perseus
cybersecurity services

PERSEUS

Informe Semestral de Ciberinteligencia

PERSEUS
Informe Semestral de Ciberinteligencia

Organización solicitante
PERSEUS

Referencia propuesta
CTI-INF-2026-S1

Elaborada por
Unidad de Ciberinteligencia PERSEUS
comercial@pers.eus

Fecha
4 de agosto de 2026

This document may not be reproduced, in whole or in part, nor shown to others, nor used for purposes other than those that originated its delivery by PERSEUS , without the prior written permission of Perseus. Its use will be limited to the valuation as a technical offer. Perseus cannot be held responsible for eventual errors or omissions in the editing of the document.

Índice

1 Resumen ejecutivo 4
1.1 Seis conclusiones del semestre 5
1.2 Qué ha cambiado respecto al semestre anterior 5
2 Vulnerabilidades: el semestre en cifras 6
2.1 Volumen y evolución 6
2.2 Cada vez más fallos graves 7
2.3 Lo que de verdad se acaba explotando 8
2.4 Qué productos se atacan 9
3 Quién ataca: grupos y campañas 10
3.1 Cuántos grupos hay y cuáles están activos 10
3.2 Grupos vinculados a Estados 10
3.2.1 República Popular China 10
3.2.2 Federación Rusa 11
3.2.3 Corea del Norte 11
3.2.4 Irán 11
3.3 Ransomware y extorsión 11
3.3.1 Cada vez más grupos, cada vez más pequeños 11
3.3.2 Cuántas víctimas y a qué ritmo 12
3.3.3 Del cifrado a la amenaza de publicar 12
3.3.4 Cuánto cuesta y cuánto se tarda en volver a la normalidad 13
3.3.5 Quién ataca a España 13
3.4 Qué buscan los atacantes en cada fase 13
3.5 Las técnicas más usadas 15
3.6 Lo que más ha crecido 15
3.7 Ataques sin malware 18
3.8 Inteligencia artificial en el ataque 18
4 Qué sectores reciben más ataques 20
4.1 Perfil de los seis sectores más atacados 20
4.1.1 Administración pública 20
4.1.2 Tecnología y proveedores de servicios 20
4.1.3 Sector financiero 21
4.1.4 Industria y entornos industriales 21
4.1.5 Sanidad 21

4.1.6 Transporte y logística 22
4.2 Por dónde entran y cuánto cuesta, sector a sector 22
4.3 Quién ataca y por qué, según el sector 22
4.4 Lo que cuesta una brecha 23
4.5 Con qué frecuencia ocurre 23
5 Europa y España 25
5.1 Dónde se concentra la actividad 25
5.2 España en nuestros datos 25
5.3 España comparada con sus vecinos 25
5.4 Qué tipo de ataques recibe España 26
5.5 Cifras nacionales de incidentes 27
6 Qué esperamos del segundo semestre 29
6.1 Cuántas vulnerabilidades esperamos 29
6.2 Escenarios previstos 30
6.3 Qué amenazas pesan más 32
7 Recomendaciones 33
7.1 Los próximos noventa días 33
7.2 De aquí a fin de año 33
7.3 Qué medir 34
8 Cómo trabajamos 35
8.1 Anticipar lo que viene 35
8.2 Conocer y reducir la exposición 35
8.3 Detectar y responder a tiempo 35
8.4 Controlar el acceso y proteger el dato 35
8.5 Gobernar y sostener en el tiempo 35
9 Anexos 36
9.1 Anexo A · Glosario 36

1 Resumen ejecutivo

El primer semestre de 2026 ha sido el periodo con más actividad hostil que PERSEUS ha registrado desde que lleva series comparables. Y no es el repunte de un mes suelto: la subida aparece en todos los indicadores que seguimos, se mantiene trimestre a trimestre y aguanta el contraste con las redes de compartición en las que participamos. Entre enero y junio se han publicado **35.364 vulnerabilidades**, un **49,5 % más** que en el mismo periodo de 2025 y un **73,6 % más** que en 2024: una nueva cada siete minutos y medio, sin pausa, durante seis meses. Pero lo que más pesa no es el volumen sino su composición: **el 49,1 % son de severidad alta o crítica**, frente al 39,4 % del conjunto de 2025.

Ese dato resume bien el semestre. Los atacantes no han inventado técnicas nuevas: ha industrializado las que ya funcionaban y ha desplazado su esfuerzo hacia los puntos donde la defensa tiene menos visibilidad. Desde PERSEUS observamos tres movimientos de fondo que recorren todo el análisis y que ayudan a leer todo lo que viene después.

