INFORME DE PAÍS · BRANDEFENSE COUNTRY REPORT · SPAIN 2026 · TLP:CLEAR · 98 MIN DE LECTURA

Brandefense Informe sobre el Panorama de Ciberamenazas de España 2026

Datos de clientes, extorsión y fraude con cuentas bancarias en una economía grande y digital

TRANSLATED WITH AI

Esta edición se ha traducido con IA a partir del texto original en inglés. En caso de diferencia, prevalece la edición en inglés.

POR
Odin by Brandefense

REVISADO
21 de noviembre de 2026

TIEMPO DE LECTURA
98 min de lectura

EDICIÓN
Versión 1.0 · Public Research Edition · TLP:CLEAR

PERIODO DE INVESTIGACIÓN
1 de enero-20 de noviembre de 2026

163 de 250
organizaciones tenían una credencial anunciada a la venta el día de la comprobación

87 %
de las publicaciones etiquetadas con España procedía de una familia de bots en turco

30
incidentes que afectaron a organizaciones o clientes españoles, confirmados por la organización o por una autoridad

220
entradas de ransomware en sitios de filtraciones sobre España, 1 de enero-20 de noviembre de 2026

CONTENIDO

01 Resumen ejecutivo
Mapa del informe
02 El contexto digital y de amenazas de España
03 Exposición nacional: 250 organizaciones destacadas
04 Lo que vemos en la dark web
05 Incidentes confirmados y reivindicaciones por sector
06 Hacktivismo y DDoS
07 Actores de amenaza
08 La economía del fraude
09 Análisis en profundidad: banca y finanzas
10 Regulación y respuesta nacional
11 Perspectivas
12 Plan de acción
A Anexo A. Método
B Anexo B. Registro de evidencias
C Anexo C. Fuentes
D Anexo D. Glosario
Acerca de este informe

CAPÍTULO 1

Resumen ejecutivo

01

ESTE CAPÍTULO RESPONDE

¿Qué ocurrió en 2026, qué es lo más importante para las organizaciones españolas y qué deben decidir primero sus directivos?

4

decisiones para directivos, cada una vinculada a evidencias de los capítulos

EN ESTE CAPÍTULO

Cuatro decisiones para directivos | El año en cifras

EN RESUMEN

En 2026, el panorama español gira en torno a datos y dinero de clientes. Grandes marcas confirmaron incidentes con datos de clientes; cuatro empezaron en un proveedor. Los grupos de extorsión publicaron 220 entradas sobre España, más que en todo 2025, como en los países vecinos. Lo más anunciado en el mercado clandestino son cuentas bancarias para el fraude. Una oleada DDoS prorrusa en febrero fue ruidosa y breve. Por orden: valide los anuncios vigentes, exija avisos de brecha a los proveedores y refuerce transferencias y respuesta DDoS.

Este informe combina tres fuentes de datos propias de Brandefense con información pública verificada. **Brandefense Blackhole** aportó 932.584 publicaciones etiquetadas como relativas a España. El 87 % procede de una familia de bots en turco, y el rango depurado es de 58.657-62.086 publicaciones relevantes. También aportó registros de dispositivos y credenciales de 250 organizaciones, y tarjetas vistas en texto claro en publicaciones. **Ransompedia** aportó las entradas de sitios de filtraciones de ransomware de España y de tres países de comparación. **Atlas** calificó a las 250 organizaciones. Son poblaciones distintas y nunca se suman.

1. Las entradas de extorsión subieron, en línea con la región, repartidas entre muchos grupos. Ransompedia registra 220 entradas aceptadas sobre España del periodo 1 de enero-20 de noviembre de 2026, ya más que las 157 de todo 2025. Portugal, Italia y Francia también superaron sus totales de 2025 dentro del mismo año parcial, y por márgenes mayores, así que el aumento no parece exclusivo de España.

Encabezan la lista Qilin (49), The Gentlemen (26) y Deadlock (14), pero otros 50 nombres de grupo suman el 60 % de las entradas. Se nombró a ayuntamientos, un gobierno autonómico, universidades y un hospital; varios confirmaron un incidente y otros no. Una entrada es una reivindicación, no una prueba de cifrado o robo. [S1]

2. La exposición de identidad es casi universal en las 250 organizaciones evaluadas. De ellas, 241 tienen asociaciones con dispositivos infectados, al menos 1,2 millones en total. Y 243 tienen registros históricos de credenciales, 11,6 millones en total. En conjunto, 163 de las 250 organizaciones tenían una credencial anunciada a la venta en el momento de la comprobación. La mayoría de los dispositivos quedan fuera de la clasificación de empleados; lo más plausible es que sean de clientes, aunque no está establecido. [S2][S3]

3. Marcas de consumo confirmaron incidentes con datos de clientes, algunos a través de proveedores. Organizaciones o autoridades confirmaron 30 incidentes que afectaron a organizaciones o clientes españoles. Endesa (enero) y Naturgy (mayo) expusieron datos identificativos y de contacto y, en el caso de algunos clientes, datos bancarios. Tras la intrusión en Adif y Renfe (septiembre), Renfe avisó de que pudieron quedar expuestos DNI, contraseñas con hash y viajes. Cuatro de los 30 empezaron en un proveedor actual o anterior. No se confirmaron las cifras de los atacantes, como «20 millones de personas». [S4][S5][S6]

4. El comercio de cuentas bancarias es la familia delictiva más anunciada. Tras la depuración, el comercio de cuentas bancarias y de pago es la mayor parte de las publicaciones sobre España (alrededor del 37 %), por delante de tarjetas, filtraciones de datos y documentos de identidad. El número de publicaciones mide la publicidad, no el valor del comercio. Los canales en español venden cuentas ya abiertas, «cargas» de dinero y cuentas mula. La policía desarticuló en 2026 varias redes de suplantación bancaria y de blanqueo de capitales. [S3][S7][S8]

5. Una oleada DDoS prorrusa afectó a sitios públicos en febrero; después llegó el reclutamiento. NoName057(16) y Server Killers reivindicaron ataques contra sitios web de la Administración central y de ministerios, un parlamento autonómico, ayuntamientos y sitios de transporte entre el 16

y el 21 de febrero. Las interrupciones fueron breves. Los mismos canales reivindicaron accesos a paneles de control industrial y pidieron a ciudadanos españoles datos sobre personal de defensa.

La policía detuvo en marzo a un presunto colaborador de grupos prorrusos (anunciado en julio). En una operación anunciada en noviembre detuvo al presunto principal instigador de NoName057(16) en España. Por otra parte, en febrero fueron detenidos miembros del grupo nacional Anonymous Fénix. [S9][S10]

6. El espionaje usó temas del Gobierno español, según investigaciones de proveedores. Recorded Future vincula, con confianza moderada, una campaña de 2025-2026 a BlueDelta (que se solapa con APT28). Su primer señuelo imitaba el orden del día de una reunión de un ministerio español. ESET informó de que Webworm, un grupo que describe como alineado con China, atacó a organismos del Gobierno español. Ninguno apareció en los datos de sitios de filtraciones y foros que consultamos. [S11][S12]

Cuatro decisiones para directivos

1. **Trate los anuncios vigentes de credenciales como detonante de un incidente.** Derive cada anuncio vigente vinculado a sus dominios al equipo de identidad y registre una resolución en un plazo de 5 días hábiles. Escale el caso si encuentra una cuenta activa sin autenticación multifactor (MFA) (§3.4, §12.1).
2. **Exija a los proveedores plazos de aviso de brechas.** Cuatro de los 30 incidentes confirmados en 2026 empezaron en un proveedor. Pregunte a cada proveedor que custodie datos de sus clientes con qué rapidez le avisará, para poder cumplir su propio plazo de notificación del RGPD, y ensáyelo con él (§5.8, §10.5).
3. **Rompa la cadena del fraude en las transferencias y los cambios de SIM.** Los bancos deberían añadir fricción a las primeras transferencias a nuevos beneficiarios y a los patrones de «cuenta segura». Las operadoras deberían reforzar los cambios de SIM, y todos deberían informar a sus centros de atención al cliente (§8, §12.1).
4. **Prepárese para oleadas DDoS ruidosas y breves.** Acuerde antes de la próxima oleada quién activa la mitigación en el proveedor o el filtrado geográfico por tiempo limitado, y quién habla durante una caída (§6.6).

El año en cifras

220
Entradas de ransomware aceptadas en Ransompedia para España, 1 ene-20 nov 2026 (157 en 2025)

QUÉ NO ES
No prueban cifrado ni robo de datos

932.584
Publicaciones de Blackhole etiquetadas como España, 1 ene-20 nov 2026

QUÉ NO ES
No son ataques; el 87 % procede de bots en turco

58.657-62.086
publicaciones relevantes tras la depuración (un rango, no dos recuentos)

QUÉ NO ES
No son incidentes ni ofertas únicos

30
incidentes con organizaciones o clientes españoles, confirmados por la organización o una autoridad

QUÉ NO ES
No es un recuento completo

250
organizaciones públicas y privadas destacadas evaluadas con calificaciones de Atlas

QUÉ NO ES
No es una muestra aleatoria ni una estimación de prevalencia nacional

1.217.865
asociaciones de dispositivos infectados con esos 250 dominios (límite inferior; 46.895 de empleados), acumuladas a 21 nov 2026

QUÉ NO ES
No son solo de 2026 ni infecciones actuales verificadas

11.610.286
registros históricos de credenciales de los mismos dominios

QUÉ NO ES
No son cuentas únicas ni contraseñas activas

163 de 250
organizaciones con una credencial anunciada a la venta en el momento de la comprobación

QUÉ NO ES
No es un recuento de cuentas ni de brechas confirmadas

759
tarjetas distintas atribuidas a España vistas en texto claro en las publicaciones recopiladas

QUÉ NO ES
No es una cifra de pérdidas por fraude; alcance limitado (§8.2)

Mapa del informe

Doce capítulos, cinco itinerarios de lectura. Empiece por la fila que corresponda a su función; cada capítulo empieza con la pregunta que responde, y los capítulos 2-12 terminan con tres conclusiones.

Consejo y alta dirección

¿Qué pasó, cuánta exposición tenemos y qué debemos decidir?

IR A 1 3 5 12

CISO y responsables de seguridad

¿Qué exposiciones son nuestras, qué actores importan y qué controles van primero?

IR A 3 5 6 7 10 12

SOC e inteligencia de amenazas

¿Qué publicaron los actores, cómo se relacionan y qué técnicas usó el espionaje?

IR A 4 6 7 12 Anexo A-B

Fraude y protección del cliente

¿Cómo se comercia con identidades, cuentas y tarjetas españolas, y dónde lo ven los bancos?

IR A 4 8 9

Comunicación y jurídico

¿Cómo hablar de reivindicaciones no verificadas y qué normas se aplican ahora?

IR A 5 6 10 12

01 **Resumen ejecutivo**
Qué pasó en 2026 y qué deben decidir primero los directivos

02 **Contexto**
Qué rasgos de España determinan las amenazas

03 **Exposición nacional**
Cómo califica Atlas a 250 organizaciones destacadas

04 **Dark web**
Qué publican los delincuentes sobre España más allá del ruido de bots

05 **Incidentes**
Qué incidentes se confirmaron y cuáles son solo reivindicaciones

06 **Hacktivismo**
Qué se reivindicó, qué se confirmó y cómo prepararse

07 **Actores de amenaza**
Quiénes son los actores, cómo se relacionan y qué dicen las fuentes

08 **Economía del fraude**
Cómo se convierten identidades y cuentas en dinero

09 **Banca**
Dónde está la exposición visible de los bancos

10 **Regulación**
Qué normas se aplican mientras llega la NIS2

11 **Perspectivas**
Para qué prepararse y qué cambiaría el plan

12 **Plan de acción**
Quién hace qué en 90 días

CAPÍTULO 2

El contexto digital y de amenazas de España

ESTE CAPÍTULO RESPONDE

¿Qué rasgos de España determinan las amenazas de este informe?

96,8 %

de penetración de internet, con 65,1 millones de conexiones móviles

EN ESTE CAPÍTULO

2.1 Una población grande y conectada
2.2 Muchas administraciones, muchos sistemas
2.3 Un objetivo frecuente de reivindicaciones con encuadre político
2.4 Unas elecciones al final del periodo
2.5 Una ley de ciberseguridad todavía pendiente
2.6 Cifras nacionales de incidentes

EN RESUMEN

Cuatro rasgos definen el panorama de amenazas de España en 2026. Una población grande y digital tiene datos de identidad y bancarios que se pueden revender. Las administraciones autonómicas y locales gestionan muchos sistemas separados. Actores que invocan cuestiones de política exterior, sobre todo el apoyo español a Ucrania, reivindicaron ataques DDoS breves contra sitios españoles. Y la nueva ley de ciberseguridad sigue pendiente. Planifique a la vez para el fraude de identidad, las brechas en proveedores y las ráfagas DDoS breves.

2.1 Una población grande y conectada

España tenía 46,3 millones de usuarios de internet en octubre de 2026, una penetración del 96,8 %. Tenía 65,1 millones de conexiones móviles (136 % de la población) y 40,5 millones de identidades de usuario en redes sociales [S13]. Casi todos los adultos tienen un número de identidad (DNI o NIE) y un número de cuenta bancaria (IBAN). Ambos figuran en registros de suministros, telecomunicaciones, comercio y servicios públicos. Esto ayuda a explicar por qué tantos incidentes de 2026 de este informe afectan a registros de clientes y no a servidores cifrados.

2.2 Muchas administraciones, muchos sistemas

El sector público español se reparte entre la Administración central, 17 comunidades autónomas, dos ciudades autónomas, las diputaciones provinciales y más de 8.000 municipios. Cada nivel gestiona sus propios sitios web, sedes electrónicas, plataformas tributarias y escolares y proveedores. En 2026 encontramos incidentes confirmados en un ministerio, un gobierno autonómico, un servicio de salud autonómico, una autoridad portuaria y varios ayuntamientos (capítulo 5). En nuestra lectura, el patrón sigue la arquitectura. Las administraciones más pequeñas, con menos personal y conectadas a proveedores de software compartidos, son objetivos atractivos para la extorsión.

2.3 Un objetivo frecuente de reivindicaciones con encuadre político

El CERT del Centro Criptológico Nacional (CCN-CERT) publicó su informe *Ciberamenazas y Tendencias* 2025, del que se informó en julio de 2026. En él situó a España en tercer lugar entre los países más afectados por la actividad hacktivista [S14]. El informe vincula el aumento a campañas contra miembros de la OTAN y países que apoyan a Ucrania. En mayo, la Secretaría General del Centro Nacional de Inteligencia (CNI) afirmó que España es uno de los países más ciberatacados, y citó el ransomware, el espionaje y las actividades de influencia [S15]. Recogemos ambas como valoraciones oficiales, no como mediciones propias.

En nuestros datos de 2026, las reivindicaciones con encuadre político contra objetivos españoles procedieron sobre todo de grupos DDoS prorrusos. Un número menor se enmarcó en torno a Palestina (capítulo 6). Estos grupos describen sus propios motivos. Este informe cita esas descripciones como reivindicaciones y no toma posición sobre ellas.

2.4 Unas elecciones al final del periodo

El Real Decreto 806/2026 disolvió las Cortes Generales el 6 de octubre y convocó elecciones generales para el 29 de noviembre de 2026, nueve días después de nuestra fecha de corte [S16]. La campaña electoral empezó el 13 de noviembre. El Ministerio del Interior activó una red para anticipar riesgos como ciberataques y desinformación en torno a la votación [S17]. Las organizaciones que gestionan sitios de información pública o medios pueden tomar el periodo como contexto de planificación para ráfagas DDoS breves y phishing de temática electoral. Es una hipótesis de planificación, no una previsión.

2.5 Una ley de ciberseguridad todavía pendiente

España aún no ha transpuesto la Directiva NIS2 de la UE, cuyo plazo vencía el 17 de octubre de 2024. El 8 de julio de 2026, la Comisión Europea llevó a España, junto con Irlanda, Francia y los Países Bajos, ante el Tribunal de Justicia y pidió sanciones económicas [S18]. El anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, publicado en enero de 2025, no se había presentado a las Cortes Generales a nuestra fecha de corte [S19]. El capítulo 10 expone lo que sigue vigente y lo que las organizaciones deberían hacer ahora.

2.6 Cifras nacionales de incidentes

El Instituto Nacional de Ciberseguridad (INCIBE) gestionó 122.223 incidentes en 2025, un 26 % más que en 2024. Entre ellos hubo 55.411 casos de malware (392 de ellos de ransomware) y 45.445 casos de fraude en línea, de los que 25.133 fueron phishing. Gestionó 401 incidentes en operadores esenciales, el 34 % de ellos en banca [S20]. La agencia de ciberseguridad de Cataluña contabilizó 6.544 incidentes en 2025 en organismos y entidades públicas de la Generalitat, casi el doble que el año anterior [S21]. Son recuentos de casos gestionados, no tasas de prevalencia, y ambos organismos cuentan de forma distinta.

CONCLUSIONES CLAVE

01

Los datos de identidad y bancarios españoles son el hilo común de los incidentes de 2026 en todos los sectores.

02

Las administraciones pequeñas y sus proveedores compartidos son un punto de entrada recurrente.

03

La NIS2 aún no es ley en España, así que las obligaciones dependen de las normas vigentes y de los reguladores sectoriales.

CAPÍTULO 3

Exposición nacional: 250 organizaciones destacadas

ESTE CAPÍTULO RESPONDE

¿Cuánta exposición tienen las 250 principales organizaciones públicas y privadas de España cuando se califican como Brandefense Atlas califica a un cliente, y qué deben atender primero?

163 de 250

organizaciones tenían una credencial anunciada a la venta el día de la comprobación

EN ESTE CAPÍTULO

3.1 Ficha del universo
3.2 Señales de exposición por sector
3.3 Dispositivos y credenciales
3.4 Anuncios vigentes de credenciales: lo primero que hay que priorizar
3.5 Dominios similares, documentos expuestos y menciones
3.6 Higiene del correo y de la web

EN RESUMEN

Evaluamos 250 organizaciones españolas destacadas con las calificaciones de exposición de Brandefense Atlas. En conjunto, 163 de las 250 tenían una credencial anunciada a la venta al comprobarlo. Casi todas tienen dispositivos infectados y registros históricos de credenciales asociados a sus dominios. La cifra principal nacional de Atlas es 66 sobre 100. Uno de cada tres dominios no aplica DMARC. Priorice los anuncios vigentes, después los dispositivos de empleados y luego la autenticación del correo.

3.1 Ficha del universo

Elemento	Definición
Población	250 organizaciones: 72 de la Administración pública (organismos centrales, autonómicos y municipales), 27 de educación (universidades), 25 de banca y finanzas (bancos y empresas de pago), 21 de comercio y grupos empresariales, 18 de transporte y logística, 16 de fabricación e industria, 15 de medios y entretenimiento (incluido el deporte), 14 de energía y servicios públicos, 11 de seguros, 11 de sanidad, 10 de telecomunicaciones y 10 de hostelería y turismo. 122 de titularidad pública, 107 privadas y 21 extranjeras o mixtas
Selección	Intencional: ministerios y agencias de la Administración central, todos los gobiernos de las comunidades autónomas, los mayores ayuntamientos, los bancos supervisados por el BCE o el Banco de España, la infraestructura de pagos, las empresas públicas, el IBEX y los líderes de mercado. Seleccionadas por tamaño o papel sistémico, no ordenadas por ingresos
Unidad	Un dominio principal por organización. Los 250 resuelven en DNS (21 de noviembre de 2026)
Mediciones	Dispositivos infectados y dispositivos de empleados, registros de bases de datos de brechas, de registros de stealers y de combolists, menciones en chats y foros de la dark web, dominios similares, documentos expuestos y anuncios vigentes en mercados de credenciales; además, resultados públicos de DNS, TLS y cabeceras HTTP
Fecha	Recuentos leídos el 21 de noviembre de 2026. Los recuentos de dispositivos, credenciales y anuncios incluyen todos los registros disponibles en esa fecha, sea cual sea su fecha de captura (acumulados, no solo de 2026). Las menciones cubren los 365 días anteriores; los dominios similares, los últimos 30 días
Sin deduplicar	Ni entre fuentes, ni entre organizaciones, ni entre personas. Una persona puede aparecer en varias fuentes; un dispositivo puede contener inicios de sesión de varias organizaciones
No representativo	Los resultados describen esta lista. No son tasas de prevalencia nacional

3.2 Señales de exposición por sector

Cada organización recibió una calificación de exposición de Atlas de 0 (ningún riesgo observado) a 100. La cifra principal nacional de Atlas para las 250 organizaciones es 66. Este informe no publica calificaciones sectoriales; la tabla muestra recuentos medidos por sector.

Términos usados aquí.

Término	Significado
Cifra principal nacional	La cifra única de Atlas para toda la lista de 250, en la misma escala de 0-100
Anuncio vigente	Una credencial vinculada al dominio a la venta en el momento de la comprobación
Historial de anuncios	Una credencial vinculada al dominio se ofreció en algún momento anterior

Las credenciales y los dispositivos infectados son casi universales; dos de cada tres organizaciones tenían un anuncio vigente de credenciales

Cuota de organizaciones de cada sector con la señal. Los anuncios vigentes de credenciales se muestran en coral.

	Dispositivos infectados	Dispositivos de empleados	Registros de credenciales	Anuncio vigente	Historial de anuncios	Dominios similares (30 días)	Documentos expuestos
Seguros (11)	100%	91%	100%	91%	91%	91%	91%
Educación (27)	100%	96%	100%	85%	81%	96%	89%
Hostelería y turismo (10)	100%	100%	100%	80%	80%	100%	90%
Medios y entretenimiento (15)	100%	100%	100%	80%	80%	87%	93%
Telecomunicaciones (10)	90%	80%	100%	80%	60%	80%	80%
Comercio y grupos empresariales (21)	95%	95%	100%	76%	76%	100%	95%
Banca y finanzas (25)	100%	76%	100%	68%	68%	92%	80%
Sanidad (11)	91%	82%	91%	64%	45%	73%	64%
Transporte y logística (18)	100%	100%	100%	61%	56%	56%	78%
Energía y servicios públicos (14)	100%	86%	100%	57%	50%	79%	71%
Administración pública (72)	93%	79%	92%	51%	50%	96%	69%
Fabricación e industria (16)	94%	81%	100%	38%	0%	75%	88%

Fuente: Brandefense Atlas y asociaciones de Blackhole para 250 organizaciones, leídas el 21 de noviembre de 2026 [S2]. Los registros son acumulados, no solo de 2026.

