com/240008-la-cybercriminalite-un-phenomene-menacant-que-la-dgsn-prend-tres-au-serieux.html> [Almirantazgo: B2]

[130] Le360 (institutional). 2026. Cybercriminalité: un célèbre hacker arrêté au Maroc, lors d'une opération conjointe entre la DGSN et Interpol. Le360 (undated (2009-2018 offending window referenced)). Recuperado el 10 de septiembre de 2026 de <https://fr.le360.ma/societe/cybercriminalite-un-celebre-hacker-arrete-au-maroc-lors-dune-operation-conjointe-entre-la-dgsn-et-241581/> [Almirantazgo: B2]

[131] Le360 (institutional). 2022. Cybercriminalité: recherché par Interpol, un hacker interpellé à Casablanca. Le360 (event dated 18 de octubre de 2022). Recuperado el 10 de septiembre de 2026 de <https://fr.le360.ma/societe/cybercriminalite-recherche-par-interpol-un-hacker-interpelle-a-casablanca-268785/> [Almirantazgo: B2]

[132] Perspectives Med (institutional). 2026. Cybercriminalité: Le Maroc s'implique dans la lutte menée par Interpol. Perspectives Med (20 de mayo de 2026). Recuperado el 10 de septiembre de 2026 de <https://perspectivesmed.com/cybercriminalite-le-maroc-simplique-dans-la-lutte-menee-par-interpol/> [Almirantazgo: C3]

[133] Infomag (institutional). 2026. Kaspersky alerta sur la rapidité des fraudes au Maroc. InfoMagazine Maroc (16 de junio de 2026). Recuperado el 10 de septiembre de 2026 de

<https://www.infomagazine.ma/cybersecurite/kaspersky-alerte-sur-la-rapidite-des-fraudes-au-maroc-15586-2026/> [Almirantazgo: C2]

[134] Estrella Digital (institutional). 2026. JabaROOT hackea RAMED: datos de 17 millones de marroquíes. Estrella Digital (20 de agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.estrelladigital.es/articulo/ciberseguridad/jabaroot-hackea-ramed-datos-17-millones-marroquies/20260820013152450106.html> [Almirantazgo: E4]

[135] Wikipedia contributors. 2026. Jabaroot. Wikipedia (Spanish) (consultado 8 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://es.wikipedia.org/wiki/Jabaroot> [Almirantazgo: F3]

[136] Lucas Barreiro. 2026. 70.000 nombres en juego: la amenaza que golpea al aparato de inteligencia de Marruecos. Catalunya Press (20 de agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.catalunyapress.es/articulo/internacional/2026-08-20/5989486-70000-nombres-juego-amenaza-golpea-aparato-inteligencia-marruecos>

[Almirantazgo: C3]

[137] ESdiario (citing journalist Ketty Garat). 2026. Ketty Garat revela los datos del espionaje de Pegasus a Sánchez vinculados a Marruecos. ESdiario (8 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://esdiario.com/nacional/260908/197171/ketty-garat-sanchez-pegasus-marruecos.html> [Almirantazgo: D4]

[138] TSA — Tout sur l'Algérie (relaying Le Monde). 2026. Jabaroot: la piste algérienne s'efface, d'ex-espions marocains derrière la fuite de 70.000 noms d'agents. TSA (Tout sur l'Algérie) (27 de agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.tsa-algerie.com/jabaroot-la-piste-algerienne-sefface-dex-espions-marocains-derriere-la-fuite-de-70-000-noms-dagents/> [Almirantazgo: E4]

[139] Morocco World News (institutional). 2026. Morocco's Security Pole Denies Any Database Breach, Points to Old Insurance Data. Morocco World News (agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.moroccoworldnews.com/2026/08/336320/moroccos-security-pole-denies-any-database-breach-points-to-old-insurance-data/> [Almirantazgo: C3]

[140] CybelAngel (institutional). 2025. Our Investigation of the ANCFCC Data Leak (Flash Report). CybelAngel (5 de junio de 2025). Recuperado el 10 de septiembre de 2026 de <https://cybelangel.com/blog/ancfcc-data-leak-flash-report/> [Almirantazgo: B2]

[141] Betty de G.. 2025. Des hackers marocains ripostent à l'Algérie avec une attaque ciblée. Bladi.net (12 de abril de 2025). Recuperado el 10 de septiembre de 2026 de <https://www.bladi.net/hackers-marocains-ripostent-algerie-attaque-ciblee,114181.html>

[Almirantazgo: F3]

[142] ECSaharaui (institutional). 2026. Telegram cierra el canal de los hackers Jabaroot tras la identificación de 70.000 espías marroquíes. ECSaharaui (agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://ecsaharaui.com/08/2026/telegram-cierra-el-canal-de-los-hackers-jabaroot-tras-la-identificacion-de-70-000-espias-marroquies/> [Almirantazgo: F4]