El perímetro ha vuelto a ser el frente principal. Los dispositivos de borde —cortafuegos, concentradores VPN, controladores de red, pasarelas de gestión— concentran una proporción desmedida de las vulnerabilidades de máxima gravedad del semestre y son, además, donde el tiempo entre la publicación y la explotación se ha reducido casi a cero. Siete de las diez vulnerabilidades con puntuación 10,0 y explotación confirmada que hemos catalogado en el semestre afectan a este tipo de equipos. Son sistemas que rara vez soportan agentes de detección, que no suelen entrar en las ventanas de mantenimiento ordinarias y que, por diseño, están expuestos a internet.

La identidad se ha consolidado como el hilo conductor de la intrusión. Ya no es un vector más entre otros: es el elemento que aparece en prácticamente todas las cadenas de ataque que hemos reconstruido, en un punto u otro. En nuestra telemetría, las técnicas asociadas a la obtención y el abuso de credenciales concentran los mayores crecimientos individuales del semestre. La técnica *Unsecured Credentials* (T1552) se multiplica por casi nueve respecto al trimestre anterior, y *Kerberoasting* (T1558.003) por once. El adversario dedica cada vez menos esfuerzo a romper el perímetro y cada vez más a autenticarse legítimamente contra él.

El borrado de huellas se ha convertido en una fase estándar de la operación. Es, con diferencia, el desplazamiento más llamativo del semestre y el que más nos preocupa desde el punto de vista de la detección. La técnica *Indicator Removal* (T1070) pasa de 89 a 398 observaciones entre los dos últimos trimestres, y su variante específica de borrado de registros de eventos de Windows (T1070.001) se multiplica por nueve y medio. Un adversario que limpia sistemáticamente detrás de sí no solo dificulta la respuesta: degrada la calidad de la propia inteligencia futura.

Indicador del primer semestre	2024	2025	2026	Var. 26/25
Vulnerabilidades publicadas	20.374	23.656	**35.364**	**+49,5 %**
Media diaria	111,9	130,7	**195,4**	**+49,5 %**
CVSS medio	6,65	6,57	**6,89**	**+4,9 %**
Altas en el catálogo KEV	—	132	**146**	**+10,6 %**
Actores con actividad registrada	368	221	**703**	**+218,1 %**

Figura 1. Cuadro de indicadores del primer semestre. Comparativa 2024–2026 sobre las series de PERSEUS.

1.1 Seis conclusiones del semestre

1. El volumen de vulnerabilidades ha entrado en un régimen distinto. El primer semestre supera por sí solo cualquier año completo anterior a 2024, y crítica y alta suman ya el 49,1 % de lo publicado frente al 39,4 % del conjunto de 2025. La severidad ha dejado de servir como criterio de priorización.
2. La explotación real no acompaña. De las 35.364 vulnerabilidades del semestre, apenas 85 tienen evidencia pública de explotación: el 0,24 %. El problema no es que se explote más, sino que resulta cada vez más difícil anticipar qué se va a explotar.
3. Los dispositivos de borde son el objetivo preferente. Siete de las diez vulnerabilidades de puntuación máxima con explotación confirmada afectan a equipamiento de red o appliances de seguridad, y presentan los tiempos de armamentización más cortos medidos.
4. Evadir la detección es la prioridad número uno del atacante: concentra el 24,0 % de la actividad observada. Borrar el rastro se ha incorporado al manual estándar —el borrado de indicadores se multiplica por 4,5— y el 82 % de las detecciones ya no implica malware.
5. El ransomware fragmenta y cambia de modelo: noventa y un grupos distintos publicando víctimas, un 13,8 % más de víctimas que el semestre anterior, y una tasa de pago que cae del 78,9 % de 2022 al 28,8 %. La extorsión se desplaza del cifrado a la amenaza de publicar.
6. España no recibe menos ataques que Europa: tiene menos averías. Está por encima de la media europea en caídas por ataque externo y es tercera de la Unión en ransomware. El retraso en la transposición de NIS2 la sitúa además en posición asimétrica.

1.2 Qué ha cambiado respecto al semestre anterior

Un informe semestral corre el riesgo de describir un estado sin señalar el movimiento. Interesa por tanto separar lo que continúa de lo que ha cambiado. Continúa el crecimiento del catálogo de vulnerabilidades, la centralidad del ransomware como amenaza de mayor impacto y el predominio de las técnicas de evasión. Cambia, y bastante, la velocidad a la que se convierte una vulnerabilidad publicada en un incidente, la profundidad con la que el adversario borra sus huellas y la proporción de operaciones que prescinden por completo del malware tradicional.

El cambio más difícil de asimilar para un equipo de seguridad es el tercero. Durante quince años la defensa se ha construido alrededor de la idea de detectar algo que no debería estar ahí: un binario, un proceso, una conexión anómala. Cuando el adversario opera con credenciales válidas, herramientas legítimas del sistema y utilidades de administración remota contratadas por la propia organización, esa premisa deja de sostenerse. La detección tiene que moverse del artefacto al comportamiento, y esa transición es cara, lenta y difícil de justificar ante un comité que ya ha aprobado inversiones en la generación anterior de herramientas.