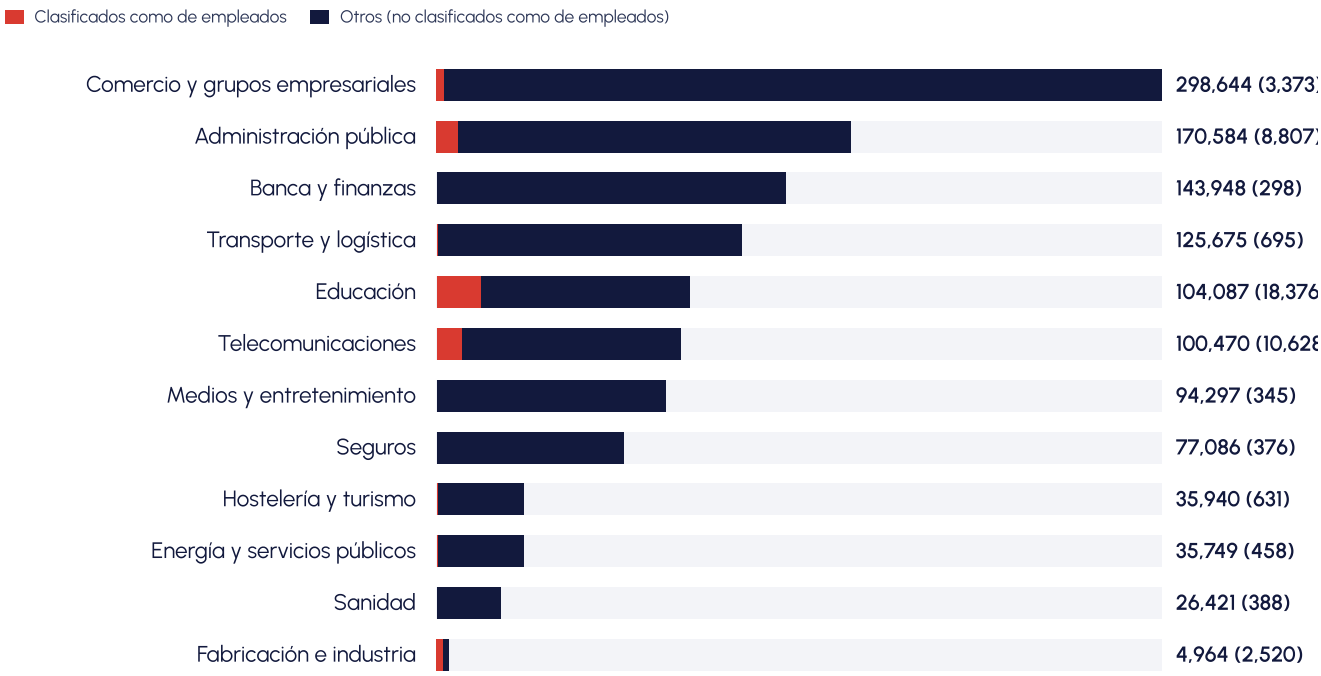
Sector	Org.	Org. con anuncio vigente de credenciales	Org. con historial de anuncios	Org. con dispositivos de empleados	Org. con do
Administración pública	72	37	36	57	
Educación	27	23	22	26	
Banca y finanzas	25	17	17	19	

Sector	Org.	Org. con anuncio vigente de credenciales	Org. con historial de anuncios	Org. con dispositivos de empleados	Org. con do
Comercio y grupos empresariales	21	16	16	20	
Transporte y logística	18	11	10	18	
Fabricación e industria	16	6	0	13	
Medios y entretenimiento	15	12	12	15	
Energía y servicios públicos	14	8	7	12	
Seguros	11	10	10	10	
Sanidad	11	7	5	9	
Telecomunicaciones	10	8	6	8	
Hostelería y turismo	10	8	8	10	
Las 250	**250**	**163**	**149**	**217**	

Cómo leer la tabla. Los anuncios vigentes son más frecuentes en seguros (10 de 11), educación (23 de 27) y medios (12 de 15). Son menos frecuentes en la Administración pública (37 de 72) y en fabricación (6 de 16). Hay dispositivos clasificados como de empleados en 217 de las 250 organizaciones. Un anuncio es motivo para validar cuentas, no prueba de una brecha (§3.4).

3.3 Dispositivos y credenciales

Comercio, Administración pública y banca concentran más asociaciones de dispositivos infectados, casi todas fuera de la clasificación de empleados



Fuente: Brandefense Atlas y asociaciones de Blackhole para 250 organizaciones, leídas el 21 de noviembre de 2026 [S2]. Los registros son acumulados, no solo de 2026.

Sector	Org. con dispositivos infectados	Dispositivos, límite inferior (empleados)	Registros de credenciales	Cuota de credenciales, dos mo
Comercio y grupos empresariales	20 de 21	298.644 (3.373)	339.747	
Administración pública	67 de 72	170.584 (8.807)	1.257.137	
Banca y finanzas	25 de 25	143.948 (298)	135.365	
Transporte y logística	18 de 18	125.675 (695)	131.230	
Educación	27 de 27	104.087 (18.376)	2.943.162	
Telecomunicaciones	9 de 10	100.470 (10.628)	6.077.675	
Medios y entretenimiento	15 de 15	94.297 (345)	60.177	
Seguros	11 de 11	77.086 (376)	126.255	
Hostelería y turismo	10 de 10	35.940 (631)	81.178	

Sector	Org. con dispositivos infectados	Dispositivos, límite inferior (empleados)	Registros de credenciales	Cuota de credenciales, dos ma
Energía y servicios públicos	14 de 14	35.749 (458)	106.817	
Sanidad	10 de 11	26.421 (388)	122.527	
Fabricación e industria	15 de 16	4.964 (2.520)	229.016	
Todos	**241 de 250**	**1.217.865 (46.895)**	**11.610.286**	

Algunos totales de dispositivos son límites inferiores. Las filas de banca se tratan con más detalle en el capítulo 9. Los registros de credenciales se dividen en 2.050.519 registros de bases de datos de brechas, 3.469.083 líneas de registros de stealers y 6.090.684 entradas de combolists. Los dispositivos infectados contienen en total al menos 4,2 millones de credenciales capturadas (límite inferior), de todos los servicios y no solo de la propia organización.

Qué significa.

- **Las marcas de consumo concentran los dispositivos, sobre todo fuera de la clasificación de empleados.** De los 298.644 dispositivos asociados al comercio, 295.271 no están clasificados como de empleados, y tampoco 143.650 de los 143.948 asociados a bancos. Sus registros de stealers incluyen un inicio de sesión en el sitio de la empresa. Por eso lo más plausible es que sean ordenadores de los propios clientes, aunque no se ha establecido su titularidad. Estas asociaciones son una señal de fraude y de toma de control de cuentas; por sí solas no establecen una intrusión en la empresa.
- **Las universidades y las operadoras concentran el problema de los dispositivos de empleados.** Educación tiene 18.376 dispositivos clasificados como de empleados y telecomunicaciones 10.628; juntos suman el 62 % del total nacional de nuestra lista. El personal y los estudiantes universitarios comparten dominios, así que aquí «empleado» puede incluir a estudiantes. Los dominios de telecomunicaciones también sirven como direcciones de correo de clientes. Eso explica además que dos operadoras concentren el 84 % de los 6,1 millones de registros de credenciales del sector.
- **La Administración pública acumula 1,26 millones de registros de credenciales, segunda tras las universidades.** Educación, donde 25 de las 27 universidades son públicas, acumula 2,94 millones. La causa probable son los portales autonómicos y municipales que emiten cuentas de personal y de ciudadanos en el mismo dominio; la validación debería separar ambas.
- **La organización mediana no es pequeña.** La organización mediana tiene unas 1.900 asociaciones de dispositivos infectados y 4.500 registros de credenciales. Unos pocos dominios con mucho volumen dominan los totales, así que el total de un sector orienta mal sobre un miembro típico.

3.4 Anuncios vigentes de credenciales: lo primero que hay que priorizar

En la comprobación, 163 de las 250 organizaciones tenían una credencial vinculada a su dominio en un mercado monitorizado. De ellas, 149 tienen también historial de anuncios.

Un anuncio vigente es la señal de mercado más directa de que se ofrece un inicio de sesión vinculado al dominio. Si ese acceso sigue funcionando es lo que debe establecer la validación. El anuncio no dice cuántas cuentas hay, de quién son ni si una cuenta está activa, protegida con autenticación multifactor o ya restablecida. La decisión que respalda es «validar la cuenta ahora», no «declarar una brecha».

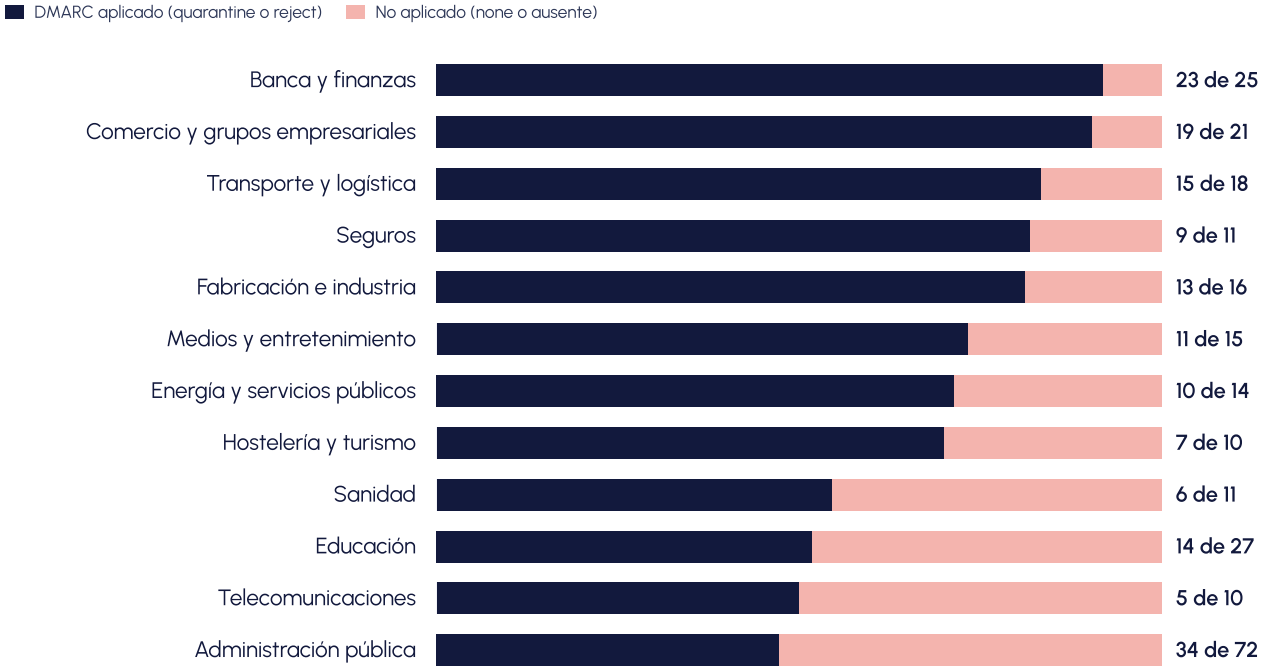
3.5 Dominios similares, documentos expuestos y menciones

- **Dominios similares:** 221 organizaciones tenían al menos un dominio similar observado por primera vez en los últimos 30 días. Los nombres comerciales cortos o genéricos recogen dominios sin relación; de las 182 organizaciones con un nombre comercial distintivo, 153 tenían al menos uno; estos recuentos sirven para priorizar. Los dominios similares son candidatos, no sitios de phishing confirmados.
- **Documentos expuestos:** 200 organizaciones tienen al menos un documento expuesto que menciona su dominio (6.990 en total).
- **Menciones:** 111 organizaciones fueron mencionadas en fuentes de chats clandestinos en los últimos 365 días y 82 en fuentes de la dark web (onion). Los dominios de medios y telecomunicaciones dominan los mayores recuentos porque los canales enlazan a ellos; las menciones miden

visibilidad, no hostilidad.

3.6 Higiene del correo y de la web

Los bancos y el comercio aplican DMARC en su mayoría; la Administración pública, las telecomunicaciones y la educación a menudo no



Fuente: comprobaciones públicas de DNS, TLS y página de inicio de 250 dominios, 21 de noviembre de 2026 [S22].

Resultados de nuestras comprobaciones públicas de DNS, TLS y páginas de inicio [S22]:

Control	Resultado (de 250 salvo indicación)	Lectura
DMARC reject	99	El correo suplantado desde el dominio debería rechazarse
DMARC quarantine	67	El correo suplantado debería ir a spam
DMARC p=none o ausente	84 (62 none, 22 ausentes)	Sin aplicación; suplantar el dominio es más fácil
SPF que termina en -all / ~all / ?all / redirect / sin término "all" / sin SPF	182 / 45 / 1 / 4 / 1 / 17	17 dominios no publican política SPF
Registro DKIM encontrado	193	No encontrar un registro DKIM no prueba que no exista
Registro DS observado (delegación DNSSEC)	43	No se observó registro DS en 207 dominios; 28 de los 43 son dominios de la Administración pública
Certificado TLS no válido	13 de 234 comprobados	Certificados caducados, no coincidentes o no fiables
HSTS en la página de inicio	145 de 191 accesibles	La mayoría de los sitios accesibles fuerzan HTTPS para los visitantes recurrentes
Proveedor de correo	63 Microsoft 365, 20 Google, 27 sin MX	El resto usa correo propio o regional

Los bancos y el comercio van por delante; los organismos públicos, por detrás. Aplican DMARC 23 de las 25 organizaciones de banca y pagos y 19 de las 21 de comercio. Los organismos de la Administración pública (34 de 72), las operadoras (5 de 10), las universidades (14 de 27) y la sanidad (6 de 11) son los que menos lo aplican.

La Administración pública es también donde más se usa la delegación DNSSEC: 28 de los 43 dominios con registro DS observado son de la Administración pública. El sector es heterogéneo y no uniformemente débil.

CONCLUSIONES CLAVE

01

Las asociaciones de dispositivos infectados y de credenciales son casi universales en la lista; piden validación, no alarma.

02

Un anuncio vigente de credenciales es la señal más directa de que se ofrece un acceso, así que es lo primero que hay que priorizar.

03

Cerca de la mitad de los organismos públicos y universidades comprobados no aplica DMARC, lo que deja sus nombres expuestos a la suplantación.

CAPÍTULO 4

Lo que vemos en la dark web

ESTE CAPÍTULO RESPONDE

¿Qué ofrecen realmente los canales y foros delictivos sobre España más allá del ruido de bots, y qué ofertas merecen el tiempo de un defensor?

87 %

de las publicaciones etiquetadas con España procedía de una familia de bots en turco

EN ESTE CAPÍTULO

4.1 Ficha del universo | 4.2 Plataformas, idiomas y volumen | 4.3 Familias delictivas tras la depuración | 4.4 Ofertas de datos específicas de España | 4.5 Ofertas de temática gubernamental y material recirculado | 4.6 Estudios de caso | 4.7 Lo que aportan los foros

EN RESUMEN

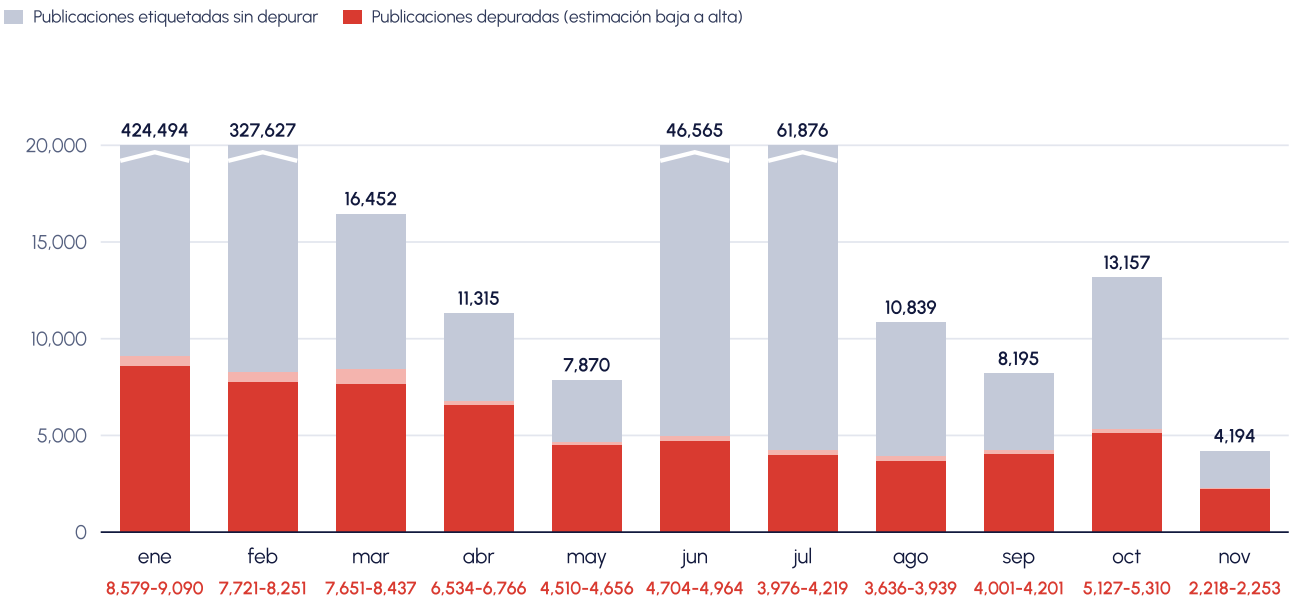
Las publicaciones etiquetadas con España suman 932.584 en 2026, pero el 87 % procede de una familia de bots en turco que etiqueta todos los países. Quedan unas 60.000 relevantes. La mayor parte comercia con cuentas bancarias y de pago, seguida de tarjetas, filtraciones de datos y documentos de identidad. Las ofertas de más peso fueron una vinculada al incidente confirmado de una comercializadora de energía y varias grandes reivindicaciones que las organizaciones nombradas negaron. Trate cada anuncio como una pista que comprobar, no como una brecha.

4.1 Ficha del universo

Elemento	Definición
Población	Publicaciones de Brandefense Blackhole etiquetadas como relativas a España, con fecha de publicación 1 de enero-20 de noviembre de 2026: 932.584. De ellas, 1.454 son publicaciones de foros
Familia de bots	Alrededor del 87 % de las publicaciones etiquetadas procede de una familia de plantillas automatizadas en turco que también etiqueta Portugal, Italia, Francia y Turquía. Es ruido publicitario, no una señal propia de España
Depuradas	58.657-62.086 publicaciones relevantes. El rango es una banda de incertidumbre, no dos recuentos
Unidad	Una publicación. Las publicaciones no son ofertas, vendedores, víctimas ni incidentes únicos
No establecido	Que un anuncio sea real, actual, propio de España o se haya vendido. Una etiqueta de país significa «relativo a España», no «dirigido contra España»

4.2 Plataformas, idiomas y volumen

Una familia de bots infla enero, febrero, junio y julio; el volumen depurado se mantiene entre unas 2.200 y 9.100 publicaciones al mes



Fuente: Brandefense Blackhole, publicaciones etiquetadas como España, fechas de publicación del 1 de enero al 20 de noviembre de 2026, noviembre parcial [S3]. Las cifras depuradas son un límite superior.

Telegram concentra el 99,8 % de las publicaciones etiquetadas. Los foros tienen pocas publicaciones, pero la mayoría de las grandes ofertas de bases de datos. El volumen de la familia de bots alcanza su máximo en enero y febrero, y ese pico aparece en todos los países de comparación. El aumento de junio y julio es mucho mayor en España (en junio, unas seis veces el nivel de mayo) que en cualquier país de comparación. Se debe a plantillas en turco de la misma familia (gráfico c09), así que ningún pico es una señal delictiva propia de España.

El turco domina la etiqueta sin depurar; tras la depuración, pesan las publicaciones en inglés y en español



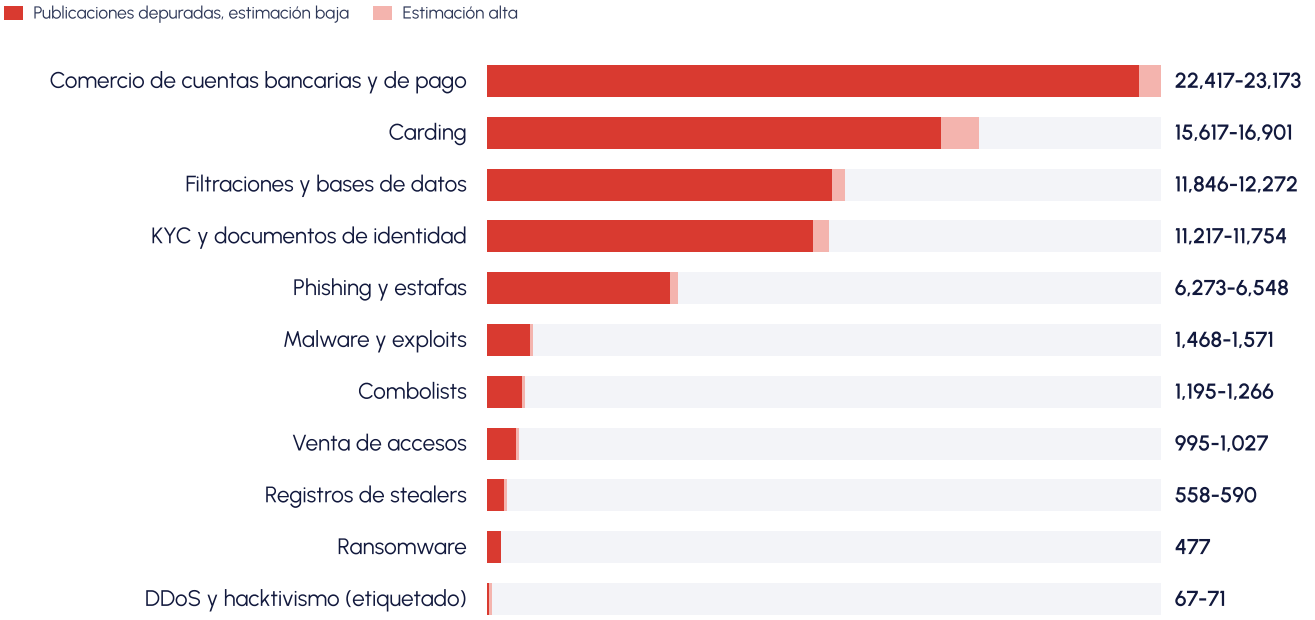
Telegram concentra el 99.83% de las publicaciones etiquetadas. Fuente: Brandefense Blackhole, publicaciones etiquetadas como España, fechas de publicación del 1 de enero al 20 de noviembre de 2026, noviembre parcial [S3]. Las cifras depuradas son un límite superior.

Idioma	Cuota sin depurar	Cuota tras la depuración
Inglés	7,4 %	54 %
Español	3,6 %	34 %
Ruso	1,6 %	6 %
Chino	0,7 %	5 %

El turco es el 86,9 % de la etiqueta bruta, sobre todo de la familia de bots. Tras la depuración, el reparto es 54% / 34% para inglés y español. Las publicaciones en español proceden sobre todo de canales de fraude y de servicios bancarios dirigidos a un público hispanohablante. El ruso aparece sobre todo en canales de DDoS y hacktivismo (capítulo 6).

4.3 Familias delictivas tras la depuración

El comercio de cuentas bancarias y de pago encabeza el corpus depurado; le siguen tarjetas, filtraciones de datos y documentos de identidad



Fuente: Brandefense Blackhole, publicaciones etiquetadas como España, fechas de publicación del 1 de enero al 20 de noviembre de 2026, noviembre parcial [S3]. Las cifras depuradas son un límite superior.

Familia	Publicaciones depuradas (baja-alta)	Precio mediano en las publicaciones que lo indican
Comercio de cuentas bancarias y de pago	22.417-23.173	180 USD
Carding	15.617-16.901	80 USD
Filtraciones y bases de datos	11.846-12.272	20 USD
KYC y documentos de identidad	11.217-11.754	100 USD
Phishing y estafas	6.273-6.548	60 USD
Malware y exploits	1.468-1.571	300 USD
Combolists	1.195-1.266	59 USD
Venta de accesos	995-1.027	80 USD
Registros de stealers	558-590	63 USD
Ransomware (menciones y reenvíos)	477	no significativo
DDoS y hacktivismo (etiquetado)	67-71	no significativo

Una publicación puede pertenecer a más de una familia, así que las filas no suman el total depurado. Los precios son precios de venta anunciados en las publicaciones que los indican; no son precios de transacción.

Lo que destaca. La mayor parte del corpus depurado de España (alrededor del 37 %) es el comercio de cuentas bancarias, no las filtraciones de bases de datos. Los canales de Telegram en español anuncian «cuentas», «cargas» y «drops»: cuentas bancarias y de pago ya abiertas o alquiladas, «cargas» de dinero y cuentas mula para recibir y mover el dinero del fraude. Los nombres de los canales y las publicaciones citan como productos a los mayores bancos minoristas y neobancos españoles. Es una economía del fraude dirigida a los clientes de los bancos, y el capítulo 8 la trata en detalle.