[143] Escudo Digital (institutional). 2026. From Pegasus to JabaROOT: Inside the Undeclared Cyber Warfare Between Spain and Morocco. Escudo Digital (21 de agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.escudodigital.com/en/latest-reports/from-pegasus-to-jabaroot-inside-the-undeclared-cyber-warfare-between-spain-and-morocco.html> [Almirantazgo: C2]

[144] Ali Attar. 2026. Fuite Jabaroot: le Maroc et ses partenaires sécuritaires africains fragilisés. Afrik.com (25 de agosto de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.afrik.com/fuite-jabaroot-le-maroc-et-ses-partenaires-securitaires-africains-fragilises>

[Almirantazgo: C3]

- [145] FIRST (institutional). 2026. FIRST Members (team directory). FIRST.org (consultado 8 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.first.org/members/teams/> [Almirantazgo: A1]
- [146] DataProtect (institutional). 2026. DataProtect homepage (service catalogue). dataprotect.ma (consultado 8 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.dataprotect.ma/> [Almirantazgo: C2]
- [147] Wikipedia contributors. 2026. Pegasus (spyware). Wikipedia (consultado 9 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de [https://en.wikipedia.org/wiki/Pegasus_\(spyware\)](https://en.wikipedia.org/wiki/Pegasus_(spyware)) [Almirantazgo: D2]
- [148] Fatima Gomez. 2026. El arsenal de espionaje de Marruecos más allá de Pegasus. Merca2.es (18 de julio de 2026). Recuperado el 10 de septiembre de 2026 de <https://www.merca2.es/2026/07/18/arsenal-espionaje-marruecos-pegasus-2420008/> [Almirantazgo: E4]
- [149] Cisco Talos. 2024. Starry Addax targets human rights defenders in North Africa with new malware. Cisco Talos Intelligence Blog (9 de abril de 2024). Recuperado el 10 de septiembre de 2026 de <https://blog.talosintelligence.com/starry-addax/> [Almirantazgo: A1]
- [150] Medusa Submarine Cable System (AFR-IX Telecom-led consortium). 2026. Medusa Submarine Cable System — official project site. medusascs.com (undated, consultado 8 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://medusascs.com/> [Almirantazgo: B2]
- [151] Wikipedia contributors. 2026. List of international submarine communications cables. Wikipedia (consultado 9 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/List_of_international_submarine_communications_cables [Almirantazgo: D3]
- [152] Wikipedia contributors. 2026. 2Africa. Wikipedia (consultado 9 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://en.wikipedia.org/wiki/2Africa> [Almirantazgo: D2]
- [153] Wikipedia contributors. 2026. Inwi. Wikipedia (consultado 9 de septiembre de 2026 (el artículo indica última actualización mayo de 2026)). Recuperado el 10 de septiembre de 2026 de <https://en.wikipedia.org/wiki/Inwi> [Almirantazgo: D3]
- [154] Microsoft Corporation. 2026. Azure global infrastructure — geographies. Microsoft Azure (official corporate page) (consultado 9 de septiembre de 2026 (página en vivo)). Recuperado el 10 de septiembre de 2026 de <https://azure.microsoft.com/en-us/explore/global-infrastructure/geographies/> [Almirantazgo: B2]
- [155] Google LLC. 2026. Google Cloud locations. Google Cloud Platform (official corporate page) (consultado 9 de septiembre de 2026 (página en vivo)). Recuperado el 10 de septiembre de 2026 de <https://cloud.google.com/about/locations> [Almirantazgo: B2]
- [156] Cloudflare, Inc.. 2026. Cloudflare network map. Cloudflare (official corporate page) (consultado 9 de septiembre de 2026 (página en vivo)). Recuperado el 10 de septiembre de 2026 de <https://www.cloudflare.com/network/> [Almirantazgo: B2]
- [157] Wikipedia contributors. 2026. Huawei. Wikipedia (consultado 9 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://en.wikipedia.org/wiki/Huawei> [Almirantazgo: F6]
- [158] Wikipedia contributors. 2026. Energy in Morocco. Wikipedia (consultado 9 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/Energy_in_Morocco [Almirantazgo: D2]
- [159] Wikipedia contributors. 2026. STMicroelectronics. Wikipedia (consultado 9 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://en.wikipedia.org/wiki/STMicroelectronics> [Almirantazgo: D2]