CONCLUSIONES RÁPIDAS

El semestre no exige una revisión estratégica: exige acelerar decisiones ya tomadas. Tres de ellas concentran la mayor parte del riesgo reducible a corto plazo.

Reducir el tiempo de parcheo del perímetro por debajo de las 72 horas. No de todo el parque: exclusivamente de los sistemas expuestos a internet y de los appliances de seguridad. Es la única medida que actúa sobre el vector con menor margen de reacción.

Cerrar la brecha de autenticación resistente a *phishing*. El segundo factor basado en códigos o notificaciones ya no protege frente a las técnicas observadas este semestre. La prioridad es la administración, los accesos remotos y las cuentas de servicio.

Proteger la telemetría como se protege un activo. Si el borrado de registros forma parte del manual estándar del adversario, la centralización e inmutabilidad de los registros deja de ser una buena práctica para convertirse en un requisito de detección.

2 Vulnerabilidades: el semestre en cifras

2.1 Volumen y evolución

El primer semestre de 2026 cierra con **35.364 vulnerabilidades publicadas**, una vez descontados los identificadores rechazados. Son **49,5 % más** que en el mismo periodo de 2025 y **73,6 % más** que en 2024. Equivale a **195,4 vulnerabilidades al día**: una nueva cada siete minutos y medio, sin pausa durante seis meses.

Para hacerse una idea del salto sirve esta comparación: **el primer semestre de 2026, por sí solo, supera cualquier año completo anterior a 2024**. El ejercicio 2023 cerró con 28.817 vulnerabilidades; el semestre analizado las supera en más de seis mil. Los años completos de referencia son 39.962 en 2024 —cifra revisada a la baja respecto a las 40.009 publicadas inicialmente, por rechazos posteriores— y 48.185 en 2025.

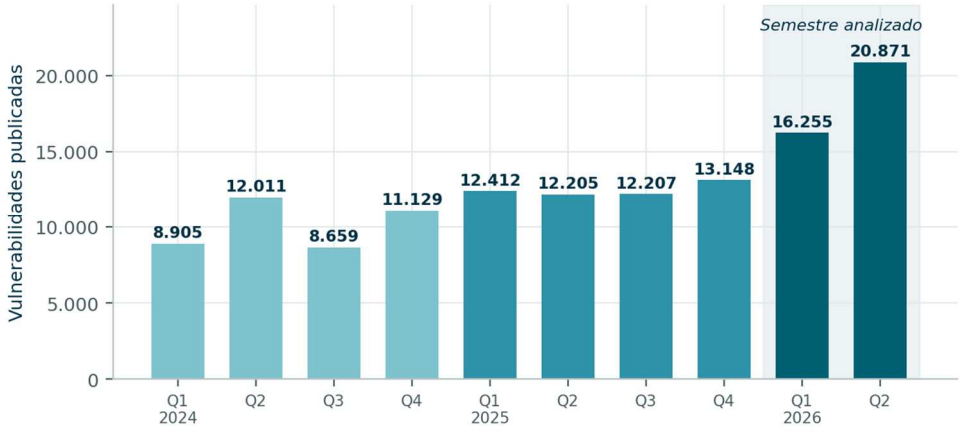

Figura 2. Vulnerabilidades publicadas por trimestre, 2024 a junio de 2026. Serie de la base de datos nacional de vulnerabilidades, consultada el 4 de agosto de 2026.

La serie trimestral muestra que el cambio de régimen no es gradual. Durante 2024 y 2025 el caudal osciló entre las 8.659 y las 13.148 vulnerabilidades por trimestre, con la estacionalidad propia de los ciclos de publicación coordinada. El primer trimestre de 2026 rompe la banda con 16.255 y el segundo la supera con claridad con **20.871**, un 71 % por encima del mismo trimestre del año anterior.

El segundo trimestre da para un párrafo aparte. Con 20.871 registros es, con diferencia, el más cargado de toda la serie, y supone un salto del **28,4 % sobre el trimestre inmediatamente anterior**. Es la señal que más pesa en la previsión del último capítulo, y también la que más cautela exige: un solo trimestre puede reflejar tanto una aceleración real como la absorción de trabajo administrativo atrasado.