4.4 Ofertas de datos específicas de España

Cuándo	Fuente reivindicada (función)	Qué se ofrecía	Situación
4 de enero	Endesa (comercializadora de electricidad y gas)	Base de datos de clientes, «más de 20 millones de personas», alrededor de 1 TB	La empresa confirmó un incidente; cifras no confirmadas (caso A)
20 de enero, 5 de febrero	PcComponentes (comercio electrónico de informática)	16,3 millones de perfiles de usuario; datos de personal y de logística	La empresa negó el acceso a sus bases de datos y confirmó un ataque de relleno de credenciales contra cuentas `[S23]`
30 de enero	Una gran comercializadora de energía	Nueva subida de datos de clientes que el autor fecha en mayo de 2024	Datos que el autor fecha en 2024, ofrecidos de nuevo (caso C)
31 de enero	Un organismo del sector público	«47,3M de ciudadanos» con DNI, dirección, teléfono e IBAN	Negado; compradores del foro lo calificaron de falso (caso B)
Febrero-marzo	Bancos minoristas españoles («leads» de clientes)	Listas de precios por banco de registros de contacto de clientes	Reivindicación; no verificada (caso D)
21 de agosto	Sitios web de un cuerpo policial	Archivos que, según el autor, proceden de un «simple escaneo»	Reivindicación; no verificada
Agosto	Particulares en España	Varias listas de nombres, números de identificación fiscal e IBAN; escaneos de pasaportes	Reivindicaciones; origen desconocido
2 de noviembre	Un comercio de electrónica de consumo	Registros de clientes (cifra reivindicada omitida)	Reivindicación; no verificada
4 de noviembre	Un operador de infraestructura de telecomunicaciones	Inventario de red	Reivindicación; no verificada

FICHA DE EVIDENCIA B01 — 4 ene 2026

spain Foro de filtraciones · Forum · Inglés

ORIGINAL

```
BIGGEST Spain DATABASE (Endesa)
This database is new, fresh, never seen before, not a
previous leak
ONLY SELLING IT TO 1 PERSON [...]
Total size: (1,055,950,885,115 bytes)
If you want more information/buy message me on my Telegram
[contacto eliminado]
More than +20.000.000 people in one single .sql [...]
[lista de archivos de tablas de clientes, cuentas,
expedientes y facturación eliminada]
```

TRADUCCIÓN

LA MAYOR BASE DE DATOS DE España (Endesa)
Esta base de datos es nueva, reciente, nunca vista, no es una filtración anterior
SOLO LA VENDO A 1 PERSONA [...]
Tamaño total: (1.055.950.885.115 bytes)
Si quieres más información o comprar, escríbeme a mi Telegram [contacto eliminado]
Más de +20.000.000 de personas en un único .sql [...]
[lista de archivos de tablas de clientes, cuentas, expedientes y facturación eliminada]

LO QUE CONSTA	La oferta, el tamaño reivindicado y el número de personas reivindicado; la empresa confirmó por separado un incidente.
LO QUE NO CONSTA	El número de personas afectadas, la antigüedad de cada archivo, cualquier venta.

FICHA DE EVIDENCIA B03 — 31 ene 2026

[alias omitido; nombra al organismo reivindicado] Foro de filtraciones · Forum · Inglés, con nombres de campo en español

ORIGINAL

```
Hello. Today I am selling the updated database of [un
organismo del sector público] containing the information of
47.3M citizens
The data includes: ID, DNI/NIF, Nombre completo, [...]
Direccion, [...] Telefono, IBAN, ContactEmail [...]
Sample: [registros de muestra eliminados]
```

TRADUCCIÓN

Hola. Hoy vendo la base de datos actualizada de [un organismo del sector público] con la información de 47,3M de ciudadanos
Los datos incluyen: ID, DNI/NIF, nombre completo, [...] dirección, [...] teléfono, IBAN, correo de contacto [...]
Muestra: [registros de muestra eliminados]

LO QUE CONSTA	La reivindicación y su lista de campos; la muestra usa valores que parecen inventados.
LO QUE NO CONSTA	Que algún registro proceda del organismo nombrado, que dijo no haber encontrado rastro de ningún incidente.

FICHA DE EVIDENCIA B04 — 2 feb 2026

Usuario del foro Foro de filtraciones · Forum · Inglés

ORIGINAL

```
This is a scam. The mails do not exist
```

TRADUCCIÓN

Esto es una estafa. Los correos no existen

LO QUE CONSTA	Un usuario del foro cuestionó públicamente la reivindicación sobre la base de datos del sector público dos días después de su publicación.
LO QUE NO CONSTA	Quién es el autor de la respuesta ni cómo se comprobaron los correos.

FICHA DE EVIDENCIA B06 — 5 feb 2026

Leonsky Foro de filtraciones · Forum · Inglés

ORIGINAL

```
I am selling a complete, private SQL dump of
PCComponentes.com (Spain's #1 Tech E-commerce). This is a
fresh extraction from January 2026
Users: 16,342,881 unique records
Fields: Full Name, Email, Bcrypt Hash, Salt, DNI/NIF, Phone,
Full Address [...]
Price 28.000$ [contacto eliminado]
[muestra de personal eliminada]
```

TRADUCCIÓN

Vendo un volcado SQL completo y privado de PCComponentes.com (el comercio electrónico tecnológico n.o 1 de España). Es una extracción reciente de enero de 2026
Usuarios: 16.342.881 registros únicos
Campos: nombre completo, correo, hash Bcrypt, salt, DNI/NIF, teléfono, dirección completa [...]
Precio: 28.000 $ [contacto eliminado]
[muestra de personal eliminada]

LO QUE CONSTA	La oferta, su precio y el número de registros reivindicado.
LO QUE NO CONSTA	Una brecha en la base de datos; la empresa negó el acceso a sus bases de datos y confirmó un ataque de relleno de credenciales contra cuentas.

4.5 Ofertas de temática gubernamental y material recirculado

Las ofertas que nombran organismos del Estado se concentran en registros nacionales y sistemas policiales. La mayoría de esas ofertas no superan comprobaciones básicas. La muestra de enero de la base de datos del sector público usa valores que parecen inventados, como dígitos de cuenta bancaria secuenciales y números de teléfono de manual. Los usuarios del foro la calificaron de falsa en dos días. En febrero, un perfil de foro reenvió la propia declaración de un ministerio sobre un «incidente técnico» como prueba de una brecha; el ministerio solo confirmó un incidente «muy limitado» (capítulo 5).

Los mismos perfiles reaparecen. Un perfil que reenvió la filtración de enero de datos de altos cargos también volvió a subir datos de la comercializadora de energía que fecha en 2024. Además anunció una base de datos de fidelización de viajes que un grupo de ransomware filtró por primera vez en diciembre de 2025. Volver a subir material antiguo es barato y da reputación en el foro. Para los defensores, la pregunta es siempre la misma: si es nuevo y si es nuestro.



4.6 Estudios de caso

A

CASO A

Un incidente confirmado con clientes de energía y anuncios republicados

LA EMPRESA CONFIRMÓ UN INCIDENTE

Ficha de evidencia B01 | 4 ene 2026 | Foro de filtraciones | Energía

Reivindicación	El 4 de enero, un perfil que se hacía llamar «spain» ofreció una base de datos que atribuía a Endesa, con más de 20 millones de personas y alrededor de 1 TB, según afirmó. Enumeraba nombres de archivo de tablas de clientes, cuentas, expedientes y facturación, y decía que «solo la vendía a 1 persona».
Cronología	En enero, la empresa informó a sus clientes de un acceso a una plataforma comercial. Según la empresa, quedaron expuestos datos identificativos, de contacto y de contrato y, en algunos casos, números de cuenta bancaria (caso G). El 16 de febrero, un segundo perfil volvió a publicar el mismo tamaño y texto con un título de 2026 y un nuevo contacto (B02); un tercer perfil lo republicó más tarde.
Qué podemos establecer	Que la oferta precedió a la notificación de la empresa o coincidió con ella, y que otros perfiles republicaron el mismo anuncio. Las publicaciones no establecen el número de personas afectadas, que algún perfil tenga los datos ni que se produjera una venta.
Alternativas	Un único vendedor con varios nombres; revendedores que copian el anuncio; una mezcla de datos reales y de relleno.
Límites	No se evaluó ninguna muestra. La cifra del atacante no es la de la empresa.
Respuesta	Los clientes de cualquier comercializadora de energía deberían esperar llamadas y mensajes que citen datos reales de su contrato. Las comercializadoras deberían indicar a sus centros de atención al cliente que nunca pidan datos bancarios completos en contactos entrantes.
EN DEFINITIVA	**Incidente confirmado, cifras sin confirmar, anuncios republicados: advierta a los clientes sobre llamadas que citen datos reales del contrato.**

B

CASO B

Una reivindicación sobre una base de datos del sector público que los compradores calificaron de falsa

REIVINDICACIÓN NEGADA

Ficha de evidencia B03 | 31 ene 2026 | Foro de filtraciones | Administración pública

Reivindicación	El 31 de enero, un perfil cuyo alias nombra al organismo reivindicado ofreció «la base de datos actualizada de [un organismo del sector público] con la información de 47,3M de ciudadanos». Incluía campos de DNI, dirección, teléfono, IBAN y pagos.
Cronología	El 3 de febrero, la prensa informó de que el organismo afectado había descartado la reivindicación; un portavoz dijo que no había encontrado rastro de ningún incidente [S24]. En los dos días siguientes a la publicación, un usuario del foro respondió «Esto es una estafa. Los correos no existen» (B04).
Qué podemos establecer	Que la reivindicación se hizo y se cuestionó en el mismo foro. Los valores de la muestra parecen inventados.
Alternativas	Invención para ganar reputación; una falsificación de un revendedor; una mezcla de registros públicos y antiguos.
Límites	No contrastamos la muestra con ningún dato real.
Respuesta	Los ciudadanos verán phishing con temática de la Administración en cualquier caso, como muestran los avisos de INCIBE de 2026 (capítulo 8).
EN DEFINITIVA	**Las grandes reivindicaciones sobre bases de datos del Estado a menudo no superan comprobaciones básicas; compare las muestras antes de hablar de una brecha.**

CASO C

Datos de una comercializadora de energía que el autor fecha en 2024, ofrecidos de nuevo

DATOS QUE EL AUTOR FECHA EN 2024

Ficha de evidencia B05 | 30 ene 2026 | Foro de filtraciones | Energía

Reivindicación	El 30 de enero, un perfil de foro publicó una «base de datos» de una gran comercializadora de energía. Afirmó que los datos se exportaron en mayo de 2024 desde una unidad en la nube usada por el personal de un centro de atención al cliente.
Qué podemos establecer	Que en 2026 un perfil que también reenvía otras filtraciones volvió a ofrecer datos que el autor fecha en 2024. La fecha procede de la publicación, no de una comprobación independiente.
Alternativas	Una exportación auténtica de 2024; un conjunto de datos más antiguo reempaquetado.
Respuesta	Tómelo como recordatorio de que las exportaciones de los centros de atención sobreviven al incidente. Revise quién puede exportar listas de clientes a unidades personales o compartidas.
EN DEFINITIVA	**Las exportaciones de los centros de atención al cliente sobreviven al incidente que las produjo.**

FICHA DE EVIDENCIA B02 — 16 feb 2026

Koipo Foro de filtraciones · Forum · Inglés

ORIGINAL

```
ENDESA SPAIN (2026) IBAN 20M+
DM Price: [contacto eliminado]
More than +20.000.000 people in one single .sql (fresh data,
never seen)
Total size: (1,055,950,885,115 bytes)
File Tree: [enlace eliminado]
SAMPLE ALL FILES: [enlace eliminado]
```

TRADUCCIÓN

ENDESA ESPAÑA (2026) IBAN 20M+
Precio por MD: [contacto eliminado]
Más de +20.000.000 de personas en un único .sql (datos recientes, nunca vistos)
Tamaño total: (1.055.950.885.115 bytes)
Árbol de archivos: [enlace eliminado]
MUESTRA DE TODOS LOS ARCHIVOS: [enlace eliminado]

LO QUE CONSTA	Un segundo perfil volvió a publicar el mismo anuncio, con el mismo tamaño y texto, seis semanas después y con un nuevo contacto.
LO QUE NO CONSTA	Si quien lo republicó tiene algún dato o solo copió el anuncio; cualquier venta.

FICHA DE EVIDENCIA B05 — 30 ene 2026

IntelShadow Foro de filtraciones · Forum · Inglés, con nombres de campo en español

ORIGINAL

```
Hi [foro], today I have uploaded the [comercializadora de
energía] database, the data breach occurred in May 2024
[...] when [número de archivos eliminado] files were
exported with the email [dirección eliminada] from Google
Drive.
DATA [lista de campos eliminada: número de identidad,
nombre, teléfono, dirección, IBAN, punto de suministro]
SAMPLE [registros eliminados]
```

TRADUCCIÓN

Hola, [foro]: hoy he subido la base de datos de [comercializadora de energía]; la brecha de datos se produjo en mayo de 2024 [...] cuando se exportaron [número de archivos eliminado] archivos con el correo [dirección eliminada] desde Google Drive.
DATOS [lista de campos eliminada: número de identidad, nombre, teléfono, dirección, IBAN, punto de suministro]
MUESTRA [registros eliminados]

LO QUE CONSTA	El autor fecha los datos en mayo de 2024 y describe una exportación desde una unidad en la nube de un centro de atención al cliente.
LO QUE NO CONSTA	Que los datos sean nuevos, o que se accediera a los sistemas de la comercializadora en 2026.

D

CASO D

«leads» de clientes con precio por banco

REIVINDICACIÓN NO VERIFICADA

Ficha de evidencia B07 | 28 feb 2026 | Canal de Telegram de servicios bancarios | Banca

Reivindicación	Un vendedor de Telegram publicó una lista de precios de «leads» de clientes españoles por banco, de 600 a 750 euros por cada 5.000 registros, con una «nueva actualización» fechada.
Qué podemos establecer	Que un vendedor comercializa listas de contacto segmentadas por banco. Estas listas alimentan las campañas de SMS y llamadas de suplantación bancaria que la policía desarticuló en 2026 (capítulo 8).
Alternativas	Listas construidas a partir de brechas antiguas y datos públicos, no de ningún banco.
Respuesta	Los bancos deberían asumir que sus clientes recibirán llamadas de quien sabe qué banco usan. También deberían repetir que el banco nunca pide mover dinero a una «cuenta segura».
EN DEFINITIVA	**Las listas de «leads» segmentadas por banco alimentan las llamadas de suplantación; advierta a los clientes sobre las estafas de la «cuenta segura».**

FICHA DE EVIDENCIA B07 — 28 feb 2026

L34ds Canal de Telegram de servicios bancarios · Telegram · Español e inglés

ORIGINAL

```
Leads Spain EN VENTA:
[banco A]: 750€ - 5k
[banco B]: 750€ - 5k
[banco C]: 650€ - 5k
[...doce bancos y neobancos enumerados...]
Papa y mamá 600€ - 5k
NUEVA ACTUALIZACIÓN / NEW UPDATE 24-2-2026 [contacto eliminado]
```

LO QUE CONSTA	Se comercializan listas de contacto por banco, además de una lista dirigida a padres.
LO QUE NO CONSTA	Que algún banco sufriera una brecha; estas listas suelen construirse a partir de filtraciones antiguas.

FICHA DE EVIDENCIA B08 — 1 ene 2026

Autor anónimo Canal de Telegram en español de fraude bancario · Telegram · Español

ORIGINAL

```
Necesito
[banco A] + [plataforma de criptomonedas]
[neobanco] creada +1€
[neobanco] a crear
DM [contacto eliminado]
```

LO QUE CONSTA	Demanda de cuentas ya abiertas y por abrir, el producto central de estos canales.
LO QUE NO CONSTA	Quién abriría las cuentas ni a nombre de quién.

E

CASO E

Archivos anunciados como combinaciones de acceso para la página de acceso de un banco

ARCHIVOS ANUNCIADOS OBSERVADOS

Ficha de evidencia B15 | 26 jun 2026 | Foro de filtraciones (bot automatizado) | Banca, comercio, educación

Reivindicación	En mayo y junio, un bot automatizado de un foro publicó pequeños archivos de credenciales con nombres de páginas de acceso de bancos, comercios y universidades españoles. Cada uno tenía entre unas decenas y unos cientos de líneas.
Qué podemos establecer	Que archivos anunciados como combinaciones de URL, correo y contraseña se clasifican por la página de acceso que nombran y se regalan como muestras.
Alternativas	Líneas capturadas por malware infostealer; líneas recicladas de combolists más antiguas; líneas de relleno o no válidas regaladas para atraer compradores.
Respuesta	Los bancos y comercios deberían vigilar si sus URL de acceso aparecen en estos archivos y exigir autenticación reforzada en las cuentas afectadas.
EN DEFINITIVA	**Los archivos anunciados como combinaciones de acceso nombran páginas de acceso bancario; exija autenticación reforzada en las cuentas afectadas.**

F

CASO F

Un inventario de red de telecomunicaciones

REIVINDICACIÓN NO VERIFICADA

Ficha de evidencia B16 | 4 nov 2026 | Foro de filtraciones | Telecomunicaciones

Reivindicación	El 4 de noviembre, un perfil de foro ofreció lo que describía como el inventario de red de un operador de infraestructura de telecomunicaciones. La publicación daba recuentos de activos de red y de buzones de personal.
Qué podemos establecer	Que la oferta existe. Estos inventarios son sensibles porque cartografían la infraestructura física.
Alternativas	Un extracto de planificación compartido con contratistas; datos antiguos.
Respuesta	Los operadores deberían comprobar qué contratistas reciben exportaciones completas del inventario y si esas exportaciones llevan marcas de agua.
EN DEFINITIVA	**Los inventarios de red cartografían la infraestructura física; controle las exportaciones a contratistas y póngales marcas de agua.**

FICHA DE EVIDENCIA B15 — 26 jun 2026

Bot del foro Foro de filtraciones (bot automatizado) · Forum · Inglés

ORIGINAL

```
Log:Pass [acceso a la banca en línea de un banco
español]-110
File Information
Total Lines: 110
Content Type: URL / Email / Password Combo
Sample Data: [líneas de credenciales eliminadas]
```

TRADUCCIÓN

Usuario:contraseña [acceso a la banca en línea de un banco español]-110
Información del archivo
Total de líneas: 110
Tipo de contenido: combinación de URL, correo y contraseña
Datos de muestra: [líneas de credenciales eliminadas]

LO QUE CONSTA	Un archivo de 110 líneas anunciado como combinaciones de URL, correo y contraseña para la página de acceso a la banca en línea de un banco.
LO QUE NO CONSTA	Que los accesos sean válidos, de dónde proceden las líneas, o que se accediera a los sistemas del banco.

FICHA DE EVIDENCIA B16 — 4 nov 2026

Perfil de foro Foro de filtraciones · Forum · Inglés

ORIGINAL

```
[operador de infraestructura de telecomunicaciones]:
internal network platform
[recuentos de activos y buzones eliminados]
[descripción del operador y de la red eliminada] [...]
[registro de muestra y lista de operadores eliminados]
```

TRADUCCIÓN

[operador de infraestructura de telecomunicaciones]: plataforma de red interna
[recuentos de activos y buzones eliminados]
[descripción del operador y de la red eliminada] [...]
[registro de muestra y lista de operadores eliminados]

LO QUE CONSTA	La reivindicación y el tipo de datos descritos.
LO QUE NO CONSTA	Que los datos sean actuales o completos, ni cómo se obtuvieron.

4.7 Lo que aportan los foros

Los foros tienen pocas publicaciones sobre España, pero la mayoría de las grandes reivindicaciones de bases de datos. Las respuestas importan. En al menos tres hilos de 2026, usuarios del foro cuestionaron a un vendedor en pocos días y calificaron los datos de falsos, reciclados de una filtración anterior o tomados de otra empresa. Esas respuestas son una primera comprobación barata para un defensor, aunque también pueden ser competidores que desacreditan a un rival.

CONCLUSIONES CLAVE

01
El comercio de cuentas bancarias, no las filtraciones de bases de datos, es la mayor parte de las publicaciones depuradas sobre España (alrededor del 37 %).

02
Las grandes reivindicaciones contra organismos del Estado y comercios a menudo no superan comprobaciones básicas o reciclan datos antiguos.

03
Varios perfiles volvieron a publicar en pocas semanas una oferta vinculada a un incidente confirmado con clientes de energía.

CAPÍTULO 5

Incidentes confirmados y reivindicaciones por sector

05

ESTE CAPÍTULO RESPONDE

¿Qué organizaciones españolas confirmaron un incidente en 2026, cuáles solo aparecen en la reivindicación de un atacante y qué le dice el patrón a cada sector?

30

incidentes que afectaron a organizaciones o clientes españoles, confirmados por la organización o por una autoridad

EN ESTE CAPÍTULO

5.1 Cómo clasificamos los casos
5.2 Energía y servicios públicos: registros de clientes a gran escala
5.3 Transporte, puertos y logística
5.4 Administración pública
5.5 Educación y sanidad
5.6 Comercio, servicios al consumidor y tecnología
5.7 Otros incidentes confirmados
5.8 Qué muestra el patrón

EN RESUMEN

Hasta la fecha de corte, organizaciones o autoridades confirmaron 30 incidentes con organizaciones o clientes españoles; los atacantes reivindicaron muchos más. Los casos confirmados se agrupan en tres ámbitos. Primero, bases de datos de clientes de energía, comercio y transporte, algunas a través de un proveedor. Segundo, ayuntamientos, un gobierno autonómico y una autoridad portuaria afectados por ransomware o nombrados en reivindicaciones de extorsión. Tercero, universidades y servicios de salud. Trate la base de clientes de un proveedor como superficie de ataque propia y ensaye antes el aviso a clientes.

5.1 Cómo clasificamos los casos

Consideramos un incidente **confirmado** cuando la propia organización o una autoridad pública afirmó que hubo un ataque o un acceso no autorizado. Solo en ese caso nombramos a una organización, y solo si el incidente tuvo amplia difusión. Los casos confirmados más pequeños, publicados sobre todo por un único medio o en un resumen de un CERT, se describen por su función; la fuente citada los nombra.

Todo lo demás es una **reivindicación**: una entrada de extorsión, una publicación en un foro o un mensaje de un canal. Las reivindicaciones se describen por sector y función, nunca por nombre. Un incidente confirmado no confirma las cifras del atacante; cuando difieren, damos ambas.

El recuento. Los 30 incidentes confirmados son: energía 2, transporte y puertos 2, Administración pública 6, educación y sanidad 3, comercio y tecnología 5, otros incidentes confirmados 7 y plataformas extranjeras usadas por clientes españoles 5.

5.2 Energía y servicios públicos: registros de clientes a gran escala

G

CASO G

Datos de contratos de clientes de Endesa (enero)

Energía

CONFIRMADO POR LA EMPRESA

Qué se confirmó	En enero, Endesa informó a sus clientes de un acceso no autorizado a una plataforma comercial. Según la empresa, quedaron expuestos datos identificativos, de contacto y de contrato, números de DNI y, en algunos casos, números de cuenta bancaria. Afirmó que las contraseñas no se vieron afectadas y lo notificó a la Agencia Española de Protección de Datos (AEPD) [S4][S25].
Qué se reivindicó o publicó	Un perfil de foro que se hacía llamar «spain» reivindicó alrededor de 1 TB con datos de más de 20 millones de personas [S25]. La empresa no confirmó ninguna cifra. La reventa de esa oferta figura en el caso A.
Respuesta	Cabe esperar phishing dirigido y llamadas de falsos proveedores que citen datos reales del contrato.
EN DEFINITIVA	**Quedaron expuestos datos de identidad y, en algunos clientes, datos bancarios; cabe esperar phishing dirigido durante meses.**

H

CASO H

Datos de Naturgy en un proveedor externo (mayo)

Energía

CONFIRMADO POR LA EMPRESA

Qué se confirmó	Naturgy informó de un acceso a sistemas de un proveedor externo que afectó a cerca del 3 % de sus clientes en España, con datos identificativos, de contrato y, en algunos casos, bancarios. Afirmó que sus propios sistemas no fueron atacados y que no se expusieron credenciales [S5].
Qué se reivindicó o publicó	Un vendedor reivindicó un conjunto de clientes mucho mayor; la cifra de la empresa y la reivindicación no se han conciliado.
Respuesta	Pregunte a cada proveedor que custodie datos de sus clientes con qué rapidez le avisará.
EN DEFINITIVA	**La brecha se produjo en el proveedor; los plazos de aviso pactados con los proveedores deciden con qué rapidez puede actuar.**

Dos de las mayores comercializadoras de energía de España confirmaron incidentes con datos de clientes en un plazo de cuatro meses. Ninguna confirmó las cifras de los atacantes. INCIBE advirtió a los clientes de Endesa de posibles fraudes posteriores, y la organización de consumidores OCU alertó a los clientes de Naturgy sobre phishing [S4][S5].