- [160] Wikipedia contributors. 2026. Global Positioning System. Wikipedia (consultado 9 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/Global_Positioning_System [Almirantazgo: D6]
- [161] Wikipedia contributors. 2026. General Directorate for Territorial Surveillance. Wikipedia (consultado 9 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de https://en.wikipedia.org/wiki/General_Directorate_for_Territorial_Surveillance [Almirantazgo: D3]
- [162] Wikipedia contributors. 2026. DGED. Wikipedia (consultado 9 de septiembre de 2026). Recuperado el 10 de septiembre de 2026 de <https://en.wikipedia.org/wiki/DGED> [Almirantazgo: D3]
- [163] DGSSI (Direction Générale de la Sécurité des Systèmes d'Information). 2024. Publication de la Stratégie Nationale de Cybersécurité à l'horizon 2030 (DGSSI homepage). dgssi.gov.ma (22 de julio de 2024 (page consultado 9 de septiembre de 2026)). Recuperado el 10 de septiembre de 2026 de <http://www.dgssi.gov.ma/fr/> [Almirantazgo: A2]

Acrónimos

Para referencia rápida, los acrónimos empleados a lo largo de este informe se desarrollan como sigue: AMDIE, Agence Marocaine de Développement des Investissements et des Exportations; AMMC, Autorité Marocaine du Marché des Capitaux; ANCFCC, Agence Nationale de la Conservation Foncière, du Cadastre et de la Cartographie; ANRT, Agence Nationale de Réglementation des Télécommunications; APEBI, Fédération Marocaine des Technologies de l'Information, des Télécommunications et de l'Offshoring; APT, Amenaza Persistente Avanzada (Advanced Persistent Threat); AUSIM, Association des Utilisateurs des Systèmes d'Information au Maroc; BCIJ, Bureau Central d'Investigations Judiciaires; BNPI, Brigade Nationale de la Police Judiciaire; C4ISR, Mando, Control, Comunicaciones, Informática, Inteligencia, Vigilancia y Reconocimiento (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance); CDG, Caisse de Dépôt et de Gestion; CERT, Equipo de Respuesta ante Emergencias Informáticas (Computer Emergency Response Team); CGEM, Confédération Générale des Entreprises du Maroc; CGPJ, Consejo General del Poder Judicial (España); CJEU, Tribunal de Justicia de la Unión Europea (Court of Justice of the European Union); CNDP, Commission Nationale de contrôle de la protection des Données à caractère Personnel; CNI, Centro Nacional de Inteligencia (España); CNIE, Carte Nationale d'Identité Électronique; CNOPS, Caisse Nationale des Organismes de Prévoyance Sociale; CNSS, Caisse Nationale de Sécurité Sociale; CSIRT, Equipo de Respuesta a Incidentes de Seguridad Informática (Computer Security Incident Response Team); DDoS, Denegación de Servicio Distribuida (Distributed Denial-of-Service); DGED, Direction Générale des Études et de la Documentation; DGSN, Direction Générale de la Sûreté Nationale; DGSSI, Direction Générale de la Sécurité des Systèmes d'Information; DGST, Direction Générale de la Surveillance du Territoire; FAR, Forces Armées Royales; FIRST, Forum of Incident Response and Security Teams; GCI, el Índice Mundial de Ciberseguridad de la UIT (Global Cybersecurity Index); GSI-GR, Groupement de Sécurité et d'Intervention de la Gendarmerie Royale; IAM, Itissalat Al-Maghrib (Maroc Telecom); IIV, Infrastructures d'Importance Vitale (infraestructura vital); INCIBE, Instituto Nacional de Ciberseguridad (España); IXP, Punto de Intercambio de Internet (Internet Exchange Point); maCERT, Morocco Computer Emergency Response Team; MGPTT, Mutuelle Générale des Postes et Télécommunications (fondo mutual de trabajadores postales y de telecomunicaciones de Argelia); MINURSO, Mission des Nations Unies pour l'Organisation d'un Référendum au Sahara Occidental; NARSA, Agence Nationale de la Sécurité Routière; NCSI, el Índice Nacional de

Ciberseguridad (de la Academia Estonia de Gobernanza Electrónica); OIC-CERT, Organisation of Islamic Cooperation Computer Emergency Response Team; PCR, Police des Communications Radioélectriques; PEGA, la comisión de investigación del Parlamento Europeo sobre el uso de Pegasus y programas espía de vigilancia equivalentes; PJD, Parti de la Justice et du Développement (Partido de la Justicia y el Desarrollo); PKI, Infraestructura de Clave Pública (Public Key Infrastructure); PNT, Posicionamiento, Navegación y Sincronización (Positioning, Navigation and Timing); RASCOM, Regional African Satellite Communication Organization; SCADA, Control de Supervisión y Adquisición de Datos (Supervisory Control and Data Acquisition); SIGINT, Inteligencia de Señales (Signals Intelligence); y SRBM, Système des Règlements Bruts du Maroc.



Sede S2GRUPO
Calle Luis Merelo y Mas,
6, 46023 Valencia
S2grupo.com

/s2grupo
LinkedIn
Instagram
Facebook
X