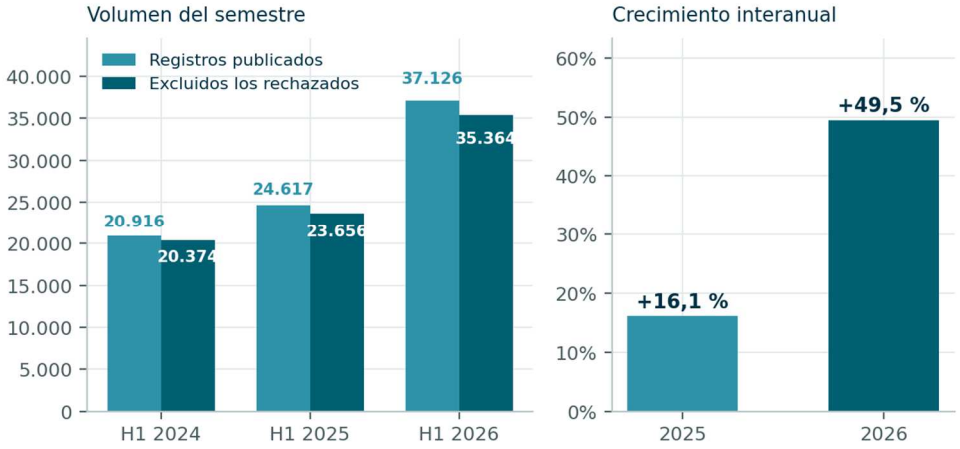

Figura 3. Comparativa del primer semestre. A la izquierda, volumen con y sin identificadores rechazados; a la derecha, crecimiento interanual.

Las causas de este crecimiento son razonablemente conocidas y ninguna apunta a un deterioro súbito de la calidad del software. Pesan tres factores: la expansión del número de autoridades autorizadas a asignar identificadores, que en el semestre alcanzó las **340 activas**; la incorporación masiva de proyectos de código abierto al proceso formal de divulgación; y la aparición de herramientas de descubrimiento asistidas por modelos que abaratan radicalmente la localización de fallos. El organismo que mantiene el catálogo nacional ha reconocido públicamente la tensión: los envíos crecieron un 263 % entre 2020 y 2025, y ha tenido que retirar el enriquecimiento de los registros anteriores a marzo de 2026 para poder atender la entrada.

2.2 Cada vez más fallos graves

Si el volumen preocupa, su composición preocupa más. De las 35.364 vulnerabilidades del semestre, **3.554 se clasifican como críticas** y **13.821 como altas**. Entre ambas suman el **49,1 %** del total: prácticamente una de cada dos. La referencia comparable más cercana es el conjunto del ejercicio 2025, en el que crítica y alta representaron el **39,4 %**. El desplazamiento hacia la gama alta es, por tanto, de casi diez puntos en poco más de medio año.

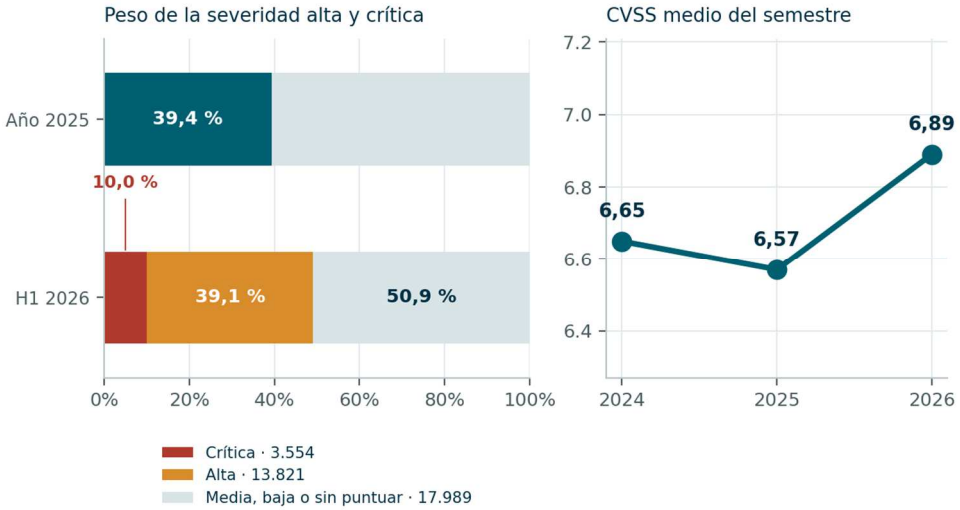

Figura 4. A la izquierda, peso de la severidad alta y crítica. A la derecha, evolución de la puntuación CVSS media del semestre.

La puntuación media confirma el mismo movimiento desde otro ángulo: **6,65** en el primer semestre de 2024, **6,57** en 2025 y **6,89** en 2026, el valor más alto de la serie. La cobertura de puntuación alcanza el 94,3 % de los registros, de modo que la media no está sesgada por ausencias masivas.

Cabe preguntarse si este desplazamiento refleja un empeoramiento real o un cambio en los criterios de puntuación. Nuestra valoración, con confianza media, es que intervienen ambos factores. Por un lado existe una tendencia documentada a la inflación de puntuaciones por parte de algunas autoridades emisoras, especialmente en el ámbito del código abierto, donde el volumen ha crecido más deprisa. Por otro, el peso creciente de las vulnerabilidades en dispositivos de red y componentes de infraestructura —que por su naturaleza puntúan alto en impacto y bajo en complejidad— empuja la distribución hacia arriba de forma legítima.