5.3 Transporte, puertos y logística

I

CASO I

Sistemas de venta de billetes de Adif y Renfe (septiembre)

Transporte

CONFIRMADO POR LA EMPRESA

Qué se confirmó	El 24 de septiembre, un intruso llegó a sistemas de venta de billetes de Renfe y del administrador de infraestructuras ferroviarias Adif. En noviembre, Renfe informó a sus clientes de que pudieron quedar expuestos datos identificativos y de contacto, números de documento de identidad, contraseñas con hash y registros de viajes. Afirmó que la Guardia Civil había detenido a un sospechoso en octubre [S6].
Qué se reivindicó o publicó	Ni Renfe ni Adif confirmaron las informaciones de prensa sobre 500 GB sustraídos y sobre una intrusión asistida por IA [S26].
Respuesta	Fuerce el restablecimiento de contraseñas donde puedan ser débiles y advierta a los clientes sobre llamadas que citen viajes reales.
EN DEFINITIVA	**Pudieron quedar expuestos números de DNI, contraseñas con hash y viajes; fuerce restablecimientos y advierta sobre llamadas que citen viajes reales.**

J

CASO J

Ransomware en el Puerto de Vigo (marzo)

Transporte

CONFIRMADO POR LA AUTORIDAD PORTUARIA

Qué se confirmó	Un ataque detectado a primera hora del 24 de marzo alteró los sistemas de gestión de mercancías del puerto, y la autoridad portuaria aisló sus sistemas de las redes externas. El presidente del puerto afirmó que los sistemas seguirían desconectados hasta completar todas las comprobaciones de seguridad, y las autoridades confirmaron que se trataba de ransomware [S27].
Qué se informó	Los usuarios del puerto pasaron a procedimientos manuales y en papel para mantener la actividad de carga. El presidente afirmó que las operaciones físicas del puerto no se vieron afectadas [S27].
Qué no consta	Si se sustrajeron datos y qué grupo fue el responsable.
Respuesta	Mantenga un modo manual para las operaciones portuarias y logísticas que pueda funcionar durante días.
EN DEFINITIVA	**Los procedimientos en papel mantuvieron la actividad de carga; ensaye un modo manual antes de necesitarlo.**

5.4 Administración pública

Cuándo	Organismo	Qué se confirmó	Reivindicación, si la hubo
Enero	Concello de Sanxenxo (ayuntamiento)	Un ransomware cifró documentos del servidor municipal; se restauraron desde una copia de seguridad; no se pagó rescate [S28]	Ninguna conocida
Febrero	Ministerio de Ciencia, Innovación y Universidades	Acceso no autorizado a datos personales de solicitantes de homologación de títulos, descrito como «muy limitado» [S29]	El perfil «GordonFreeman» reivindicó pasaportes, documentos de identidad y datos bancarios
Mayo	Ayuntamiento de Valdemoro	Incidente de red el 5 de mayo; servidores desconectados; notificado al Centro Criptológico Nacional (CCN) [S30]	Kairos reivindicó 1,8 TB

Cuándo	Organismo	Qué se confirmó	Reivindicación, si la hubo
Junio (detención anunciada en noviembre)	Ayuntamiento de Ciudad Real	El ayuntamiento suspendió su plataforma de la Zona de Bajas Emisiones tras un incidente de ciberseguridad en junio [S31]. La Guardia Civil afirmó que un intruso entró en la plataforma sin autorización y usó herramientas de IA. Afirmó que intentó una extorsión, pero no nombró a los objetivos. También resultó afectada una empresa de software que presta servicios de administración electrónica [S32]	Ninguna conocida
Agosto	Junta de Comunidades de Castilla-La Mancha (gobierno autonómico)	Ciberataque confirmado; protocolos activados; se informó a las personas afectadas [S33]	Panzer reivindicó unos 3 GB, con registros de alumnos y familias
Noviembre	Ayuntamiento de San Cristóbal de La Laguna	Un incidente el 2 de noviembre dejó fuera de servicio la web, la sede electrónica y los sistemas de gestión de expedientes [S34]	Ninguna a nuestra fecha de corte

Otros dos organismos públicos aparecieron en reivindicaciones de robo de datos que negaron o no confirmaron. Una fue la reivindicación de más de 47 millones de registros contra un organismo del sector público, publicada el 31 de enero (caso B). La otra fue una reivindicación contra una agencia estatal en septiembre, que describimos solo por su función.

5.5 Educación y sanidad

K

CASO K

Contención en la Universidad de Alicante (julio)

Educación

CONFIRMADO POR LA UNIVERSIDAD

Qué se confirmó	La universidad describió el intento de ataque más grave contra sus sistemas hasta la fecha. Aisló sistemas y suspendió temporalmente los plazos de su sede electrónica. Afirmó que se alcanzaron algunos servidores secundarios, pero que las comprobaciones no hallaron indicios de exfiltración de datos [S35].
Qué se reivindicó o publicó	Nada.
Respuesta	Ensaye la decisión de apagar servicios pronto.
EN DEFINITIVA	**La universidad afirma que el aislamiento temprano limitó el ataque a servidores secundarios; ensaye esa decisión.**

L

CASO L

Servidor de investigación de la Universitat de València (mayo)

Educación

CONFIRMADO; REIVINDICACIÓN NO CONCILIADA

Qué se confirmó	La universidad confirmó una intrusión que, según afirmó, alcanzó un servidor obsoleto de un grupo de investigación [S36].
Qué se reivindicó o publicó	NOVA reivindicó 300 GB con datos de personal y estudiantes.
Respuesta	Inventaríe los servidores de investigación que quedan fuera de los servicios informáticos centrales.
EN DEFINITIVA	**La universidad afirma que se alcanzó un servidor de investigación obsoleto; inventaríe los servidores fuera de los servicios informáticos centrales.**

El Servicio Extremeño de Salud informó en octubre de que un acceso automatizado a su portal sanitario en línea afectó a 18.416 usuarios [S37]. Un grupo de ransomware incluyó en su lista a un hospital de Barcelona en octubre, y otro a un grupo hospitalario privado en agosto; ninguno había confirmado un incidente a nuestra fecha de corte.

5.6 Comercio, servicios al consumidor y tecnología

Cuándo	Organización	Qué se confirmó
Enero	PcComponentes	Ningún acceso a sus bases de datos, según la empresa, pero sí un ataque de relleno de credenciales contra cuentas de clientes con contraseñas reutilizadas de otras brechas [S23]
Abril	Inditex	Acceso no autorizado a bases de datos alojadas por un antiguo proveedor tecnológico; la empresa afirmó que no contenían nombres, datos de contacto, contraseñas ni datos de pago, y que sus propios sistemas no se vieron afectados [S38]
Abril	Basic-Fit (afecta a socios españoles)	Acceso a un sistema de registro de visitas el 8 de abril; se descargaron nombres, números de identificación, datos de contacto, fechas de nacimiento y datos de cuentas bancarias [S39]
Junio-julio	Indra (una filial)	Ataque de ransomware en una filial, confirmado por la empresa [S40]; The Gentlemen la incluyó en su sitio de filtraciones, y esa atribución a un grupo sigue siendo una reivindicación [S1]
Julio	Lidl (clientes de la tienda en línea)	Acceso, a través de un proveedor informático, a un archivo independiente con nombres, datos de contacto, fechas de nacimiento y números de cliente [S41]

5.7 Otros incidentes confirmados

Cuándo	Organización (función)	Qué se confirmó
Enero (brecha en diciembre de 2025)	Proveedor de servicios de extranjería de un ministerio	Exposición de datos de residentes extranjeros en poder del proveedor; el ministerio lo confirmó [S42]
Enero	Un ayuntamiento de Canarias	Un ataque dejó la web fuera de servicio durante la noche; el ayuntamiento afirmó que no se vieron afectados datos de la ciudadanía [S43]
Junio	Plataforma de servicios para el hogar de un comercio de bricolaje	Incidente de seguridad reconocido; seguía en investigación una posible brecha de nombres, datos de contacto y números de identificación de algunos clientes. La empresa afirmó que no se vieron afectados contraseñas ni datos bancarios. Una reivindicación de filtración citó unos 55.000 registros [S44]
Julio	Una plataforma autonómica de gestión escolar	El gobierno autonómico informó de un posible acceso no autorizado a cuentas de algunos docentes, restableció las contraseñas de todos los usuarios profesionales y lo denunció a la policía [S45]
Septiembre	Una organización que notificó a la AEPD	Brecha descrita como ejecutada por un agente de IA [S46]
Octubre	Un club de fútbol profesional	Anomalía en servidores de datos con posible impacto en datos personales de aficionados; notificada a la AEPD [S47]
Noviembre	Un comercio de videojuegos	Un acceso no autorizado detectado el 9 de noviembre alcanzó números de cliente, teléfonos, correos electrónicos e historiales de pedidos; la empresa afirmó que no almacena datos de pago [S48]

Además de Basic-Fit (§5.6), otros cinco incidentes confirmados ocurrieron en plataformas extranjeras usadas por clientes españoles. Dos fueron un operador europeo de pases ferroviarios en enero [S49] y Booking.com en abril [S50]. La brecha de mayo de un proveedor de software educativo afectó a una universidad española, una de casi 9.000 instituciones afectadas a escala mundial. Los datos potencialmente afectados eran identificativos, de contacto y de mensajes de aula [S51]. Los otros dos fueron un banco digital que reveló datos tras falsas solicitudes oficiales en septiembre [S52] y una plataforma de experiencias regalo con un acceso no autorizado detectado el 3 de noviembre [S53].

5.8 Qué muestra el patrón

Sector	Confirmados	Qué describen las confirmaciones	Una acción
Energía y servicios públicos	2	Una plataforma comercial y un proveedor externo	Plazos de aviso de brechas en los contratos con proveedores
Transporte y puertos	2	Sistemas de venta de billetes; ransomware en sistemas de mercancías	Restablecimiento de contraseñas; un modo manual ensayado
Administración pública	6	Ransomware, reivindicaciones de extorsión y caídas de sedes electrónicas	Copias de seguridad probadas y aislamiento temprano
Educación y sanidad	3	Servidores secundarios y obsoletos; acceso automatizado a un portal	Un inventario de servidores fuera de los servicios informáticos centrales
Comercio y tecnología	5	Proveedores antiguos y actuales; relleno de credenciales	Lista de proveedores; MFA y control de reutilización en cuentas de clientes
Otros	7	Proveedores, sitios web, servidores de un club y cuentas de docentes	Plantillas de aviso a clientes preparadas
Plataformas extranjeras	5	Brechas en plataformas con datos de clientes españoles	Advertir a los clientes sobre phishing posterior

La tabla ordena los casos por sector, no por titularidad. Si se cuentan organismos públicos, empresas públicas y el proveedor de un ministerio, 14 de los 30 afectaron al sector público. Además de los seis del §5.4, fueron Adif y Renfe, el Puerto de Vigo, dos universidades públicas y un servicio de salud autonómico. Los otros tres figuran en el §5.7: un ayuntamiento de Canarias, una plataforma escolar autonómica y el proveedor de servicios de extranjería de un ministerio.

Cuatro incidentes confirmados (Naturgy, Inditex, Lidl y el proveedor de servicios de extranjería de un ministerio) empezaron en un proveedor actual o anterior de la organización española. Un quinto (Basic-Fit) empezó en un sistema secundario que registraba las visitas a los clubes. El incidente del software educativo es en sí la brecha de un proveedor; lo contamos entre las plataformas extranjeras. En Ciudad Real también resultó afectado un proveedor de software, pero la Guardia Civil no dijo que fuera el punto de entrada, así que no lo contamos como caso de proveedor.

Seis incidentes confirmados tuvieron ransomware confirmado o un grupo de extorsión que incluyó al organismo en su lista o lo reivindicó. Fueron Sanxenxo, Vigo y una filial de Indra (ransomware confirmado), y Valdemoro, Castilla-La Mancha y la Universitat de València (incluidos en listas o reivindicados). En el caso de la filial de Indra, el nombre del grupo es la reivindicación del propio grupo.

Los organismos públicos fueron cinco de los seis: dos ayuntamientos, un gobierno autonómico, una autoridad portuaria y una universidad pública. La Guardia Civil afirmó que el intruso de Ciudad Real intentó una extorsión sin nombrar a sus objetivos, así que ese caso no entra en este recuento. Muchas reivindicaciones de atacantes nombraron a organizaciones que nunca confirmaron nada. Una reivindicación por sí sola es motivo para comprobar, no un hecho.

CONCLUSIONES CLAVE

01

La mayoría de los incidentes confirmados de 2026 expusieron registros de clientes, no sistemas de producción.

02

Cinco incidentes confirmados empezaron en un proveedor o en un sistema secundario.

03

Los organismos públicos fueron cinco de los seis incidentes confirmados con ransomware confirmado o una entrada de extorsión.

CAPÍTULO 6

Hacktivismo y DDoS

ESTE CAPÍTULO RESPONDE

¿Quién reivindicó ataques con encuadre político contra objetivos españoles en 2026, qué interrumpieron realmente esos ataques y cómo deben prepararse los defensores para la próxima oleada?

16-21 feb

la principal oleada DDoS prorrusa contra sitios web públicos españoles

EN ESTE CAPÍTULO

6.1 Cronología | 6.2 La oleada de febrero: reivindicación frente a medición | 6.3 Reivindicaciones contra sistemas industriales | 6.4 Reclutamiento y datos de cargos públicos | 6.5 Otras reivindicaciones en sus propias palabras | 6.6 Lecciones para los defensores

EN RESUMEN

La principal acción hacktivista fue una oleada DDoS prorrusa en febrero contra ministerios, un parlamento autonómico, ayuntamientos y sitios de transporte, reivindicada por NoName057(16) y Server Killers. Fue breve; según los grupos, varios objetivos solo admitían visitantes españoles. Los mismos canales reivindicaron accesos a paneles industriales y pidieron a españoles datos de personal de defensa. Después, la policía detuvo a un presunto colaborador de grupos prorrusos y al presunto instigador de NoName057(16) en España. Prepare mitigación en el proveedor, filtrado geográfico y comunicados antes de la próxima oleada.

6.1 Cronología

26 ene 2026 — **BD Anonymous Team**
Afirma haber tumbado la web de un ayuntamiento gallego y cita Palestina como motivo (B13)

9 feb 2026 — **DDoSia Project (NoName057(16))**
Incluye a un organismo deportivo español entre los sitios que afirma haber dejado sin servicio

16 feb 2026 — **Server Killers con NoName057(16)**
Anuncia ataques contra la «infraestructura gubernamental crítica» de España; enumera sitios web de la Administración central y de ministerios (B10)

16 feb 2026 — **DDoSia Project (NoName057(16))**
Enumera un parlamento autonómico, portales turísticos y sitios de transporte urbano, y cita la ayuda española a Ucrania (B11)

16 feb 2026 — **Z-Pentest Alliance (reenviado)**
Afirma tener acceso completo al panel de control de una estación de bombeo de aguas residuales en España (B12)

17 feb 2026 — **Prensa y observatorios**
Informan de interrupciones temporales; las autoridades no habían hecho comentarios [S9]

19 feb 2026 — **DDoSia Project (NoName057(16))**
Afirma que su ataque contra una empresa de equipos de red causó una caída de la telefonía empresarial; la causa de esa caída no se confirmó

22 feb 2026 — **Guardia Civil**
Anuncia la detención de los cuatro principales miembros del grupo nacional Anonymous Fénix, dos en 2025 y dos en febrero de 2026

3 mar 2026 ●
Canal en español que reenvía a NoName057(16)
Pide a sus seguidores datos personales de trabajadores de la industria de defensa española (B09)

24 mar 2026 ●
DDoSia Project (NoName057(16))
Afirma tener acceso al terminal de venta de billetes de un autobús urbano español

6 jul 2026 ●
Policía Nacional
Anuncia la detención en marzo, tras un aviso del FBI, de un presunto colaborador de CARR y Z-Pentest

17 ago 2026 ○
Prensa
Informa de una lista filtrada de unos 1.000 policías, guardias civiles y militares, investigada por su posible vínculo con NoName057(16)

20 nov 2026 ●
Policía Nacional
Anuncia la detención en Burgos del presunto principal instigador en España de NoName057(16); atribuye al grupo 447 ataques en España desde 2024

6.2 La oleada de febrero: reivindicación frente a medición

Entre el 16 y el 21 de febrero, los canales de NoName057(16), su proyecto de voluntarios DDoSia y el grupo aliado Server Killers publicaron listas de objetivos en España casi a diario. Las listas nombraban sitios web de la Administración central y de ministerios, un parlamento autonómico y una sede electrónica policial. También incluían un organismo nacional de ciberseguridad, ayuntamientos, sitios de transporte público de varias ciudades y empresas privadas. La prensa recogió los objetivos como temporalmente no disponibles el 16 y el 17 de febrero [S9]. Cada objetivo en los canales iba acompañado de un enlace a un informe público de comprobación de disponibilidad como «prueba» (B10, B11).

FICHA DE EVIDENCIA B10 — 16 feb 2026

Server Killers (reenviado) Canal en español que reenvía a Server Killers · Telegram · Español

ORIGINAL

```
Detuvimos todos los ataques. [...] Los siguientes sitios web
ya han sido cerrados por los propietarios [...] y solo se
puede acceder a ellos a través de direcciones IP españolas
[siete sitios de ministerios y del Gobierno enumerados]
Prueba: [enlaces de comprobación de disponibilidad
eliminados]
[frase final de jactancia eliminada]
```

LO QUE CONSTA	La reivindicación del propio grupo, incluida su afirmación de que los objetivos restringieron el acceso a direcciones españolas.
LO QUE NO CONSTA	Cuánto tiempo estuvo caído cada sitio, ni para quién; ningún impacto más allá de la propia reivindicación del grupo.

FICHA DE EVIDENCIA B11 — 16 feb 2026

NoName057(16) Canal de DDoSia Project · Telegram · Ruso

ORIGINAL

```
Показываем Испании последствия поддержки [...]
❌ [туристический портал города] (закрыт по гео)
❌ [региональный парламент] (закрыт по гео)
❌ [общественный транспорт города]
[otros dos sitios de transporte enumerados]
#OpSpain NoName057(16)
```

TRADUCCIÓN

Mostramos a España las consecuencias de apoyar [...]
❌ [portal turístico de una ciudad] (cerrado por geo)
❌ [parlamento autonómico] (cerrado por geo)
❌ [transporte público de una ciudad]
[otros dos sitios de transporte enumerados]
#OpSpain NoName057(16)

LO QUE CONSTA	Una lista de objetivos fechada, que el grupo presenta como respuesta al apoyo de España a Ucrania (se omite la formulación del grupo), y la nota del propio grupo de que dos sitios tenían restricción geográfica.
LO QUE NO CONSTA	La duración real de la caída o su impacto.

Punto	Reivindicación del actor	Versión oficial	Información de prensa y observatorios
Qué se atacó	«Infraestructura gubernamental crítica» de España, decenas de sitios durante seis días (B10, B11)	Ninguna declaración oficial durante la oleada	La prensa recogió ministerios, un parlamento autonómico y sitios de transporte y de ayuntamientos como temporalmente no disponibles [S9]

Punto	Reivindicación del actor	Versión oficial	Información de prensa y observatorios
Impacto	Sitios «cerrados por sus propietarios», accesibles solo desde direcciones españolas (B10)	No se publicó ninguna	La mayoría de las páginas funcionaban con normalidad cuando se informó; un ataque DDoS no roba datos [S9]
Quién	NoName057(16) y Server Killers, que citan el apoyo español a Ucrania	Ninguna atribución oficial durante la oleada; la Policía Nacional anunció después la detención del presunto instigador de NoName057(16) en España (noviembre) [S54]	Los observatorios reenviaron las reivindicaciones de los propios grupos

Cómo leer el panel. La «prueba» del grupo muestra que un sitio no respondió en un momento dado a comprobaciones de disponibilidad desde el extranjero. No muestra cuánto duró la caída, a quién afectó ni si el sitio bloqueaba a propósito las conexiones desde el extranjero. Los propios grupos señalaron que los objetivos habían limitado el acceso a direcciones españolas. Si es cierto, se trata de una mitigación que funciona como estaba previsto.

6.3 Reivindicaciones contra sistemas industriales

En febrero y marzo, los mismos canales reenviaron reivindicaciones de Z-Pentest Alliance y otros de acceso a paneles de control industrial españoles. Las reivindicaciones nombraban una estación de bombeo de aguas residuales, un controlador de riego, un sistema de bombeo de desalación, refrigeración industrial y un terminal de venta de billetes de autobús urbano. Las publicaciones muestran capturas de pantalla de interfaces web de control y describen cambios de configuración.

FICHA DE EVIDENCIA B12 — 16 feb 2026

Z-Pentest Alliance (reenviado)

Canal en español que reenvía a Z-Pentest Alliance · Telegram · Español

ORIGINAL

```
Nuestro estudiante de la Z-Pentest Alliance obtuvo acceso
completo al sistema de control industrial de una estación de
bombeo de aguas residuales en España [nombre del sitio
eliminado]
Esta interfaz SCADA/HMI monitoriza y controla las bombas
[...]
```

LO QUE CONSTA	La reivindicación y el tipo de interfaz mostrado.
LO QUE NO CONSTA	Que se cambiara algún ajuste o se viera afectado algún proceso; ningún operador lo confirmó.

No pudimos verificar ninguna de estas reivindicaciones, y ningún operador ni autoridad confirmó públicamente ninguna a nuestra fecha de corte. El patrón coincide con un aviso conjunto de diciembre de 2025 de agencias de Estados Unidos y aliadas sobre CARR, Z-Pentest, NoName057(16) y Sector16. Describía accesos oportunistas a interfaces de control expuestas en internet con contraseñas débiles, y reivindicaciones falsas o exageradas frecuentes [S55]. Las publicaciones muestran interfaces reivindicadas; no se estableció su autenticidad, su ubicación ni su exposición a internet. El aviso describe el riesgo general de las interfaces de control expuestas en internet, así que los operadores deberían revisar sus propios activos [S55].

6.4 Reclutamiento y datos de cargos públicos

Un canal de Telegram en español reenvía la actividad de NoName057(16). Desde marzo también pidió a sus seguidores datos personales de militares españoles, directivos y trabajadores de la industria de defensa y políticos occidentales, y pidió a ciudadanos españoles que se pusieran en contacto. No se estableció ninguna respuesta ni transferencia de datos. En abril nombró a empresas españolas de defensa y de drones como objetivos de esa recogida de datos.

FICHA DE EVIDENCIA B09 — 3 mar 2026

Administrador del canal

Canal de Telegram en español que reenvía a NoName057(16) · Telegram · Español

ORIGINAL

```
Necesitamos
Datos de empresarios y de trabajadores de empresas
armamentísticas españolas: nombres y apellidos, fotos,
números de DNI y de pasaportes, direcciones de sus
domicilios [...]
[llamamiento de reclutamiento eliminado]
[contacto eliminado]
```

LO QUE CONSTA	La publicación solicita datos identificativos y domicilios de personal del sector de defensa; publicaciones posteriores repiten la petición.
LO QUE NO CONSTA	Que alguien respondiera o transfiriera datos, ni quién gestiona el canal.

En enero, un perfil que se hacía llamar Vindex publicó datos personales de altos cargos públicos [S56]. En agosto, la prensa informó de una lista filtrada de unos 1.000 policías, guardias civiles y militares con nombres, teléfonos y fotografías. Los investigadores la examinaban por su posible vínculo con NoName057(16) [S57]. En noviembre, la Policía Nacional anunció la detención en Burgos del hombre al que describió como principal instigador en España de NoName057(16). Afirmó que hacía propaganda y reclutamiento y que estaba creando la primera célula física del grupo en el país [S10][S54]. Recogemos estos hechos como declaraciones oficiales e informaciones de prensa; una detención no es una condena.

6.5 Otras reivindicaciones en sus propias palabras

- **Encuadre propalestino.** BD Anonymous Team reivindicó en enero haber tumbado la web de un ayuntamiento gallego. Dijo que actuaba porque, a su juicio, el Gobierno español ya no defiende a Palestina (B13). No encontramos confirmación de ninguna caída.
- **Hacktivistas nacionales.** La Guardia Civil afirmó que Anonymous Fénix atacó ministerios, partidos políticos e instituciones públicas en España. Difundió material contra instituciones españolas y de varios países sudamericanos, con un pico tras las inundaciones de 2024 en Valencia. Sus cuatro principales miembros han sido detenidos: su administrador y su moderador en mayo de 2025, y dos de sus miembros más activos en febrero de 2026 [S58][S59].

FICHA DE EVIDENCIA B13 — 26 ene 2026

BD Anonymous Team Canal hacktivista de Telegram · Telegram · Inglés, tal como se publicó

ORIGINAL

```
[afirmación de que el grupo dejó fuera de servicio el sitio
web oficial de un ayuntamiento gallego; enlace de
comprobación de disponibilidad eliminado]
[declaración de motivo parafraseada: el grupo dice que actuó
porque el Gobierno español ya no defiende a Palestina]
BD Anonymous Team #OpSpain
```

LO QUE CONSTA	La reivindicación y el motivo que da el grupo.
LO QUE NO CONSTA	Que el sitio estuviera caído para alguien más que el verificador.

6.6 Lecciones para los defensores

1. **Planifique la mitigación para oleadas breves.** Los grupos dijeron que varios objetivos limitaron el acceso a visitantes españoles durante la oleada de febrero. Use primero la limpieza de peticiones en el proveedor o una red de distribución de contenidos. Aplique filtrado geográfico solo durante un periodo fijo, con una vía de excepción para ciudadanos en el extranjero, y acuerde de antemano quién puede activarlo.

2. **Acuerde de antemano un comunicado público.** La mayoría de las reivindicaciones DDoS se apoyan en el silencio. Un aviso breve que diga que un servicio funciona de forma degradada y que, por ahora, no hay indicios de acceso a datos resta fuerza a la reivindicación.
3. **Saque de internet las interfaces de control.** Todo operador de bombas, riego, refrigeración o equipos de venta de billetes debería buscar paneles web de control accesibles desde internet y exigir autenticación fuerte.
4. **Informe al personal sobre el reclutamiento y la exposición de datos personales (doxxing).** El personal de defensa, de la policía y del sector público debería saber que se están buscando sus datos personales y cómo comunicar un intento de contacto.

CONCLUSIONES CLAVE

01

La oleada DDoS de febrero fue ruidosa y breve; los grupos dijeron que el filtrado geográfico limitó su alcance.

02

Los mismos canales reivindicaron accesos a paneles de control industrial y buscaron datos de cargos públicos.

03

Las detenciones policiales de 2026 se dirigieron al reclutamiento y la coordinación, no solo a los ataques en sí.

CAPÍTULO 7

Actores de amenaza

ESTE CAPÍTULO RESPONDE

¿Qué actores dejaron una huella documentada en España en 2026, qué los vincula y qué significa cada uno para un defensor español?

220

entradas de ransomware en sitios de filtraciones sobre España, 1 de enero-20 de noviembre de 2026

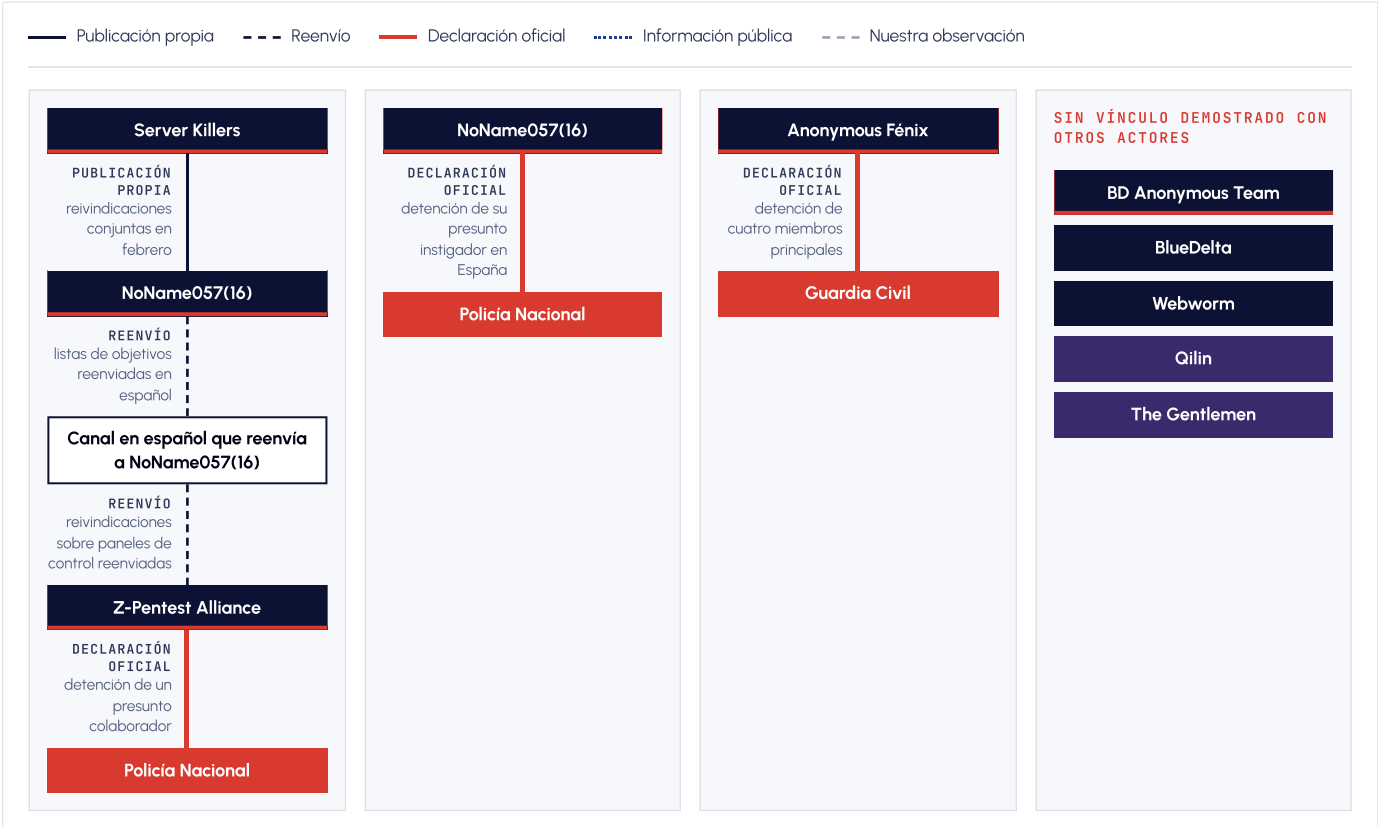
EN ESTE CAPÍTULO

7.1 Cómo se relacionan los actores
7.2 Espionaje vinculado a Estados
7.3 Actores hacktivistas y DDoS
7.4 Ransomware y extorsión
7.5 Perfiles criminales vistos en Blackhole
7.6 Campañas de intrusión no atribuidas

EN RESUMEN

Cuatro tipos de actor definieron el panorama de España en 2026. Los grupos de extorsión, encabezados por Qilin y The Gentlemen, publicaron 220 entradas sobre España. Los grupos DDoS prorrusos llevaron a cabo la campaña más ruidosa. Según investigaciones de proveedores, grupos de espionaje vinculados a Estados usaron temas del Gobierno español y atacaron organismos públicos españoles. Vendedores criminales anunciaron cuentas bancarias y datos de clientes. Priorice la preparación ante la extorsión y las copias de seguridad probadas, y después las defensas de correo contra señuelos de temática gubernamental.

7.1 Cómo se relacionan los actores



Las líneas muestran el tipo de evidencia de cada vínculo. Un vínculo indica una publicación compartida, una declaración oficial o una atribución de un proveedor, no un operador común. Cuando nada vincula a dos actores, el mapa los muestra por separado; no los unimos en «redes» sin un

elemento compartido concreto.

7.2 Espionaje vinculado a Estados

Actor (según lo nombra la fuente)	Qué se observó	Atribución según la fuente	Qué significa para España
BlueDelta (se solapa con APT28)	Señuelos de Word con macros, el primero haciéndose pasar por el orden del día de una reunión de un ministerio español (septiembre de 2025); campañas hasta abril de 2026 contra objetivos gubernamentales, diplomáticos y de fabricación de defensa en Rumanía, España y Turquía. La puerta trasera HOOKEDGE usa servicios legítimos de webhook para el control [S11]	Recorded Future Insikt Group, confianza moderada; un grupo que atribuye a la inteligencia militar rusa [S11]	Los temas del Gobierno español se usan como cebo; bloquee las macros en documentos procedentes de internet
Webworm	Nuevas puertas traseras que usan Discord y Microsoft Graph para el control; objetivos gubernamentales en Bélgica, Italia, Polonia, Serbia y España	ESET, que lo describe como alineado con China [S12]	El C2 a través de servicios en la nube se confunde con la actividad normal de red; vigile el uso inusual de OneDrive y Discord desde servidores

BlueDelta

APT28, Fancy Bear, Forest Blizzard (solapamientos según Insikt)

Espionaje vinculado a un Estado

Atribuido por Recorded Future a la inteligencia militar rusa (GRU)

EN ESPAÑA, 2026

sep 2025	El primer señuelo imita el orden del día de una reunión de un ministerio español
hasta abr 2026	Campañas de HOOKEDGE contra objetivos gubernamentales, diplomáticos y de fabricación de defensa en Rumanía, España y Turquía

OBJETIVOS REIVINDICADOS

Organizaciones gubernamentales, diplomáticas y de fabricación de defensa

EN FUENTES PÚBLICAS

- [S11] Insikt Group, confianza moderada: señuelos de Word con macros instalan la puerta trasera HOOKEDGE, que usa servicios de webhook para el control y la exfiltración
- [S11] Insikt Group: no se pudo verificar la autenticidad del señuelo; no se informa de ningún compromiso del ministerio

NUESTRA VALORACIÓN

Se usaron temas del Gobierno español como cebo. Bloquee las macros en documentos procedentes de internet y alerte de conexiones desde servidores a servicios de webhook.

CONFIANZA **Moderada, según la fuente**

TÉCNICAS CITADAS EN LA INVESTIGACIÓN DEL PROVEEDOR, POR TÁCTICA

Desarrollo de recursos	Ejecución	Persistencia	Evasión de defensas	Descubrimiento	Recopilación
T1583.006 Servicios web	T1059.003 Intérprete de comandos de Windows	T1053.005 Tarea programada	T1027.013 Archivo cifrado o codificado	T1083 Descubrimiento de archivos y directorios	T1074.001 Preparación local de datos
	T1059.005 Visual Basic		T1070.004 Eliminación de archivos		
	T1204.002 Archivo malicioso		T1140 Desofuscación o decodificación de archivos o información		

Mando y control	Exfiltración
T1071.001 Protocolos web	T1041 Exfiltración por el canal de C2
T1105 Transferencia de herramientas al sistema	T1567.004 Exfiltración mediante webhook

Técnicas de HOOKEDGE de BlueDelta. Identificadores de técnica y tácticas según el informe de Recorded Future Insikt Group del 27 de agosto de 2026. [S11]

Webworm

Espionaje vinculado a un Estado | Alineado con China (según ESET)

EN ESPAÑA, 2026

2025-26	Ataques contra organizaciones gubernamentales de Bélgica, Italia, Polonia, Serbia y España

OBJETIVOS REIVINDICADOS

Organizaciones gubernamentales

EN FUENTES PÚBLICAS

- [S12] ESET: nuevas puertas traseras EchoCreep (control mediante Discord) y GraphWorm (control mediante Microsoft Graph y OneDrive); herramientas de proxy propias

NUESTRA VALORACIÓN

Los canales de control a través de servicios en la nube se confunden con la actividad normal de red. Vigile el uso inusual de Discord y OneDrive desde servidores.

CONFIANZA **Según la fuente**

Insikt afirma que no se pudo verificar la autenticidad del señuelo y señala que BlueDelta ha usado históricamente documentos gubernamentales auténticos, incluido material público [S11]. En nuestra lectura, nada en el informe indica una intrusión en el ministerio. El Centro Nacional de Inteligencia afirmó en mayo que España se enfrenta al espionaje, además de al ransomware y a actividades de influencia [S15]. Ninguna de las dos campañas apareció en los datos de sitios de filtraciones y foros que consultamos; la evidencia de ambas procede de investigaciones de proveedores.

7.3 Actores hacktivistas y DDoS

Actor	Actividad en 2026 contra España	Evidencia	Valoración
NoName057(16) y DDoSia Project	Listas de objetivos DDoS en febrero; reivindicaciones contra la venta de billetes de transporte en marzo	Publicaciones propias (B11); declaraciones policiales	El reivindicador más activo; interrupción breve

Actor	Actividad en 2026 contra España	Evidencia	Valoración
Server Killers	Reivindicaciones DDoS conjuntas con NoName057(16) en febrero	Publicaciones propias reenviadas (B10)	Amplificador de la oleada de febrero
Z-Pentest Alliance	Reivindicaciones de acceso a paneles de control españoles	Publicaciones reenviadas (B12); aviso de países aliados [S55]	Reivindicaciones no verificadas; los operadores deberían revisar sus propias interfaces
Un canal en español que reenvía a NoName057(16)	Reenvíos, reclutamiento y peticiones de datos de cargos públicos	Publicaciones propias (B09)	Reenvíos y peticiones de reclutas y datos personales; no muestra capacidad técnica
BD Anonymous Team	Una caída reivindicada de la web de un ayuntamiento	Publicación propia (B13)	Reivindicación única no confirmada; motivo declarado: Palestina
Anonymous Fénix	DDoS contra organismos públicos, con un pico tras las inundaciones de 2024	Declaración de la Guardia Civil [S58][S59]	Grupo nacional; principales miembros detenidos

NoName057(16)

DDoSia Project

Hacktivista (DDoS) | Prorruso (según CISA y socios)

EN ESPAÑA, 2026

9 feb	Incluye a un organismo deportivo español entre los sitios que afirma haber dejado sin servicio
16-21 feb	Listas diarias de objetivos en España, con referencia a la ayuda a Ucrania (B11)
24 mar	Afirma tener acceso a un terminal de venta de billetes de autobús urbano
20 nov	La policía anuncia la detención de su presunto principal instigador en España

OBJETIVOS REIVINDICADOS

Ministerios, un parlamento autonómico, ayuntamientos, transporte público, portales turísticos, empresas privadas

EN SUS PROPIAS PALABRAS

> *"Mostramos a España las consecuencias"* B11

EN FUENTES PÚBLICAS

- [S54] Policía Nacional: detención en Burgos de su presunto principal instigador en España
- [S10] Información de prensa sobre el comunicado de la Policía Nacional: se atribuyen al grupo 447 ataques en España desde 2024
- [S81] Policía Nacional: detención en marzo de un presunto colaborador de los grupos prorrusos CARR y Z-Pentest
- [S55] CISA y socios: hace con frecuencia reivindicaciones falsas o exageradas; voluntarios manejan su herramienta DDoS

NUESTRA VALORACIÓN

El reivindicador más activo contra sitios web públicos españoles en 2026. La interrupción fue breve; el propio grupo informó de restricciones geográficas, y sus cifras son reivindicaciones.

CONFIANZA **Alta en que reivindicó la oleada; impacto no verificado**

Z-Pentest Alliance

Z-Pentest

Hacktivista (reivindicaciones sobre OT) | Prorruso (según CISA y socios)

EN ESPAÑA, 2026

16 feb	Afirma tener acceso completo al panel de control de una estación de bombeo de aguas residuales (B12)
17-18 feb	Afirma tener acceso a un sistema de bombeo de desalación y a refrigeración industrial
mar	Nuevas reivindicaciones contra interfaces de control españolas, reenviadas por un canal en español

OBJETIVOS REIVINDICADOS

Paneles de control reivindicados de bombas, riego, refrigeración y tratamiento de agua

EN SUS PROPIAS PALABRAS

> *"obtuvo acceso completo al sistema de control industrial"* B12

EN FUENTES PÚBLICAS

- [S55] CISA y socios: uno de cuatro grupos prorrusos que acceden a dispositivos HMI expuestos, a menudo mediante contraseñas débiles
- [S81] Policía Nacional: un presunto colaborador de CARR y Z-Pentest fue detenido en Palencia en marzo

NUESTRA VALORACIÓN

Ningún operador ni autoridad de España confirmó ninguna de sus reivindicaciones a nuestra fecha de corte. Las publicaciones muestran interfaces reivindicadas cuya autenticidad y exposición a internet no se establecieron; CISA y sus socios describen el riesgo general, así que los operadores deberían revisar sus propios activos.

CONFIANZA **Alta en que publicó las reivindicaciones; acceso e impacto no verificados**

Para los defensores, la respuesta a estos actores es la mitigación DDoS en el proveedor y retirar de internet los paneles de control (§6.6).

7.4 Ransomware y extorsión

España tuvo 220 entradas en sitios de filtraciones en 2026 hasta el 20 de noviembre, frente a 35 en Portugal, 286 en Italia y 295 en Francia

ESPAÑA	PORTUGAL	ITALIA	FRANCIA
220	**35**	**286**	**295**
Anuncios aceptados, 1 ene–20 nov 2026	Anuncios aceptados, 1 ene–20 nov 2026	Anuncios aceptados, 1 ene–20 nov 2026	Anuncios aceptados, 1 ene–20 nov 2026
2025 HISTÓRICO 157 633	2025 HISTÓRICO 21 103	2025 HISTÓRICO 161 871	2025 HISTÓRICO 182 885
GRUPOS EN 2026 Qilin, The Gentlemen, Deadlock, NightSpire, SafePay, INC Ransom	GRUPOS EN 2026 The Gentlemen, Qilin, SafePay, Majinahanashi, Nova, Booba-project	GRUPOS EN 2026 Qilin, The Gentlemen, LockBit 5, SafePay, Deadlock, Space Bears	GRUPOS EN 2026 Qilin, The Gentlemen, Coinbasecartel, Lapsus$, LockBit 5, NightSpire

Fuente: anuncios aceptados de Brandefense Ransompedia, todas las fechas, hasta el 20 de noviembre de 2026 [S1].

Ransompedia registró 220 entradas aceptadas sobre España del periodo 1 de enero-20 de noviembre de 2026, ya más que las 157 de todo 2025 [S1]. Los recuentos mensuales oscilaron entre 12 y 30. Se compara un año parcial con un año completo, así que no es una tasa de crecimiento.

Qilin publicó 49, The Gentlemen 26 y Deadlock 14; les siguieron NightSpire (11) y SafePay (10). Los tres primeros suman 89 de las 220 entradas (40 %); otros 50 nombres de grupo se reparten el resto. Las etiquetas sectoriales más frecuentes fueron consultoría (27), fabricación (17), construcción (14), comercio (14) y tecnología (14). Les siguieron sanidad y una etiqueta «global» sin especificar (13 cada una).

Una entrada es una reivindicación criminal. No prueba cifrado, robo de datos ni interrupción, y a menudo la víctima no confirma nada. Varias entradas de 2026 nombraron ayuntamientos y un hospital; algunos de los organismos nombrados confirmaron un incidente y otros no (capítulo 5). La entrada de The Gentlemen sobre una filial de Indra coincide con un incidente que la empresa confirmó (§5.6).

Qilin

Agenda

Ransomware y extorsión | Motivación económica

EN ESPAÑA, 2026

2026	49 entradas sobre España en sitios de filtraciones, más que ningún otro grupo
may	Incluye en su lista una cadena española de supermercados; no se encontró confirmación

OBJETIVOS REIVINDICADOS

Fabricación, comercio, servicios, energía y organismos públicos

EN FUENTES PÚBLICAS

- [S1] Ransompedia: 49 entradas aceptadas sobre España del periodo 1 de enero-20 de noviembre de 2026

NUESTRA VALORACIÓN

El reivindicador de extorsión más frecuente contra organizaciones españolas. Una entrada es una reivindicación; planifique una recuperación que no dependa del nombre de un grupo.

CONFIANZA **Alta para los recuentos de entradas**

The Gentlemen

Ransomware y extorsión | Motivación económica

EN ESPAÑA, 2026

jun-jul	Incluye en su lista una filial de Indra; la empresa confirmó un incidente (§5.6)
oct	Incluye en su lista un hospital de Barcelona; sin confirmación a nuestra fecha de corte

OBJETIVOS REIVINDICADOS

Tecnología, sanidad, logística y servicios

EN FUENTES PÚBLICAS

- [S1] Ransompedia: 26 entradas aceptadas sobre España, solo por detrás de Qilin
- [S40] INCIBE-CERT: incidente de ciberseguridad en una filial de Indra

NUESTRA VALORACIÓN

Un reivindicador frecuente en 2026 cuyas entradas sobre España van de la tecnología a la sanidad.

CONFIANZA **Alta para los recuentos de entradas**

Para los defensores: planifique la recuperación y unas copias de seguridad probadas que no dependan de qué grupo le incluya en su lista.

Actuación policial contra la extorsión. El 30 de septiembre, una operación internacional en la que participó la Guardia Civil detuvo a tres sospechosos del grupo de extorsión KillSec. Entre ellos estaba un joven de 16 años en Alicante, sospechoso de ser su administrador. Las autoridades vincularon al grupo con más de 1.000 ataques y más de 280 víctimas, intervinieron cinco servidores y aseguraron al menos 110 TB de datos robados [S60]. La investigación en España empezó tras un ataque en 2025 contra una organización catalana.

7.5 Perfiles criminales vistos en Blackhole

Alias	Tipo de espacio	Actividad en 2026	Nota
spain	Foro de filtraciones	Oferta de la base de datos de clientes de Endesa (B01)	Coincidió con la notificación de la empresa
Koipo, Leads	Foro de filtraciones	Republicación del mismo anuncio (B02)	Perfiles que republican; contacto cambiado
[alias omitido; nombra al organismo reivindicado]	Foro de filtraciones	Reivindicación sobre una base de datos del sector público (B03)	Usuarios del foro la cuestionaron como falsa
IntelShadow	Foro de filtraciones	Nuevas subidas de datos españoles antiguos (B05)	Reenviador que busca reputación
Leonsky, daghetiaw	Foro de filtraciones	Reivindicaciones contra un comercio de electrónica (B06)	La empresa negó una brecha en sus bases de datos

Alias	Tipo de espacio	Actividad en 2026	Nota
updap	Sitio propio y foros	Reivindicaciones contra sitios policiales, de telecomunicaciones y de pagos	No verificadas; publica con frecuencia
L34ds	Telegram	«Leads» de clientes segmentados por banco (B07)	Alimenta el fraude por suplantación

Solo publicamos alias. Son perfiles, no personas identificadas, y una persona puede usar varios.