El efecto práctico es el mismo en los dos casos, y es la conclusión más accionable de este capítulo: **la severidad ha perdido capacidad de discriminación como criterio único de priorización**. Un catálogo en el que la mitad de las entradas son graves no permite ordenar el trabajo. Hace falta un segundo eje.

2.3 Lo que de verdad se acaba explotando

Ese segundo eje es la evidencia de explotación real, y el contraste con el volumen es rotundo. Durante el primer semestre de 2026 se incorporaron **146 entradas al catálogo público de vulnerabilidades explotadas conocidas**, frente a las 132 del mismo periodo de 2025. El catálogo pasó de 1.239 registros a cierre de 2024 a **1.484 a cierre de 2025** —un crecimiento del 20 %— y rondaba las 1.630 al terminar el semestre analizado.

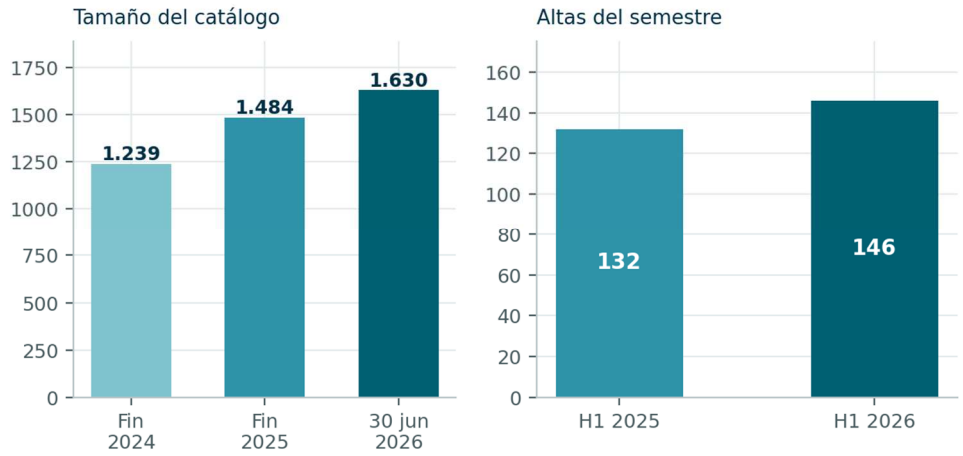

Figura 5. Catálogo público de vulnerabilidades con explotación confirmada: tamaño acumulado y altas registradas en el primer semestre. De las 35.364 vulnerabilidades publicadas entre enero y junio de 2026, solo 85 habían entrado en el catálogo a cierre del semestre.

Pero el dato que de verdad importa es otro. De las **35.364** vulnerabilidades publicadas entre enero y junio de 2026, las que a cierre del semestre contaban con evidencia pública de explotación eran **85**: el **0,24 %**. Ese número irá subiendo con el tiempo, porque la explotación de una vulnerabilidad puede confirmarse meses o incluso años después de que se publique.

LA CUENTA QUE REORDENA CUALQUIER PLAN DE PARCHEO

Por cada vulnerabilidad del semestre que ha acabado con explotación confirmada hay **más de cuatrocientas quince que no**. Una organización que persiga cobertura completa dedicará un esfuerzo creciente a un conjunto que en su inmensa mayoría nunca se aprovechará, mientras compite por los mismos recursos con el puñado de casos que sí importan.

El problema, por tanto, no es que se explote más: es que resulta cada vez **más difícil anticipar qué se va a explotar**. El numerador de la explotación real crece a un ritmo modesto —un 11 % interanual en altas del catálogo— mientras el denominador se dispara casi un 50 %.

2.4 Qué productos se atacan

El análisis de las vulnerabilidades del semestre que han acabado en el catálogo de explotadas ofrece una imagen bastante clara del objetivo preferente. Predominan los fallos que no requieren autenticación previa, con puntuaciones en la franja de 9,8 a 10,0, y una concentración muy marcada en equipamiento de red y en dispositivos de seguridad perimetral.

Tabla 3. Vulnerabilidades destacadas del semestre con explotación confirmada.

Identificador	Producto afectado	CVSS	Alta en el catálogo
CVE-2026-24858	Fortinet FortiOS, FortiProxy, FortiManager y otros	9,8	27 de enero
CVE-2026-22769	Dell RecoverPoint for Virtual Machines	10,0	18 de febrero
CVE-2026-20127	Cisco Catalyst SD-WAN Controller y Manager	10,0	25 de febrero
CVE-2026-20131	Cisco Secure Firewall Management Center	10,0	19 de marzo
CVE-2026-0300	Palo Alto Networks PAN-OS (portal de autenticación)	9,8	6 de mayo
CVE-2026-10520	Ivanti Sentry	10,0	11 de junio
CVE-2026-34908/09/10	Ubiquiti UniFi OS (tres fallos distintos)	10,0	23 de junio

Las puntuaciones de la tabla proceden en su mayoría de la autoridad que asignó el identificador, no de una evaluación independiente posterior, y conviven en el conjunto dos versiones del estándar de puntuación. No son cifras directamente comparables entre sí con precisión decimal; sirven para situar el orden de gravedad, no para establecer un ranking fino.