7.6 Campañas de intrusión no atribuidas

Los incidentes de Adif y Renfe, el Puerto de Vigo y el Ayuntamiento de La Laguna no tenían atribución pública a un grupo concreto a nuestra fecha de corte. El grupo de extorsión Panzer reivindicó el ataque al gobierno autonómico de Castilla-La Mancha (§5.4). Renfe afirmó que un sospechoso fue detenido en octubre [S6]. No vinculamos estos casos a ningún actor.

CONCLUSIONES CLAVE

01

Los grupos de extorsión nombraron a más organizaciones españolas que ningún otro actor; Qilin y The Gentlemen encabezaron la lista.

02

Los grupos prorrusos hicieron más ruido, y la policía actuó contra sus reclutadores en España.

03

Las investigaciones de proveedores muestran temas del Gobierno español usados como cebo de espionaje; no informan de ningún compromiso del organismo imitado.

CAPÍTULO 8

La economía del fraude

ESTE CAPÍTULO RESPONDE

¿Cómo convierten los delincuentes los datos de identidad y bancarios españoles en dinero, y dónde pueden romper la cadena los bancos, las operadoras y los organismos públicos?

180 USD

precio mediano pedido por una cuenta bancaria o de pago en las publicaciones que lo indican

EN ESTE CAPÍTULO

8.1 Comercio de cuentas bancarias y de pago | 8.2 Material de tarjetas en publicaciones: una visión limitada | 8.3 Servicios de identidad, KYC y SIM | 8.4 Los precios en contexto | 8.5 Qué comunicaron la policía y las autoridades de ciberseguridad

EN RESUMEN

El producto más anunciado en los canales clandestinos sobre España son las cuentas bancarias y de pago: cuentas ya abiertas, «cargas» de dinero y cuentas mula. Se anuncian sobre todo en canales de Telegram en español. Se alimenta de listas de clientes, documentos de identidad robados y registros de infostealers, y cobra mediante llamadas y SMS de suplantación. La policía desarticuló varias de estas redes en 2026. Bancos y operadoras deberían tratar la apertura de cuentas, los cambios de SIM y las llamadas de «cuenta segura» como una sola cadena.

8.1 Comercio de cuentas bancarias y de pago

El comercio de cuentas bancarias y de pago es la mayor parte del corpus depurado sobre España (22.417–23.173 publicaciones). Los canales de Telegram en español, que a menudo llevan nombres relacionados con la banca española, anuncian cuatro productos:

Producto	Qué se vende	Cómo se usa
Cuentas ya abiertas («cuentas creadas»)	Cuentas de bancos, neobancos y plataformas de criptomonedas abiertas con la identidad de otra persona	Para recibir y mover el dinero del fraude
Cargas	Fondos ingresados en una cuenta desde cuentas secuestradas o tarjetas robadas; quien hace la carga se queda una parte	Cobro del dinero robado
Drops	Cuentas de personas a las que se paga por prestarlas, o captadas con engaños	Mulas de dinero
«Leads» de clientes	Listas de contacto segmentadas por banco (caso D)	Selección de objetivos para llamadas y SMS de suplantación

Las publicaciones nombran como productos a bancos minoristas españoles, neobancos y entidades internacionales de dinero electrónico. Que se nombre una entidad no significa que alguien entrara en sus sistemas. Las cuentas se abren o se alquilan a nombre de otras personas. Por eso la cadena se rompe en los controles del propio banco durante el alta de clientes y en las transferencias salientes.

8.2 Material de tarjetas en publicaciones: una visión limitada

> ALCANCE DE LAS CIFRAS DE TARJETAS
>
> Estas cifras solo cubren tarjetas de pago que aparecieron en texto claro en las publicaciones de la dark web recopiladas para este informe. Brandefense detecta tarjetas robadas con muchos otros métodos que no se incluyen aquí. Las cifras no miden el robo de tarjetas ni las pérdidas por fraude.

Encontramos 759 tarjetas distintas atribuidas a España en texto claro en 624 publicaciones, con 14 emisores españoles nombrados. La mayoría apareció en resultados de bots verificadores automáticos y en publicaciones de canales, no en tiendas. Estas tarjetas importan sobre todo como prueba de que las tarjetas españolas se prueban y revenden de forma habitual. Los bancos deberían considerar expuesta cualquier tarjeta vista en texto claro y reemitirla tras validarla. Los emisores pueden recibir estas exposiciones de un proveedor de inteligencia de amenazas o mediante los programas de compromiso de las marcas de tarjetas.

8.3 Servicios de identidad, KYC y SIM

Las ofertas de KYC y documentos de identidad (11.217-11.754 publicaciones depuradas) incluyen escaneos de DNI y pasaportes españoles con selfis, paquetes de cuentas «verificadas» y plantillas de documentos falsificados. En agosto, la Policía Nacional detuvo a un estafador que, según afirmó, usaba un deepfake generado con IA para obtener certificados de firma electrónica a nombre de terceros [S61]. En noviembre, la Policía Nacional detuvo a cuatro personas en Málaga por una red que usaba IA para crear sitios web fraudulentos, además de phishing y fraude por SMS [S62]. También se venden cuentas de Telegram con números españoles (+34) para usarlas en estafas.

8.4 Los precios en contexto

Producto	Precio mediano pedido (USD)	Mitad central de los precios (USD)
Cuenta bancaria y de pago	180	70-350
KYC y documentos de identidad	100	35-250
Ofertas de carding	80	15-300
Venta de accesos	80	23-300
Kits de phishing y servicios de estafa	60	25-250
Filtraciones y bases de datos	20	10-50

Los precios son precios pedidos en las publicaciones que los indican, convertidos cuando hace falta; no son precios de transacción. Los precios de las bases de datos son bajos porque la mayoría de las ofertas son reventas de datos antiguos. Una cuenta bancaria cuesta más que una base de datos porque permite mover dinero.

8.5 Qué comunicaron la policía y las autoridades de ciberseguridad

Fecha	Organismo	Qué se anunció
Enero	Policía Nacional con Europol	34 detenidos en una red de compromiso del correo electrónico empresarial vinculada a Black Axe; pérdidas de más de 6 millones de dólares en 15 años [S63]
Marzo	Policía Nacional	Dos detenidos por el robo de casi diez millones de registros de una plataforma educativa autonómica (un robo conocido en 2023, distinto del caso de julio del §5.7 y no incluido entre los 30), monetizados después mediante fraude y ventas clandestinas [S64]

Fecha	Organismo	Qué se anunció
Mayo	Guardia Civil	15 detenidos en una red de llamadas de suplantación bancaria que obtuvo unos 400.000 euros [S65]
Junio	Policía Nacional	Una red de fraude por WhatsApp del «hijo en apuros» que obtuvo casi 3 millones de euros [S66]
Julio	Policía Nacional	Una red que obtuvo 140 millones de euros mediante fraude informático [S67]
Julio	Guardia Civil	Operación Fragmenta: red de smishing con una base de datos de unas 500.000 personas; unas 2.000 posibles víctimas [S8]
Septiembre	Guardia Civil	Operación Ibermellow: red de SMS de suplantación bancaria; 29 detenidos, más de un millón de euros [S7]
Octubre	Policía Nacional	El brazo de blanqueo de una red de ciberfraude que invertía las ganancias en vino y maquinaria industrial [S68]

INCIBE emitió en 2026 avisos repetidos sobre campañas de SMS y correo que suplantaban a la Agencia Tributaria, a la Seguridad Social y a la DGT con falsos reembolsos y multas [S69][S70][S71]. La AEPD informó de que se usaron datos robados de reservas hoteleras para contactar con huéspedes y exigirles pagos. Según la agencia, esos casos explicaron buena parte del aumento de sus notificaciones de brechas en julio [S72].

Qué significa. El mercado y el registro policial describen la misma cadena: entran listas e identidades robadas, las llamadas y SMS de suplantación generan el pago y las cuentas mula se llevan el dinero. Cada eslabón tiene una organización española que puede romperlo. El banco, en el alta y en las transferencias; la operadora, en los cambios de SIM; el organismo público, publicando cómo contacta realmente con la ciudadanía.

CONCLUSIONES CLAVE

01

El comercio de cuentas bancarias es la familia delictiva más anunciada en los datos sobre España.

02

Según la policía e INCIBE, la suplantación de bancos, de la Agencia Tributaria y de la DGT es una vía recurrente para convertir datos robados en dinero.

03

Las operaciones policiales de 2026 golpearon todos los eslabones de la cadena, del robo de datos al blanqueo.

CAPÍTULO 9

Análisis en profundidad: banca y finanzas

ESTE CAPÍTULO RESPONDE

¿Cuánta exposición tienen los bancos y las entidades de pago de España, y está esa exposición en los bancos o en sus clientes?

25 de 25

organizaciones de banca y pagos con asociaciones de dispositivos infectados

EN ESTE CAPÍTULO

9.1 Qué dicen las cifras | 9.2 Cómo leerlo | 9.3 Contexto regulatorio

EN RESUMEN

Las 25 organizaciones de banca y pagos evaluadas tienen asociaciones de dispositivos infectados. Casi todas quedan fuera de la clasificación de empleados; no está establecido a quién pertenecen esos dispositivos ni si los datos son actuales. De esas organizaciones, 17 tenían una credencial anunciada a la venta el día de la comprobación. Los bancos aplican la autenticación del correo mejor que cualquier otro sector. Valide primero los anuncios vigentes y ejecute en paralelo las comprobaciones de cuentas de empleados y los controles de fraude a clientes.

143.948

asociaciones de dispositivos infectados (límite inferior), 298 de ellas clasificadas como de empleados

17 de 25

tenían una credencial anunciada a la venta el día de la comprobación

23 de 25

aplican DMARC (15 reject, 8 quarantine)

9.1 Qué dicen las cifras

Señal	Banca y pagos (25 organizaciones)
Anuncio vigente de credenciales / historial de anuncios	17 / 17 organizaciones
Asociaciones de dispositivos infectados	143.948, límite inferior; 298 clasificadas como de empleados
Cuota de dispositivos en las tres mayores organizaciones	42 %
Registros de credenciales	135.365 (68.859 de bases de datos de brechas, 6.686 de registros de stealers, 59.820 de combolists)
Documentos expuestos / dominios similares en 30 días	20 / 23 organizaciones
DMARC aplicado / delegación DNSSEC	23 / 5 organizaciones
Tarjetas distintas en texto claro que nombran un banco de esta lista	414 en 13 bancos; tres bancos concentran el 70 %

Fuente: calificaciones de exposición de Atlas y asociaciones de Blackhole leídas el 21 de noviembre de 2026 [S2][S3]; comprobaciones DNS [S22]. Las cifras de tarjetas siguen el alcance del §8.2.

9.2 Cómo leerlo

- **Sobre todo fuera de la clasificación de empleados.** De las 143.948 asociaciones, 143.650 no están clasificadas como de empleados. Proceden de registros de stealers en dispositivos que accedieron a la banca en línea. Muchos pueden ser ordenadores de clientes, pero no están establecidas ni su titularidad ni su vigencia. Son una señal de fraude para el banco, no una prueba de intrusión.
- **Los anuncios van primero.** De las 25 organizaciones, 17 tenían una credencial anunciada a la venta el día de la comprobación. Valide si esas cuentas son de clientes o de personal antes de actuar.
- **Concentración.** Tres grandes bancos minoristas concentran el 42 % de las asociaciones de dispositivos. Los tres bancos con más tarjetas vistas en texto claro, que no son todos los mismos, concentran el 70 % de esas tarjetas. Los bancos más pequeños, las cooperativas de crédito y los neobancos también aparecen en las publicaciones de comercio de cuentas (capítulo 8).
- **La higiene es sólida.** La banca lidera todos los sectores en aplicación de DMARC. Esto dificulta la suplantación directa de los dominios bancarios y empuja a los delincuentes hacia dominios similares y nombres de remitente de SMS.

9.3 Contexto regulatorio

INCIBE informó de que la banca supuso el 34 % de los 401 incidentes que gestionó en operadores esenciales en 2025 [S20]. DORA se aplica a las entidades financieras españolas desde enero de 2025 (capítulo 10). Las operaciones policiales de 2026 contra redes de suplantación bancaria muestran dónde recaen las pérdidas: en clientes que autorizan transferencias bajo presión (capítulo 8).

CONCLUSIONES CLAVE

01

Las asociaciones de dispositivos de la banca quedan sobre todo fuera de la clasificación de empleados; su titularidad y su vigencia no están establecidas.

02

Los anuncios vigentes de credenciales en 17 de las 25 organizaciones de banca y pagos son las primeras cuentas que hay que validar.

03

Un DMARC sólido desplaza la suplantación hacia dominios similares, SMS y llamadas.

CAPÍTULO 10

Regulación y respuesta nacional

ESTE CAPÍTULO RESPONDE

¿Qué normas se aplican ya a las organizaciones españolas mientras llega la NIS2, qué hicieron los reguladores y la policía en 2026 y qué debería hacer un CISO antes de que llegue la ley?

17 oct 2024

plazo de transposición de la NIS2 que España aún no ha cumplido

EN ESTE CAPÍTULO

10.1 Normas que se aplican hoy | 10.2 Qué supone el retraso de la NIS2 | 10.3 Qué comunicaron los reguladores en 2026 | 10.4 Qué comunicó la policía en 2026 | 10.5 Qué deberían hacer ahora los CISO

EN RESUMEN

La ley española de la NIS2 sigue en borrador, pero no hay un vacío normativo. Ya se aplican la notificación de brechas de datos personales, el Esquema Nacional de Seguridad para el sector público y sus proveedores, el decreto vigente de seguridad de redes y DORA en finanzas. La AEPD informó de más notificaciones de brechas y señaló las de software de reservas; la policía desarticuló varias redes de fraude y hacktivistas. Relacione sus obligaciones con las normas vigentes y prepárese para la NIS2 sin esperar a su texto.

10.1 Normas que se aplican hoy

Norma	A quién se aplica	Qué exige	A quién notificar	Situación a nuestra fecha de corte
Reglamento General de Protección de Datos de la UE (RGPD) y Ley Orgánica 3/2018 (LOPDGDD)	Toda organización que trate datos personales	Los responsables notifican a la autoridad sin dilación indebida y, si es posible, en 72 horas desde que tienen constancia, salvo que sea improbable que la brecha suponga un riesgo para las personas. Los encargados notifican al responsable sin dilación indebida. Los responsables informan a los afectados cuando sea probable un riesgo alto, salvo que se aplique una excepción (RGPD, arts. 33-34)	La AEPD; los organismos públicos de Cataluña, el País Vasco y Andalucía notifican a su autoridad autonómica (APDCAT, AVPD o Consejo de Transparencia y Protección de Datos de Andalucía)	En vigor
Esquema Nacional de Seguridad (ENS), Real Decreto 311/2022	Organismos del sector público y proveedores privados de sus sistemas	Categorización de seguridad, medidas de control, notificación de incidentes	Organismos públicos: CCN-CERT. Proveedores privados: INCIBE-CERT, que traslada la notificación al CCN-CERT	En vigor
Real Decreto-ley 12/2018 y Real Decreto 43/2021 (transposición de NIS1)	Operadores de servicios esenciales y proveedores de servicios digitales	Medidas de seguridad y notificación de incidentes	El CSIRT competente: INCIBE-CERT para operadores privados, CCN-CERT para el sector público; los operadores relevantes para la defensa nacional notifican a su CSIRT, que informa al ESPDEF-CERT	En vigor hasta su sustitución

Norma	A quién se aplica	Qué exige	A quién notificar	Situación a nuestra fecha de corte
Reglamento de Resiliencia Operativa Digital de la UE (DORA)	Bancos, aseguradoras, empresas de servicios de inversión y otras entidades financieras	Gestión del riesgo TIC, notificación de incidentes graves, supervisión de terceros	La autoridad competente: Banco de España para los bancos (el BCE supervisa los bancos significativos; confirme el canal de notificación con su supervisor), la CNMV o la Dirección General de Seguros y Fondos de Pensiones (DGSFP)	Se aplica desde el 17 de enero de 2025
Directiva (UE) 2022/2555 (NIS2)	Entidades esenciales e importantes de 18 sectores	Responsabilidad de la dirección, medidas de riesgo, alerta temprana en 24 horas	Aún no fijado en la ley española	Sin transponer; el anteproyecto no se había presentado a las Cortes Generales a nuestra fecha de corte

Fuentes: `[S73][S74][S75][S76][S77][S78][S18][S19]`. Esta tabla es una ayuda de planificación, no asesoramiento jurídico. Consulte los textos consolidados en el Boletín Oficial del Estado (BOE) antes de basarse en cualquier fila.

10.2 Qué supone el retraso de la NIS2

La Comisión Europea llevó a España ante el Tribunal de Justicia el 8 de julio de 2026 por no comunicar la transposición completa, y pidió una suma a tanto alzado y multas coercitivas diarias `[S18]`. El anteproyecto de ley, publicado en enero de 2025, no se había presentado a nuestra fecha de corte. Su calendario legislativo futuro es incierto. El artículo 21 de la Ley del Gobierno limita la presentación de proyectos de ley por un gobierno en funciones `[S79]`. La transposición mediante real decreto-ley sigue siendo jurídicamente posible `[S19]`.

Hasta entonces, las entidades que cubriría la NIS2 no tienen una ley española de NIS2. Los organismos públicos pueden verse afectados por disposiciones con efecto directo, y muchas entidades ya están sujetas al ENS, a NIS1 o a DORA.

En la práctica, el retraso cambia el plazo, no el trabajo. La NIS2 pide cosas que los incidentes de 2026 muestran que hacen falta en cualquier caso: seguridad de los proveedores, autenticación multifactor, copias de seguridad probadas y notificación rápida.

10.3 Qué comunicaron los reguladores en 2026

La Agencia Española de Protección de Datos (AEPD) publica informes mensuales sobre notificaciones de brechas. Recibió 788 notificaciones en marzo y 919 en julio de 2026 `[S80][S72]`. Su informe de julio destacó a los hoteles y sus proveedores de software de reservas: los delincuentes usaron datos robados de reservas para contactar con huéspedes y exigirles el pago de las reservas `[S72]`. En septiembre, la AEPD informó de la primera notificación de brecha en España en la que el ataque se describía como ejecutado por un agente de IA. La agencia subrayó que los detalles proceden de la organización notificante y aún requieren análisis `[S46]`.

10.4 Qué comunicó la policía en 2026

La policía española anunció varias operaciones contra grupos cuya actividad coincide con las amenazas de este informe. Las operaciones de fraude y robo de datos figuran en el §8.5; la tabla siguiente añade los casos de hacktivismo, extorsión y otros relacionados. Los recogemos tal como se anunciaron; una detención no es una condena.

Fecha	Cuerpo	Qué se anunció
Febrero	Guardia Civil	Detenidos los cuatro principales miembros del grupo hacktivista Anonymous Fénix por ataques DDoS contra organismos públicos, dos de ellos en 2025 `[S58]`
Julio (detención en marzo)	Policía Nacional, tras un aviso del FBI	Detención de un presunto colaborador de los grupos prorrusos CARR y Z-Pentest `[S81]`

Fecha	Cuerpo	Qué se anunció
30 de septiembre	Guardia Civil y socios	Operación internacional contra el grupo de extorsión KillSec; detenido en Alicante un joven de 16 años, presunto administrador [S60]
Noviembre	Policía Nacional	Anuncio de la detención en Burgos del presunto principal instigador en España de NoName057(16) [S10] [S54]

10.5 Qué deberían hacer ahora los CISO

1. **Mapee las obligaciones actuales.** Enumere cuáles de estas normas se aplican a su organización y a cada proveedor crítico: RGPD, ENS, NIS1 y DORA.
2. **Ensaye el reloj de notificación.** Desde que tenga constancia de una brecha, practique si notificarla a la AEPD o a su autoridad autonómica en 72 horas. Decida también si informar a los afectados. Incluya a los equipos jurídico y de comunicación y al proveedor.
3. **Redacte cláusulas de aviso de brechas para los proveedores.** Los encargados deben avisarle sin dilación indebida, y las cláusulas deben permitirle cumplir su propio plazo. Cuatro de los 30 incidentes confirmados de 2026 de este informe empezaron en un proveedor (capítulo 5).
4. **Prepare ya el expediente NIS2.** La aprobación por el consejo de las medidas de riesgo, un inventario de activos y un procedimiento de alerta temprana en 24 horas servirán para cualquier ley que se apruebe.

CONCLUSIONES CLAVE

01

La NIS2 se retrasa en España, pero la notificación de brechas, el ENS y DORA ya se aplican.

02

Los reguladores señalaron las brechas en proveedores y en software de reservas como una fuente creciente de notificaciones.

03

Las operaciones policiales de 2026 se dirigieron contra la misma actividad de fraude y hacktivismo que observa este informe.

CAPÍTULO 11

Perspectivas

ESTE CAPÍTULO RESPONDE

¿Para qué deberían prepararse ahora las organizaciones españolas y qué evidencias cambiarían ese plan?

5
juicios clave, cada uno con una señal que vigilar

EN ESTE CAPÍTULO

11.1 Juicios clave | 11.2 Qué cambiaría la valoración | 11.3 Escenarios condicionales

EN RESUMEN

Planifique para las amenazas que se repitieron en 2026. Los incidentes con datos de clientes en grandes marcas de consumo y sus proveedores, la extorsión a organismos públicos pequeños, el fraude por suplantación bancaria y las oleadas DDoS prorrusas breves volvieron durante el año. La intrusión asistida por IA apareció por primera vez en información oficial. Las entradas de extorsión ya superan su total de 2025, como en los países vecinos; no hay otras series comparables. Asigne un responsable a cada señal y revise el plan cada mes.

11.1 Juicios clave

Juicio	Confianza	Base y límite
La exposición de identidad (dispositivos, registros de stealers, anuncios de credenciales) es el riesgo medible más extendido para las principales organizaciones de España	Alta para la lista de 250 organizaciones	241 con dispositivos, 243 con registros de credenciales, 163 con anuncios vigentes; no es prevalencia nacional
Si la actividad de los grupos se mantiene, los grupos de extorsión seguirán incluyendo organizaciones españolas a un ritmo similar al de 2026	Media (condicional)	220 entradas hasta el 20 de noviembre de 2026, frente a 157 en todo 2025; Portugal, Italia y Francia superaron sus totales de 2025 por márgenes mayores. Las entradas son reivindicaciones y la actividad de los grupos cambia rápido
Los incidentes con datos de clientes seguirán empezando en proveedores y sistemas secundarios	Media	Cinco de los incidentes confirmados de 2026 empezaron en un proveedor o un sistema secundario; muestra pequeña
Si los canales de los actores siguen citando el apoyo español a Ucrania, planifique para reivindicaciones DDoS prorrusas contra sitios públicos	Media (hipótesis de planificación)	La oleada de febrero lo citó; señal: listas de objetivos en canales de actores
Los agentes de IA aparecerán en más informes de intrusión	Baja a media	Una notificación a la AEPD, una detención de la Guardia Civil de un intruso que, según afirmó, usaba IA (§5.4), e informaciones de prensa no confirmadas sobre Renfe y Adif (§5.3); la AEPD dijo que esta primera notificación no establece una tendencia estadística `[S46][S32][S26]`

11.2 Qué cambiaría la valoración

Interpretación actual	Evidencia que la cambiaría	Decisión afectada
La mayoría de las grandes reivindicaciones de bases de datos contra organismos del Estado no están verificadas o son falsas	Una confirmación oficial, o una muestra que coincida con un esquema conocido	Activar la notificación y las medidas de protección de clientes para ese conjunto de datos

Interpretación actual	Evidencia que la cambiaría	Decisión afectada
Las oleadas DDoS son breves	Confirmación oficial de una caída prolongada de un servicio esencial	Revisar la capacidad de mitigación en el proveedor y los planes de continuidad
Las reivindicaciones sobre control industrial no están verificadas	Un operador o una autoridad confirma la manipulación de un proceso físico	Priorizar en todo el sector la retirada de las interfaces de control de internet
Los anuncios vigentes significan «validar», no «brecha»	La validación encuentra cuentas activas sin MFA entre las credenciales anunciadas	Escalar a respuesta a incidentes e imponer MFA a los usuarios afectados
La NIS2 aún no es ley en España	Publicación de la ley de transposición en el BOE	Redefinir obligaciones, plazos y canales de notificación

11.3 Escenarios condicionales

Estos escenarios son hipótesis de planificación, no intervalos medidos.

- **Si** una gran empresa de consumo confirma un incidente con datos de clientes, **entonces** planifique para phishing y llamadas a sus clientes que citen datos reales del contrato. **Señal:** la notificación de la empresa y las publicaciones de reventa. **Decisión:** avisar a los clientes e informar a los centros de atención al cliente el mismo día.
- **Si** un canal prorruso publica una lista de objetivos que nombra a su sector, **entonces** planifique para ráfagas DDoS breves en los días siguientes. **Señal:** enlaces de comprobación de disponibilidad en canales de actores. **Decisión:** activar la mitigación en el proveedor y el comunicado de estado acordado de antemano.
- **Si** se divulga una nueva vulnerabilidad crítica en un producto expuesto a internet, **entonces** planifique para intentos de explotación por grupos de extorsión. **Señal:** avisos de fabricantes y alertas del CCN-CERT o de INCIBE-CERT. **Decisión:** parchear y verificar primero los sistemas expuestos a internet y después buscar persistencia.

CONCLUSIONES CLAVE

01

Planifique para las amenazas que se repitieron todo el año: incidentes con datos de clientes, extorsión, fraude por suplantación y DDoS.

02

Cada juicio tiene una señal; cambie el plan cuando cambie la señal.

03

La intrusión asistida por IA ya consta en España, pero un caso aún no es una tendencia.

CAPÍTULO 12

Plan de acción

ESTE CAPÍTULO RESPONDE

¿Qué debería hacer cada equipo en los próximos 90 días y cómo sabrá el consejo que se ha hecho?

23
acciones con responsable y evidencia de cumplimiento

EN ESTE CAPÍTULO

12.1 30/60/90 días | 12.2 Por función | 12.3 Cómo puede ayudar Brandefense

EN RESUMEN

Empiece por confirmar que recibe alertas de anuncios de credenciales y de dispositivos, y actúe después sobre la evidencia que le afecta: anuncios vigentes, dispositivos de empleados y sistemas expuestos a internet. A continuación, cierre las carencias de proveedores, correo y fraude a clientes, y ensaye un escenario combinado de DDoS y filtración de datos. El consejo sabrá que el trabajo está hecho por la evidencia de cumplimiento de cada fila y por el cuadro de mando siguiente; informe de ambos antes del día 90.

12.1 30/60/90 días

Es una secuencia, no un periodo de espera. Una amenaza material actual debería entrar de inmediato en su proceso de gestión de incidentes.

1 Días 1-30

Confirme que recibe alertas de anuncios de credenciales y de dispositivos infectados para sus dominios principales, del proveedor o servicio que elija; si no, organícelo

RESPONSABLE
CISO e inteligencia de amenazas

EVIDENCIA DE CUMPLIMIENTO
Fuente de alertas identificada; primera alerta recibida

Para cada anuncio vigente de credenciales vinculado a sus dominios, valide la cuenta y su estado de MFA en 5 días hábiles

RESPONSABLE
Equipo de identidad

EVIDENCIA DE CUMPLIMIENTO
Cada anuncio tiene una resolución con fecha: restablecida, ya corregida o no es nuestra

Valide las asociaciones de dispositivos clasificados como de empleados; revoque sesiones y tokens si están activos

RESPONSABLE
Equipos de identidad y de endpoints

EVIDENCIA DE CUMPLIMIENTO
Lista de dispositivos conciliada con el inventario de activos; revocaciones registradas

2 Días 31-60

Donde DMARC esté en p=none o falte, inventaríe los remitentes y aplique la política por fases

RESPONSABLE
Mensajería

EVIDENCIA DE CUMPLIMIENTO
Remitentes alineados; p=quarantine con vía de vuelta atrás

Acuerde quién puede activar la mitigación DDoS en el proveedor y el filtrado geográfico por tiempo limitado para los portales públicos, y pruébelo

RESPONSABLE
Infraestructura

EVIDENCIA DE CUMPLIMIENTO
Registro de la prueba con el tiempo de activación

Parchee y verifique los sistemas expuestos a internet según los avisos del CCN-CERT y de INCIBE-CERT sobre vulnerabilidades explotadas

RESPONSABLE
Infraestructura

EVIDENCIA DE CUMPLIMIENTO
Lista de sistemas expuestos a internet con fechas de parcheo

3 Días 61-90

Realice una prueba cronometrada de restauración de un sistema crítico

RESPONSABLE
Infraestructura

EVIDENCIA DE CUMPLIMIENTO
Tiempo de restauración registrado frente al objetivo de tiempo de recuperación

Firme el DNS de los dominios principales donde el registrador lo permita; corrija los certificados TLS no válidos

RESPONSABLE
Equipos de red y web

EVIDENCIA DE CUMPLIMIENTO
DNSSEC valida desde un resolvedor externo; los certificados superan la comprobación

Realice un ejercicio de mesa que combine una oleada DDoS con una reivindicación simultánea de filtración de datos

RESPONSABLE
CISO, comunicación, jurídico

EVIDENCIA DE CUMPLIMIENTO
Registro de decisiones y tiempos

Enumere todos los proveedores que custodian datos de sus clientes y pregúnteles con qué rapidez le notificarán una brecha

RESPONSABLE
Compras, jurídico y CISO

EVIDENCIA DE CUMPLIMIENTO
Lista de proveedores con un compromiso de notificación por proveedor

Designe al portavoz y el canal para los comunicados sobre el estado del servicio durante un DDoS y ante reivindicaciones de filtración no verificadas

RESPONSABLE
Comunicación, CISO y jurídico

EVIDENCIA DE CUMPLIMIENTO
Un protocolo de una página, aprobado

Ensaye con el área jurídica y un proveedor clave la decisión de notificación de brechas del RGPD y su plazo de 72 horas

RESPONSABLE
Delegado de protección de datos y jurídico

EVIDENCIA DE CUMPLIMIENTO
Registro del ejercicio cronometrado

Mapee las obligaciones de RGPD, ENS, NIS1 y DORA para su organización y cada proveedor crítico, incluido a quién notificar (§10.1)

RESPONSABLE
Jurídico y CISO

EVIDENCIA DE CUMPLIMIENTO
Registro de obligaciones

Priorice los dominios similares y solicite la retirada de los sitios de phishing confirmados (§3.5)

RESPONSABLE
Inteligencia de amenazas y jurídico

EVIDENCIA DE CUMPLIMIENTO
Lista de dominios similares con una resolución por dominio

Organismos públicos: publiquen sus canales oficiales de contacto y lo que nunca piden a la ciudadanía

RESPONSABLE
Comunicación

EVIDENCIA DE CUMPLIMIENTO
Página publicada y enlazada desde la página de inicio

Retire de internet las interfaces web de control industrial y de edificios, o colóquelas tras una VPN y autenticación fuerte

RESPONSABLE
OT e instalaciones

EVIDENCIA DE CUMPLIMIENTO
Una comprobación externa no muestra paneles de control expuestos

Bancos y entidades de pago: añadan fricción a las primeras transferencias a nuevos beneficiarios y a los patrones de «cuenta segura»; repitan los avisos a clientes

RESPONSABLE
Fraude y canales digitales

EVIDENCIA DE CUMPLIMIENTO
Regla activa; aviso enviado

Operadoras de telecomunicaciones: exijan verificación fuerte para los cambios de SIM y la portabilidad de números

RESPONSABLE
Fraude y operaciones de clientes

EVIDENCIA DE CUMPLIMIENTO
Procedimiento aprobado; caso de prueba detectado

Indique a los centros de atención al cliente que nunca pidan datos bancarios completos ni códigos en contactos entrantes, y que avisen a los clientes que denuncien estas llamadas

RESPONSABLE
Operaciones de clientes

EVIDENCIA DE CUMPLIMIENTO
Guion actualizado; personal informado

Pase a los usuarios privilegiados y remotos a MFA resistente al phishing (llaves FIDO2, passkeys o certificados)

RESPONSABLE
Equipo de identidad

EVIDENCIA DE CUMPLIMIENTO
Cobertura registrada por grupo de usuarios

Prepare el expediente NIS2: aprobación por el consejo de las medidas de riesgo, un inventario de activos y un procedimiento de alerta temprana en 24 horas (§10.5)

RESPONSABLE
CISO y secretaría del consejo

EVIDENCIA DE CUMPLIMIENTO
Expediente aprobado por el consejo

Informe del cuadro de mando frente a los objetivos (abajo)

RESPONSABLE
CISO al consejo

EVIDENCIA DE CUMPLIMIENTO
Documento para el consejo con las carencias pendientes y sus responsables

Bloquee las macros en documentos procedentes de internet y alerte de conexiones salientes desde servidores hacia servicios de webhook

RESPONSABLE
Endpoints y SOC

EVIDENCIA DE CUMPLIMIENTO
Política aplicada; alerta probada

Objetivos del cuadro de mando. Son valores sugeridos por defecto; fije los suyos donde su política sea distinta.

Medida	Objetivo
Anuncios vigentes con resolución en 5 días hábiles	100 % antes del día 90
Dispositivos clasificados como de empleados conciliados con el inventario de activos	100 % antes del día 90
Proveedores con datos de clientes que tienen un compromiso de notificación de brechas	100 % antes del día 90
Dominios principales con DMARC en quarantine o reject	100 %, o un plan con fechas, antes del día 90
Usuarios privilegiados y remotos con MFA resistente al phishing	100 %, o un plan con fechas, antes del día 90
Prueba de restauración dentro del objetivo de tiempo de recuperación	Superada, o una corrección con fecha, antes del día 90

12.2 Por función

Función	Primera decisión
Consejo	Pida sus cifras de anuncios vigentes y de dispositivos de empleados, y la fecha en que se validará cada una
CISO	Implante la monitorización de anuncios y dispositivos; después, la notificación de proveedores y el parcheo de lo expuesto a internet
SOC	Añada detecciones de documentos con macros, conexiones desde servidores a servicios de webhook e inicios de sesión desde dispositivos nuevos en cuentas vistas en registros de stealers (§3.3, caso E)
Fraude	Vigile las primeras transferencias a nuevos beneficiarios, los cambios de SIM y las cuentas que reciben y reenvían fondos en pocas horas
Comunicación	Prepare comunicados para DDoS y para reivindicaciones de filtración no verificadas, separando reivindicación, hecho verificado y acción

CONCLUSIONES CLAVE

01
Confirme la monitorización y después valide los anuncios vigentes de credenciales y los dispositivos de empleados en los primeros 30 días.

02
Cierre las carencias de proveedores, DMARC, paneles de control y fraude a clientes antes del día 60.

03
Pruebe la restauración, firme el DNS y ensaye un escenario combinado de DDoS y filtración antes del día 90.

12.3 Cómo puede ayudar Brandefense

Brandefense combina inteligencia de ciberamenazas (Cyber Threat Intelligence), protección frente a riesgos digitales (Digital Risk Protection) y gestión de la superficie de ataque externa (External Attack Surface Management). El análisis de este informe usó los mismos datos y calificaciones que la plataforma aplica a las organizaciones monitorizadas. Son asociaciones de dispositivos infectados y de credenciales, anuncios vigentes en

mercados de credenciales, dominios similares, documentos expuestos y menciones en la dark web. No promete que todas las reivindicaciones puedan verificarse ni que un registro histórico siga siendo utilizable.

Traiga sus dominios, marcas y prioridades de seguridad a una demo de 30-45 minutos con nuestro equipo. El equipo puede mostrar cómo la monitorización de la plataforma relaciona las señales externas con los activos que usted gestiona. Un miembro del equipo de Brandefense o un socio de su región se pondrá en contacto con usted.

Solicitar una demo

Anexo A. Método

A.1 Periodo, fuentes y prioridad

El periodo de investigación es 1 de enero-20 de noviembre de 2026, según la fecha en que se publicó cada publicación o entrada, no la fecha de su recogida. Los datos propios van primero: Brandefense Blackhole, Ransompedia y las calificaciones de exposición de Brandefense Atlas. Blackhole aporta publicaciones de la dark web y de mensajería, asociaciones de dispositivos infectados y credenciales y material de tarjetas en publicaciones. Ransompedia aporta entradas de sitios de filtraciones de ransomware.

Las fuentes externas aportan contexto y solo se citan tras leer el pasaje que las respalda. Los datos se extrajeron el 21 de noviembre de 2026. Los datos propios de Brandefense no tienen dirección pública; cada fuente externa del Anexo C lleva un enlace y una fecha de verificación.

A.2 Publicaciones de Blackhole

Elemento	Valor
Publicaciones con la etiqueta de país España	932.584
Familia de bots en turco	Alrededor del 87 % de las publicaciones etiquetadas; ruido publicitario
Publicaciones relevantes tras la depuración	58.657-62.086, un rango y no un recuento único

Los recuentos depurados siguen siendo un límite superior de la actividad delictiva: algunos canales publican la misma oferta a diario y algunas publicaciones se refieren a varios países a la vez. El pico de enero y febrero de la familia de bots aparece en todos los países de comparación. Su aumento de junio y julio es mucho mayor en España que en cualquier país de comparación, y se debe a plantillas en turco. No interpretamos ninguno de los dos picos como propio de España.

A.3 Las 250 organizaciones

La población y los límites figuran en el §3.1. Cada organización recibió una calificación de exposición de Atlas. Los recuentos de señales medidos del capítulo 3 se presentan por separado de la calificación. Los datos se leyeron el 21 de noviembre de 2026. Algunos totales de dispositivos son límites inferiores.

A.4 Calificaciones de Atlas

Cada organización recibió una calificación de exposición de Atlas. Este informe solo publica la cifra principal nacional (66), no calificaciones sectoriales ni de organizaciones. Trate un anuncio vigente en un mercado de credenciales como motivo para validar cuentas, no como prueba de una brecha.

A.5 Comprobaciones de DNS, TLS y web

Los resultados de correo, DNS, TLS y página de inicio proceden de comprobaciones públicas y pasivas hechas el 21 de noviembre de 2026. Se considera que DMARC se aplica con una política reject o quarantine. Con p=none o sin registro, no se aplica.

A.6 Material de tarjetas en publicaciones

Alcance: solo tarjetas de pago que aparecieron en texto claro en las publicaciones de la dark web recopiladas para este informe. Brandefense detecta tarjetas robadas con muchos otros métodos, que quedan fuera de este informe. Estas cifras no miden el robo de tarjetas ni las pérdidas por fraude. Las cifras se presentan solo por emisor.

A.7 Ransomware

Usamos las entradas aceptadas de Ransompedia para España, Portugal, Italia y Francia, fechadas por su publicación. Las cifras de 2026 cubren del 1 de enero al 20 de noviembre y las de 2025 el año completo, así que la comparación no es una tasa de crecimiento con periodos equivalentes.

A.8 Cobertura de incidentes

La cobertura de incidentes se basa en publicaciones de Blackhole y en información pública de todo el periodo. Las fuentes públicas incluyen prensa nacional y regional, información de INCIBE, INCIBE-CERT y CCN-CERT, notas de prensa del Ministerio del Interior sobre la Policía Nacional y la Guardia Civil, la AEPD e investigaciones de proveedores.

Límites de cobertura.

- Las ventas acordadas en privado dejan pocas huellas públicas, así que los recuentos de publicaciones las subestiman.
- Pueden faltar publicaciones retiradas pronto.
- Los incidentes que las organizaciones gestionan sin divulgarlos siguen siendo invisibles.

Que un incidente no figure en este informe no significa que no ocurriera.

A.9 Confianza y límites

La confianza alta se aplica a una medición reproducible, no a la afirmación de fondo de un delincuente. La confianza media indica una interpretación con un respaldo claro y límites declarados. La etiqueta «no verificado» significa no establecido de forma independiente; no es prueba de invención ni prueba de una brecha. Las organizaciones víctimas se describen por su función. Solo se nombra a una organización cuando ella misma o una autoridad confirmó el incidente y este tuvo amplia difusión.

Los casos confirmados más pequeños se describen por su función aunque la fuente citada los nombre (§5.1). Se publican los alias de los actores; se omiten enlaces, contactos, indicadores y datos personales. La procedencia completa se conserva en un registro interno de evidencias.

Anexo B. Registro de evidencias

Cada publicación citada en este informe aparece como ficha de publicación anonimizada en el capítulo indicado. Los extractos son breves y las omisiones se marcan con [...]. Los identificadores, contactos, enlaces y organizaciones víctimas se sustituyen por etiquetas entre corchetes, según la política del apartado A.9. Las traducciones al español son nuestras. Las fechas de publicación no son fechas de intrusión. Los identificadores, enlaces y textos completos de las publicaciones se conservan internamente.

Ficha	Publicada	Espacio	Alias mostrado	Idioma	Se muestra en
B01	2026-01-04	Foro de filtraciones	spain	Inglés	§4.4
B02	2026-02-16	Foro de filtraciones	Koipo	Inglés	§4.6
B03	2026-01-31	Foro de filtraciones	[alias omitido; nombra al organismo reivindicado]	Inglés, con nombres de campo en español	§4.4
B04	2026-02-02	Foro de filtraciones	Usuario del foro	Inglés	§4.4

Ficha	Publicada	Espacio	Alias mostrado	Idioma	Se muestra en
B05	2026-01-30	Foro de filtraciones	IntelShadow	Inglés, con nombres de campo en español	§4.6
B06	2026-02-05	Foro de filtraciones	Leonsky	Inglés	§4.4
B07	2026-02-28	Canal de Telegram de servicios bancarios	L34ds	Español e inglés	§4.6
B08	2026-01-01	Canal de Telegram en español de fraude bancario	Autor anónimo	Español	§4.6
B09	2026-03-03	Canal de Telegram en español que reenvía a NoName057(16)	Administrador del canal	Español	§6.4
B10	2026-02-16	Canal en español que reenvía a Server Killers	Server Killers (reenviado)	Español	§6.2
B11	2026-02-16	Canal de DDoSia Project	NoName057(16)	Ruso	§6.2
B12	2026-02-16	Canal en español que reenvía a Z-Pentest Alliance	Z-Pentest Alliance (reenviado)	Español	§6.3
B13	2026-01-26	Canal hacktivista de Telegram	BD Anonymous Team	Inglés, tal como se publicó	§6.5
B14	2026-08-21	Sitio de filtraciones propio del perfil	updap	Inglés	§4.5
B15	2026-06-26	Foro de filtraciones (bot automatizado)	Bot del foro	Inglés	§4.6
B16	2026-11-04	Foro de filtraciones	Perfil de foro	Inglés	§4.6

Anexo C. Fuentes

S1 Brandefense Ransompedia, entradas aceptadas de España, Portugal, Italia y Francia, extraídas el 21 de noviembre de 2026.

S2 Calificaciones de exposición de Brandefense Atlas y asociaciones de Blackhole de dispositivos infectados, bases de datos de brechas, registros de stealers y combolists para 250 dominios, leídas el 21 de noviembre de 2026.

S3 Corpus de publicaciones de Brandefense Blackhole relativas a España, con fecha de publicación 1 de enero-20 de noviembre de 2026, extraído el 21 de noviembre de 2026.

S4 INCIBE, "Endesa notifica a sus clientes una filtración de datos personales". https://www.incibe.es/ciudadania/avisos/endesa-notifica-sus-clientes-una-filtracion-de-datos-personales. Verificado el 21 de noviembre de 2026.

S5 OCU, "Filtración de datos en Naturgy". https://www.ocu.org/tecnologia/ciberseguridad/noticias/filtracion-datos-naturgy. Verificado el 21 de noviembre de 2026.

S6 Diario Avanza, "Renfe alerta de un ciberataque que pudo exponer DNI, contraseñas y viajes de sus clientes". https://www.diarioavanza.es/nacional/renfe-alerta-ciberataque-que-pudo-exponer-dni-contrasenas-viajes-clientes/20261120090703031011.html. Verificado el 21 de noviembre de 2026.

S7 Moncloa.com (sitio de noticias privado), "La Guardia Civil desarticula en la operación Ibermellow una red de ciberestafas bancarias con 29 detenidos". https://www.moncloa.com/2026/09/15/guardia-civil-operacion-ibermellow-ciberestafas-detenidos-3431938/. Verificado el 21 de noviembre de 2026.

S8 CLM24, "La Guardia Civil desmantela una red con datos de 500.000 personas". https://www.clm24.es/articulo/toledo/guardia-civil-desmantela-red-datos-500000-personas/20260722125737480099.html. Verificado el 21 de noviembre de 2026.

S9 Escudo Digital, "El grupo pro-ruso Noname057(16) vuelve a paralizar distintas instituciones españolas con ataques DDoS". https://www.escudodigital.com/ciberseguridad/ataques-ddos-gobierno-espana-noname057.html. Verificado el 21 de noviembre de 2026.

S10 Moncloa.com (sitio de noticias privado), "La Policía Nacional detiene en Burgos al instigador de la célula en España del ciberterrorismo prorruso NoName057(16)". https://www.moncloa.com/2026/11/20/policia-nacional-noname057-ciberterrorismo-burgos-3471612/. Verificado el 21 de noviembre de 2026.

S11 Recorded Future Insikt Group, "BlueDelta targets defense and diplomacy with HOOKEDGE". https://www.recordedfuture.com/research/bluedelta-targets-with-hookedge. Verificado el 21 de noviembre de 2026.

S12 ESET, "ESET uncovers the expanded arsenal of China-aligned Webworm; European governments targeted". https://www.eset.com/us/about/newsroom/research/eset-research-china-aligned-webworm-european-governments-targeted/. Verificado el 21 de noviembre de 2026.

S13 DataReportal (Kepios), "Digital 2027: Spain". https://datareportal.com/reports/digital-2027-spain. Verificado el 21 de noviembre de 2026.

S14 El Español, "España ya es, tras Ucrania e Israel, el país más atacado por hackers rusos y chinos, según el último informe del CNI". https://elespanol.com/espana/20260711/espana-ucrania-israel-pais-atacado-hackers-rusos-chinos-ultimo-informe-cni/1003744316174_0.amp.html. Verificado el 21 de noviembre de 2026.

S15 El Español, "El CNI advierte que España es uno de los países más ciberatacados del mundo". https://www.elespanol.com/observatorio-defensa/20260505/cni-advierte-espana-paises-ciberatacados-mundo-toda-clase-artefactos/1003744233968_0.html. Verificado el 21 de noviembre de 2026.

S16 Legal Today, "El BOE publica el Real Decreto de disolución de las Cortes y la convocatoria electoral para el 29 de noviembre". https://www.legaltoday.com/actualidad-juridica/noticias-de-derecho/el-boe-publica-el-real-decreto-de-disolucion-de-las-cortes-y-la-convocatoria-electoral-para-el-29-de-noviembre-2026-10-06/. Verificado el 21 de noviembre de 2026.

S17 Demócrata, "Interior pone en marcha la red de seguridad para anticipar riesgos como ciberataques y desinformación el 29N". https://www.democrata.es/politica/interior-pone-en-marcha-la-red-de-seguridad-para-anticipar-riesgos-como-ciberataques-y-desinformacion-el-29n/. Verificado el 21 de noviembre de 2026.

S18 European Commission, "Commission refers Ireland, Spain, France and the Netherlands to the Court of Justice for failing to transpose rules". https://digital-strategy.ec.europa.eu/en/news/commission-refers-ireland-spain-france-and-netherlands-court-justice-failing-transpose-rules. Verificado el 21 de noviembre de 2026.