La lectura por categoría de producto es la que aporta valor. **Nueve de las doce entradas corresponden a equipamiento de red, dispositivos de seguridad perimetral o pasarelas de acceso remoto.** Un mismo fabricante de gestión de movilidad aparece dos veces en el semestre con dos fallos distintos; otro de conmutación y redes definidas por software, otras dos; y un tercero de redes inalámbricas concentra tres fallos publicados el mismo día. No es un problema de un producto concreto: es un problema de categoría.

RECOMENDACIÓN OPERATIVA · GESTIÓN DE VULNERABILIDADES

Sustituir la severidad como criterio primario de priorización por la combinación de tres señales: **evidencia de explotación**, **exposición del activo a internet** y **criticidad del proceso de negocio que soporta**. Una vulnerabilidad de puntuación 7,5 en un concentrador VPN publicado a internet merece más atención inmediata que una de 9,8 en un servicio interno segmentado.

Establecer un circuito diferenciado para el equipamiento de red y seguridad, con un objetivo de aplicación inferior a 72 horas y un procedimiento de verificación posterior al parcheo. Varias de las campañas del semestre mantuvieron el acceso después de la actualización, porque el parche cierra la vía de entrada pero no elimina lo que el adversario ya haya dejado instalado.

3 Quién ataca: grupos y campañas

3.1 Cuántos grupos hay y cuáles están activos

El repositorio de PERSEUS mantiene a cierre del semestre **2.632 conjuntos de actores**. La clasificación por tipología muestra 1.395 conjuntos de intrusión sin atribución consolidada, 295 operaciones identificadas como de ransomware o extorsión, 35 amenazas persistentes avanzadas con atribución establecida y 902 registros que permanecen sin clasificar a la espera de evidencia suficiente; los cinco registros restantes corresponden a categorías residuales. La cifra de los no clasificados no es un defecto del inventario: refleja la realidad de un ecosistema donde la atribución firme es cara y donde la mayor parte de la actividad procede de estructuras efímeras.

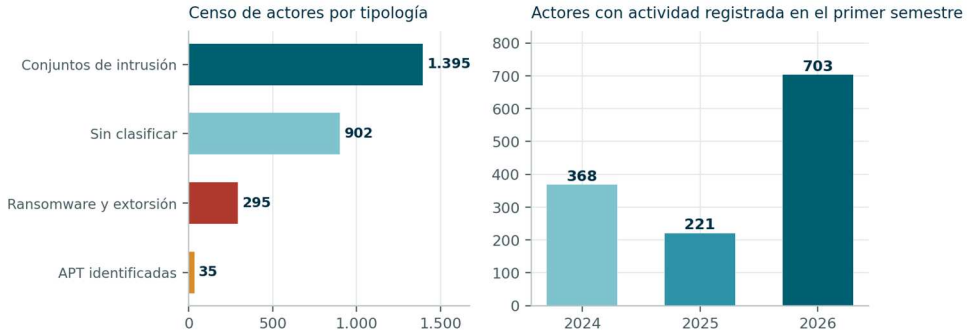

Figura 6. A la izquierda, censo de actores por tipología. A la derecha, conjuntos con actividad registrada durante el primer semestre de cada año.

El número de conjuntos con actividad registrada durante el semestre asciende a **703**, frente a 221 en 2025 y 368 en 2024. El salto es considerable y admite dos explicaciones que no se excluyen: una ampliación real del ecosistema de actores y una mejora de nuestra capacidad de seguimiento tras la incorporación de nuevas fuentes de intercambio. Nuestra valoración, con confianza media, es que la segunda pesa más en la magnitud del salto y la primera en su dirección: el ecosistema está creciendo, aunque probablemente no se haya triplicado.

3.2 Grupos vinculados a Estados

El semestre ha estado marcado por la consolidación de un patrón que ya se apuntaba: los grupos con nexo estatal han abandonado en buena medida el compromiso del puesto de trabajo para concentrarse en la infraestructura de red y en los proveedores de servicio, buscando persistencia prolongada antes que impacto inmediato.

3.2.1 República Popular China

Es el conjunto de actividad más significativo del semestre por sofisticación y por permanencia. El caso más ilustrativo es la explotación de una vulnerabilidad de credenciales embebidas en una plataforma de replicación de máquinas virtuales, aprovechada como día cero desde mediados de 2024 y no detectada hasta el primer trimestre de 2026: cerca de veinte meses de acceso sin descubrir. El objetivo declarado en estas campañas no es el dato de negocio sino el código fuente y la documentación de desarrollo del proveedor, lo que habilita un ciclo realimentado en el que el material robado alimenta el descubrimiento de nuevos días cero.