S19 Cuatrecasas, "Ciberataques en sectores críticos: a la espera de NIS2". https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/ciberataques-sectores-criticos-espera-nis2. Verificado el 21 de noviembre de 2026.

S20 España Digital / INCIBE, "INCIBE gestionó 122.223 incidentes de ciberseguridad en 2025, un 26% más que el año anterior". https://espanadigital.gob.es/actualidad/incibe-gestiono-122223-incidentes-de-ciberseguridad-en-2025-un-26-mas-que-el-ano. Verificado el 21 de noviembre de 2026.

S21 3Cat, "Ciberatacs informàtics: es doblen els ciberincidents a sistemes públics". https://www.3cat.cat/3catinfo/ciberatacs-informatics-es-doblen-el-nombre-de-ciberincidents-a-sistemes-publics/noticia/3406320/. Verificado el 21 de noviembre de 2026.

S22 Comprobaciones públicas de Brandefense de DNS, TLS y páginas de inicio de 250 dominios, 21 de noviembre de 2026.

S23 PcComponentes, "Actualización importante oficial sobre la seguridad de los datos". https://www.pccomponentes.com/actualizacion-importante-oficial-seguridad-datos. Verificado el 21 de noviembre de 2026.

S24 Escudo Digital, "Información sobre un organismo público que descartó una supuesta brecha de una base de datos, febrero de 2026". https://www.escudodigital.com/ (URL del artículo omitida). Verificado el 21 de noviembre de 2026.

S25 The Register, "Spanish power giant sparks breach probe amid claims of massive data grab". https://www.theregister.com/2026/01/14/endesa_breach/. Verificado el 21 de noviembre de 2026.

S26 Maldita, "Qué sabemos sobre el uso de inteligencia artificial en el ciberataque a Renfe y Adif". https://maldita.es/desinfo/20260929/renfe-sufre-un-ciberataque-siendo-el-primero-realizado-con-inteligencia-artificial-a-un-organismo-publico-en-espana/. Verificado el 21 de noviembre de 2026.

S27 The Cyber Express, "Port Of Vigo Cyberattack Disrupts Cargo Systems". https://thecyberexpress.com/port-of-vigo-cyberattack-disrupts-systems/. Verificado el 21 de noviembre de 2026.

S28 Escudo Digital, "Las copias de seguridad salvan al Concello de Sanxenxo de un ataque de ransomware". https://www.escudodigital.com/ciberseguridad/las-copias-de-seguridad-salvan-al-concello-de-sanxenxo-de-un-ataque-de-ransomware.html. Verificado el 21 de noviembre de 2026.

S29 Escudo Digital, "El Ministerio de Ciencia reconoce haber sufrido un hackeo, aunque con un alcance muy limitado". https://www.escudodigital.com/ciberseguridad/ministerio-ciencia-filtracion-datos.html. Verificado el 21 de noviembre de 2026.

S30 Escudo Digital, "El Ayuntamiento de Valdemoro sufre un ciberataque". https://www.escudodigital.com/ciberseguridad/ayuntamiento-valdemoro-ciberataque-ransomware.html. Verificado el 21 de noviembre de 2026.

S31 MiCiudadReal, "Suspendida la Plataforma de gestión de la Zona de Bajas Emisiones de Ciudad Real debido a un "incidente" de ciberseguridad". https://www.miciudadreal.es/2026/06/16/suspendida-la-plataforma-de-gestion-de-la-zona-de-bajas-emisiones-de-ciudad-real-debido-a-un-incidente-de-ciberseguridad/. Verificado el 21 de noviembre de 2026.

S32 Ministerio del Interior, "La Guardia Civil detiene en Ciudad Real a un hacker que utilizaba inteligencia artificial para perpetrar ciberataques". https://www.interior.gob.es/opencms/es/detalle/articulo/La-Guardia-Civil-detiene-en-Ciudad-Real-a-un-hacker-que-utilizaba-inteligencia-artificial-para-perpetrar-ciberataques/. Verificado el 21 de noviembre de 2026.

S33 Escudo Digital, "Castilla-La Mancha confirma el ciberataque de Panzer". https://www.escudodigital.com/ciberseguridad/castilla-la-mancha-confirma-el-ciberataque-de-panzer-que-reivindica-el-robo-de-datos-de-alumnos-y-familias.html. Verificado el 21 de noviembre de 2026.

S34 RTVC, "Un incidente de ciberseguridad afecta a varios sistemas y servicios digitales del Ayuntamiento de La Laguna". https://rtvc.es/incidente-ciberseguridad-afecta-varios-sistemas-servicios-digitales-ayuntamiento-la-laguna-2-noviembre-2026/. Verificado el 21 de noviembre de 2026.

S35 Escudo Digital, "Un ciberataque obliga a la Universidad de Alicante a desactivar parte de sus servicios digitales". https://www.escudodigital.com/ciberseguridad/universidad-alicante-ciberataque.html. Verificado el 21 de noviembre de 2026.

S36 Escudo Digital, "La Universitat de València confirma haber sufrido un ciberataque". https://www.escudodigital.com/ciberseguridad/la-universitat-de-valencia-confirma-haber-sufrido-un-ciberataque.html. Verificado el 21 de noviembre de 2026.

S37 INCIBE-CERT, "Acceso no autorizado a información clínica del Servicio Extremeño de Salud". https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/acceso-no-autorizado-informacion-clinica-del-servicio-extremeno-de-salud. Verificado el 21 de noviembre de 2026.

S38 FashionUnited, "Inditex suffers cyberattack". https://fashionunited.com/news/business/inditex-suffers-cyberattack/2026041671809. Verificado el 21 de noviembre de 2026.

S39 Escudo Digital, "Basic-Fit sufre una brecha de datos que afecta a sus usuarios españoles". https://www.escudodigital.com/ciberseguridad/basic-fit-sufre-una-brecha-de-datos-que-afecta-a-sus-usuarios-espanoles.html. Verificado el 21 de noviembre de 2026.

S40 INCIBE-CERT, "Cybersecurity incident at an Indra subsidiary". https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/cybersecurity-incident-indra-subsidiary. Verificado el 21 de noviembre de 2026.

S41 Escudo Digital, "Lidl informa a sus clientes en España sobre una filtración de datos". https://www.escudodigital.com/ciberseguridad/lidl-informa-a-sus-clientes-en-espana-sobre-una-filtracion-de-datos.html. Verificado el 21 de noviembre de 2026.

S42 GCN, "Breach at Spanish ministry vendor exposes sensitive information". https://gcn.com/breach-at-spanish-exposes-sensitive-information/17490/. Verificado el 21 de noviembre de 2026.

S43 RTVC, "La web del Ayuntamiento de Adeje sufre un ciberataque". https://rtvc.es/la-web-del-ayuntamiento-de-adeje-sufre-un-ciberataque-21-enero-20267/. Verificado el 21 de noviembre de 2026.

S44 INCIBE-CERT, "Investigation into a possible data breach relating to Leroy Merlin's Hogami". https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/investigation-possible-data-breach-relating-leroy-merlins-hogami. Verificado el 21 de noviembre de 2026.

S45 Merca2, "Ciberataque a la Junta de Andalucía: datos de profesores y alumnos del sistema Séneca, en riesgo". https://www.merca2.es/2026/07/26/ciberataque-junta-andalucia-sistema-seneca-2424273/. Verificado el 21 de noviembre de 2026.

S46 AEPD, "Primera notificación de una brecha de datos personales causada por un ataque ejecutado mediante un agente de IA". https://www.aepd.es/prensa-y-comunicacion/blog/primera-notiviacion-brecha-datos-personales-causada-por-ataque-ejecutado-mediante-agente-ia. Verificado el 21 de noviembre de 2026.

S47 INCIBE-CERT, "Security incident in Levante UD systems with possible impact on personal data". https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/security-incident-levante-ud-systems-possible-impact-personal-data. Verificado el 21 de noviembre de 2026.

S48 Escudo Digital, "GAME sufre un ciberataque que expone los datos personales e historiales de compra de sus clientes". https://www.escudodigital.com/ciberseguridad/game-ciberataque-brecha-datos.html. Verificado el 21 de noviembre de 2026.

S49 INCIBE-CERT, "Interrail takes action after security incident exposes its passengers' data". https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/interrail-takes-action-after-security-incident-exposes-its-passengers-data. Verificado el 21 de noviembre de 2026.

S50 INCIBE-CERT, "Detection of unauthorised access to Booking user data". https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/detection-unauthorized-access-booking-user-data. Verificado el 21 de noviembre de 2026.

S51 UOC, "Un incidente de seguridad del proveedor Canvas afecta a la UOC". https://www.uoc.edu/es/news/2026/un-incidente-de-seguridad-del-proveedor-canvas-afecta-a-la-uoc. Verificado el 21 de noviembre de 2026.

S52 INCIBE-CERT, "Data breach at Revolut following fraudulent government requests". https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/data-breach-revolut-following-fraudulent-government-requests. Verificado el 21 de noviembre de 2026.

S53 Escudo Digital, "Smartbox sufre un ciberataque que expone los nombres y correos de sus clientes". https://www.escudodigital.com/ciberseguridad/smartbox-cajas-regalo-ciberataque-brecha-seguridad.html. Verificado el 21 de noviembre de 2026.

S54 Ministerio del Interior, "La Policía Nacional frustra la implantación de la primera célula en España de la organización ciberterrorista NoName057(16)". https://www.interior.gob.es/opencms/en/detail-pages/article/La-Policia-Nacional-frustra-la-implantacion-de-la-primera-celula-en-Espana-de-la-organizacion-ciberterrorista-NoName05716/. Verificado el 21 de noviembre de 2026.

S55 CISA, FBI, NSA y socios, "Pro-Russia hacktivists conduct opportunistic attacks against US and global critical infrastructure (AA25-343A)". https://media.defense.gov/2025/Dec/09/2003840175/-1/-1/0/JOINT_CSA_PRO-RUSSIA_HACKTIVISTS_CONDUCT_ATTACKS_AGAINST_CRITICAL_INFRASTRUCTURE.PDF. Verificado el 21 de noviembre de 2026.

S56 Escudo Digital, "Información sobre una filtración de datos personales de altos cargos públicos, enero de 2026". https://www.escudodigital.com/ (URL del artículo omitida). Verificado el 21 de noviembre de 2026.

S57 Escudo Digital, "Hackers prorrusos filtran los datos de cientos de policías, guardias civiles y militares españoles". https://www.escudodigital.com/ciberseguridad/hackers-prorrusos-filtran-los-datos-de-cientos-de-policias-guardias-civiles-y-militares-espanoles.html. Verificado el 21 de noviembre de 2026.

S58 Ministerio del Interior, "Detenidos los cuatro principales integrantes del grupo hacktivista Anonymous Fénix por ciberataques contra organismos públicos". https://www.interior.gob.es/opencms/es/detalle/articulo/Detenidos-los-cuatro-principales-integrantes-del-grupo-hacktivista-Anonymous-Fenix-por-ciberataques-contra-organismos-publicos/. Verificado el 21 de noviembre de 2026.

S59 Help Net Security, "Spanish police arrest suspected Anonymous members over DDoS attacks on government sites". https://www.helpnetsecurity.com/2026/02/23/spain-guardia-civil-arrests-anonymous-fenix-ddos-attacks/. Verificado el 21 de noviembre de 2026.

S60 INCIBE-CERT, "Arrest in Alicante in the international operation against KillSec". https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/arrest-alicante-international-operation-against-killsec. Verificado el 21 de noviembre de 2026.

S61 Ministerio del Interior, "La Policía Nacional detiene a un ciberdelincuente que utilizaba una técnica pionera mediante IA para obtener certificados de firma electrónica". https://www.interior.gob.es/opencms/es/detalle/articulo/La-Policia-Nacional-detiene-a-un-ciberdelincuente-que-utilizaba-una-tecnica-pionera-mediante-IA-para-obtener-certificados-de-firma-electronica/. Verificado el 21 de noviembre de 2026.

S62 El Español, "Cae en Málaga una red que usaba inteligencia artificial para crear webs falsas y estafar a víctimas de toda España". https://elespanol.com/malaga/20261119/cae-malaga-red-usaba-inteligencia-artificial-crear-webs-falsas-estafar-victimas-toda-espana/1003744464404_0.html. Verificado el 21 de noviembre de 2026.

S63 BleepingComputer, "Spain arrests 34 suspects linked to Black Axe cyber crime". https://www.bleepingcomputer.com/news/security/spain-arrests-34-suspects-linked-to-black-axe-cyber-crime/. Verificado el 21 de noviembre de 2026.

S64 Escudo Digital, "La Policía desarticula una organización criminal autora del robo de diez millones de registros confidenciales". https://www.escudodigital.com/interior/la-policia-desarticula-una-organizacion-criminal-autora-del-robo-de-diez-millones-de-registros-confidenciales.html. Verificado el 21 de noviembre de 2026.

S65 Ministerio del Interior, "Desarticulada una red criminal que estafó 400.000 euros mediante llamadas que simulaban ser bancos". https://www.interior.gob.es/opencms/en/detail-pages/article/Desarticulada-una-red-criminal-que-estafo-400.000-euros-mediante-llamadas-que-simulaban-ser-bancos/. Verificado el 21 de noviembre de 2026.

S66 Ministerio del Interior, "La Policía Nacional desarticula un entramado criminal por estafar casi 3.000.000 de euros mediante el método del hijo en apuros". https://www.interior.gob.es/opencms/es/detalle/articulo/La-Policia-Nacional-desarticula-un-entramado-criminal-por-estafar-casi-3.000.000-de-euros-mediante-el-metodo-del-hijo-en-apuros/. Verificado el 21 de noviembre de 2026.

S67 Ministerio del Interior, "La Policía Nacional desarticula una organización criminal que se apropió de 140 millones de euros mediante fraudes informáticos". https://www.interior.gob.es/opencms/es/detalle/articulo/La-Policia-Nacional-desarticula-una-organizacion-criminal-que-se-apropio-de-140-millones-de-euros-mediante-fraudes-informaticos/. Verificado el 21 de noviembre de 2026.

S68 Ministerio del Interior, "Desarticulada la red de blanqueo de una organización de ciberdelincuencia que inyectaba el dinero de las estafas en compra de vino y maquinaria industrial". https://www.interior.gob.es/opencms/es/detalle/articulo/Desarticulada-la-red-de-blanqueo-de-una-organizacion-de-ciberdelincuencia-que-inyectaba-el-dinero-de-las-estafas-en-compra-de-vino-y-maquinaria-industrial/. Verificado el 21 de noviembre de 2026.

S69 INCIBE, "La Agencia Tributaria NO ha emitido ninguna comunicación dirigida a usted". https://www.incibe.es/ciudadania/avisos/la-agencia-tributaria-no-ha-emitido-ninguna-comunicacion-dirigida-usted. Verificado el 21 de noviembre de 2026.

S70 INCIBE, "Campaña de smishing suplantando a la Seguridad Social". https://www.incibe.es/ciudadania/avisos/campana-de-smishing-suplantando-la-seguridad-social. Verificado el 21 de noviembre de 2026.

S71 INCIBE, "Correos y SMS suplantan a la DGT para robar tus datos con falsas multas". https://www.incibe.es/ciudadania/avisos/correos-y-sms-suplantan-la-dgt-para-robar-tus-datos-con-falsas-multas. Verificado el 21 de noviembre de 2026.

S72 AEPD, "Notificaciones de brechas de datos personales, julio 2026". https://www.aepd.es/documento/informe-brechas-julio-2026.pdf. Verificado el 21 de noviembre de 2026.

S73 EUR-Lex, "Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos), artículos 33-34". https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng. Verificado el 21 de noviembre de 2026.

S74 Boletín Oficial del Estado, "Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (texto consolidado)". https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673. Verificado el 21 de noviembre de 2026.

S75 Boletín Oficial del Estado, "Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (texto consolidado)". https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191. Verificado el 21 de noviembre de 2026.

S76 Boletín Oficial del Estado, "Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (texto consolidado)". https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257. Verificado el 21 de noviembre de 2026.

S77 Boletín Oficial del Estado, "Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018 (texto consolidado)". https://www.boe.es/buscar/act.php?id=BOE-A-2021-1192. Verificado el 21 de noviembre de 2026.

S78 ECB Banking Supervision, "Operational resilience in the digital age". https://www.bankingsupervision.europa.eu/press/blog/2025/html/ssm.blog20250117~32b79d4efa.en.html. Verificado el 21 de noviembre de 2026.

S79 Boletín Oficial del Estado, "Ley 50/1997, de 27 de noviembre, del Gobierno, artículo 21 (texto consolidado)". https://www.boe.es/buscar/act.php?id=BOE-A-1997-25336. Verificado el 21 de noviembre de 2026.

S80 AEPD, "Notificaciones de brechas de datos personales, marzo 2026". https://www.aepd.es/documento/informe-brechas-marzo-2026.pdf. Verificado el 21 de noviembre de 2026.

S81 Ministerio del Interior, "La Policía Nacional detiene a un presunto colaborador de los grupos hacktivistas prorrusos CyberArmy of Russia Reborn (CARR) y Z-Pentest". https://www.interior.gob.es/opencms/es/detalle/articulo/La-Policia-Nacional-detiene-a-un-presunto-colaborador-de-los-grupos-hacktivistas-prorrusos-CyberArmy-of-Russia-Reborn-CARR-y-Z-Pentest/. Verificado el 21 de noviembre de 2026.

Anexo D. Glosario

- **AEPD:** Agencia Española de Protección de Datos, la autoridad española de protección de datos.
- **BEC:** compromiso del correo electrónico empresarial (business email compromise), fraude que suplanta por correo a un proveedor o a un directivo.
- **BIN:** los primeros dígitos de un número de tarjeta, que identifican al emisor.
- **CARR:** CyberArmy of Russia Reborn, un grupo hacktivista prorruso nombrado en el aviso encabezado por CISA.
- **CCN y CCN-CERT:** el Centro Criptológico Nacional y su CERT, que presta servicio al sector público español.
- **APDCAT y AVPD:** las autoridades catalana y vasca de protección de datos, que supervisan a los organismos públicos de sus territorios.
- **CNI:** Centro Nacional de Inteligencia, el servicio de inteligencia español, del que depende el CCN.
- **CNMV:** Comisión Nacional del Mercado de Valores, el supervisor español del mercado de valores.
- **DGSFP:** Dirección General de Seguros y Fondos de Pensiones, el supervisor español de seguros y fondos de pensiones.
- **BCE:** el Banco Central Europeo, que supervisa directamente a los bancos significativos de la zona del euro.
- **ESPDEF-CERT:** el CERT de las Fuerzas Armadas españolas para el sector de la defensa.
- **Entidad de dinero electrónico:** una entidad autorizada que emite dinero electrónico y cuentas de pago, pero que no es un banco.
- **IBEX:** el IBEX 35, el principal índice de la Bolsa de Madrid.
- **INCIBE e INCIBE-CERT:** el Instituto Nacional de Ciberseguridad y su CERT, que presta servicio a la ciudadanía y a las empresas privadas.
- **Neobanco:** un banco o entidad de pago que atiende a sus clientes solo mediante aplicaciones y la web.
- **Stresser:** un servicio de pago que satura un objetivo con peticiones; se vende como prueba de carga y se usa para DDoS.
- **Blackhole:** la fuente de datos de ciberdelincuencia de Brandefense, que cubre publicaciones, dispositivos infectados, credenciales y material de tarjetas.
- **Ransompedia:** la base de datos de ransomware de Brandefense; sus entradas recogen reivindicaciones criminales.
- **Atlas:** la calificación de exposición externa de Brandefense; va de 0 (nada observado) a 100.

- **Dispositivo infectado:** un dispositivo cuyo registro de stealer contiene un inicio de sesión en el dominio de la organización; «empleado» es una clasificación según el uso, no un empleo verificado.
- **Anuncio en un mercado de credenciales:** una credencial vinculada al dominio que se ofrece en un mercado monitorizado en el momento de la comprobación.
- **Combolist:** una lista de pares de usuario y contraseña reunidos de diversas fuentes; su antigüedad y validez varían.
- **Registro de stealer:** datos capturados de un dispositivo por malware de robo de información.
- **Relleno de credenciales (credential stuffing):** probar contraseñas filtradas de un servicio en cuentas de otro servicio.
- **Bot verificador:** un bot que prueba tarjetas robadas contra pasarelas de pago e imprime el resultado.
- **Ficha de publicación:** una reproducción anonimizada de una publicación de la dark web, con espacio, fecha, alias, idioma y lo que establece y no establece.
- **Reenvío:** un canal o bot de terceros que vuelve a publicar la reivindicación de otro actor; es una evidencia más débil que la publicación propia del actor.
- **Cargas:** dinero ingresado en una cuenta desde cuentas secuestradas o tarjetas robadas, para cobrarlo.
- **Drops y cuentas mula:** personas, y cuentas abiertas a su nombre, usadas para recibir y mover el dinero del fraude.
- **Smishing y vishing:** phishing por SMS y por teléfono.
- **DDoS:** denegación de servicio distribuida; saturar un sitio con peticiones para que los usuarios legítimos no puedan acceder.
- **Filtrado geográfico:** limitar el acceso a un servicio a visitantes de determinados países.
- **DMARC / SPF / DKIM:** estándares de autenticación del correo; DMARC indica a los receptores qué hacer con el correo que no supera la comprobación.
- **DNSSEC y registro DS:** firmas que permiten a los resolvedores verificar las respuestas DNS, y el registro de la zona superior que vincula un dominio con sus claves.
- **HSTS:** una cabecera web que indica a los navegadores que usen solo HTTPS.
- **MFA (autenticación multifactor):** un inicio de sesión que exige un segundo factor además de la contraseña.
- **MFA resistente al phishing:** inicio de sesión vinculado al sitio real (llaves FIDO2, passkeys o certificados), de modo que una página intermediaria no puede reutilizarlo.
- **KYC:** controles de identidad «conozca a su cliente» en bancos, plataformas de intercambio y otros servicios.
- **OT / SCADA / HMI:** tecnología operativa, los sistemas de control de supervisión que gestionan procesos físicos y sus pantallas de interfaz persona-máquina.
- **C2:** mando y control, la infraestructura que usa un atacante para dirigir el malware.
- **Servicio de webhook:** un servicio web que recibe peticiones HTTP; los atacantes abusan de los gratuitos para el mando y control.
- **ENS:** el Esquema Nacional de Seguridad para los sistemas de información del sector público y sus proveedores.
- **NIS2:** la directiva de la UE sobre seguridad de las redes y sistemas de información que España aún no ha transpuesto.
- **DORA:** el Reglamento de Resiliencia Operativa Digital de la UE para entidades financieras.
- **Cifra principal nacional:** la cifra única de Atlas para toda la lista de 250 organizaciones.
- **TLP:CLEAR:** puede compartirse sin restricciones; otras obligaciones legales siguen aplicándose.

Acerca de este informe

Elaborado por Odin by Brandefense. La versión 1.0 se completó el 21 de noviembre de 2026. Sustituye a un borrador anterior de Brandefense sobre España, preparado en octubre de 2026, con datos nuevos y una evaluación de 250 organizaciones.

Fecha de corte de la investigación: 20 de noviembre de 2026. Las elecciones generales del 29 de noviembre de 2026 son posteriores a la fecha de corte. Solo se mencionan como fecha, como contexto de planificación y por su efecto en el calendario legislativo. El informe prioriza los datos propios de Brandefense, separa las reivindicaciones criminales de los incidentes establecidos de forma independiente y no pretende ofrecer un censo completo de la ciberdelincuencia que afecta a España. Las recomendaciones describen lo que las organizaciones podrían hacer; no afirman

que ninguna organización las haya aplicado o no. Esta edición en español se ha traducido con IA a partir de la edición en inglés de la versión 1.0; la edición en inglés prevalece en caso de discrepancia.

© 2026 Brandefense. Todos los derechos reservados.