Los tiempos de permanencia asociados a esta actividad son órdenes de magnitud superiores a la media: las mediciones del sector sitúan la familia de puertas traseras característica de estas operaciones en torno a los 393 días de permanencia media, frente a una media global de dos semanas. Se trata de operaciones diseñadas para no ser encontradas, no para actuar rápido.

3.2.2 Federación Rusa

La actividad rusa mantiene su doble carril habitual: ciberespionaje contra objetivos gubernamentales y de defensa por un lado, y operaciones de perturbación con componente propagandístico por otro. La novedad del semestre está en el plano técnico: se han documentado familias de código dañino que consultan modelos de lenguaje en tiempo de ejecución para generar los comandos de reconocimiento y de exfiltración, en lugar de llevarlos codificados. Es el primer uso operativo confirmado de esta arquitectura, y tiene una implicación directa para la detección: si los comandos se generan en el momento, las reglas basadas en cadenas concretas dejan de servir.

En el ámbito hacktivista, las campañas de denegación de servicio contra objetivos europeos han mantenido un ritmo elevado, con selección de objetivos alineada con la agenda política. Su impacto real sobre la disponibilidad sigue siendo limitado —del conjunto de incidentes de este tipo reportados en la Unión, apenas una fracción mínima causó interrupción efectiva—, pero su valor propagandístico y su capacidad de saturar a los equipos de respuesta no deben subestimarse.

3.2.3 Corea del Norte

El programa norcoreano sigue siendo el más orientado a la obtención directa de fondos y el que mejores resultados obtiene en términos económicos. Durante 2025 se le atribuyeron más de dos mil millones de dólares en activos digitales sustraídos, un 51 % más que el año anterior, y el semestre analizado ha mantenido el ritmo con al menos una operación de gran magnitud contra un mercado descentralizado.

Hay dos vectores que afectan de lleno a las organizaciones europeas. El primero es la infiltración de trabajadores tecnológicos con identidad falsificada en procesos de contratación remota, que ha sido detectada y expulsada de más de veinte entornos empresariales solo en las investigaciones de las que tenemos constancia. El segundo es el compromiso de cuentas de mantenedores de paquetes de código abierto ampliamente utilizados, que convierte un incidente de suplantación en un problema de cadena de suministro global.

3.2.4 Irán

La actividad iraní ha mantenido un perfil de perturbación con componente destructivo, con al menos un caso documentado de despliegue de código de borrado contra una empresa de tecnología médica. Vale la pena mencionar que en el semestre hubo también un caso de atribución errónea —una familia presentada inicialmente como amenaza contra sistemas de control industrial fue posteriormente desmentida como tal por especialistas del sector—, lo que ilustra la necesidad de contrastar los avisos antes de trasladarlos a decisiones operativas.

3.3 Ransomware y extorsión

El ransomware sigue siendo la amenaza de mayor impacto agregado, pero su ecosistema ha cambiado de forma tan profunda que las conclusiones de hace dos años ya no se sostienen. Tres desplazamientos definen la situación actual.

3.3.1 Cada vez más grupos, cada vez más pequeños

El número de operaciones activas crece mientras la cuota de las mayores se reduce. Los rastreadores públicos de sitios de filtración contabilizaron **91 grupos distintos** publicando víctimas en el segundo trimestre, el valor más alto de sus series, frente a los 69 del primero. En términos mensuales el ecosistema se mueve entre **54 y 70 grupos activos**, con picos de 70 en abril.

Esa fragmentación tiene una consecuencia defensiva concreta y poco intuitiva: **las estrategias basadas en conocer a fondo a los grupos principales pierden eficacia**. Cuando cada trimestre aparecen dos docenas de operaciones nuevas, la inteligencia sobre actores concretos se deprecia muy rápido y hay que apoyarse en lo que no cambia: las técnicas que todos comparten, que son sorprendentemente estables.

3.3.2 Cuántas víctimas y a qué ritmo

El primer semestre de 2026 cierra con **4.217 víctimas publicadas** en sitios de filtración, frente a las 3.706 del mismo periodo de 2025 y las 2.456 de 2024. Son **23 víctimas al día**, cuando hace dos años eran 13. El crecimiento interanual se modera: del **+50,9 %** entre 2024 y 2025 se pasa a un **+13,8 %** este semestre, lo que apunta más a saturación del mercado que a retroceso.

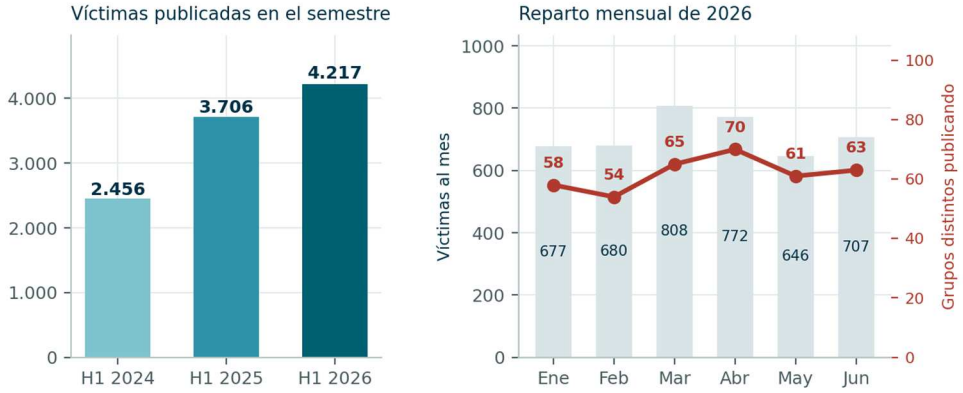

Figura 7. A la izquierda, víctimas publicadas en cada primer semestre. A la derecha, reparto mensual de 2026 y número de grupos distintos que publicaron cada mes.

Son **reclamaciones publicadas por los propios atacantes**, no incidentes verificados: de las 4.217 del semestre solo 484 fueron confirmadas por la organización afectada. El recuento incluye además reclamaciones infladas y víctimas duplicadas entre grupos, y deja fuera a quien paga antes de aparecer publicado. Es un indicador de actividad, no de daño, y distintos rastreadores dan cifras entre 4.200 y 4.600 para el mismo periodo.

3.3.3 Del cifrado a la amenaza de publicar

El tercer desplazamiento es el más relevante para el diseño de controles. La proporción de casos de extorsión que incluyen cifrado ha caído desde niveles del 90-96 %, sostenidos entre 2021 y 2024, hasta el 78 % en 2025, y la exfiltración sin cifrado alcanza el porcentaje más alto medido desde que existen series comparables. Precisemos el denominador: son casos de **extorsión**, no de ransomware en sentido estricto. La lógica es sencilla desde el punto de vista del atacante: cifrar es ruidoso, técnicamente arriesgado y activa todas las alarmas; exfiltrar es silencioso, se confunde con tráfico legítimo y produce el mismo efecto negociador.

> **IMPLICACIÓN PARA LA ESTRATEGIA DE RECUPERACIÓN**
>
> Una organización con copias de seguridad impecables está protegida frente al cifrado y completamente expuesta frente a la extorsión por exposición. Si el modelo de extorsión se desplaza hacia la exfiltración, la inversión defensiva debe desplazarse con él: clasificación del dato, control del movimiento de información hacia el exterior, y detección de transferencias anómalas con umbrales calibrados sobre el comportamiento normal de cada área.
>
> Y hay que revisar el supuesto de que la recuperación es rápida. Las copias son inútiles si el directorio activo está comprometido: el orden de restauración debe empezar por la identidad, y eso exige haberlo ensayado antes.

3.3.4 Cuánto cuesta y cuánto se tarda en volver a la normalidad

El debate sobre el ransomware suele quedarse en el rescate, que es la parte menos representativa del coste. Los datos del sector correspondientes a este año sitúan el **coste medio de recuperación, excluido el rescate, en 1,7 millones de dólares**, con una mediana de 375.000. La media sube un 11 % interanual, aunque sigue un 38 % por debajo del máximo de 2024.

En plazos, la noticia es razonablemente buena: **el 55 % de las organizaciones se recupera por completo en una semana** y el 83 % en un mes, con una media de tres semanas frente a las cinco de 2024. Y el 66 % restaura desde copias de seguridad, doce puntos más que el año anterior. El dato que mejor resume el valor de detener el cifrado a tiempo es este: entre quienes sufrieron cifrado efectivo solo el 9 % se recuperó en un día, frente al 24 % de aquellos donde el cifrado se detuvo.

Hay una dimensión que casi nunca se pone en cifras y que debería llegar al comité de dirección. Prácticamente todas las víctimas con datos cifrados reportan consecuencias sobre el equipo de seguridad: en el **21 % de los casos se sustituyó a la persona que lo dirigía**, cuatro de cada diez describen ansiedad y presión directiva, y cerca de tres de cada diez registran bajas por estrés. El coste de un incidente incluye perder al equipo que tiene que gestionarlo.

3.3.5 Quién ataca a España

El ranking del semestre lo encabeza **Qilin**, en cabeza de forma sostenida durante cinco trimestres consecutivos, seguido de **The Gentlemen** —una operación nacida este mismo año que llegó a desbancarlo en junio— y de **Akira** y **DragonForce**. Los tres primeros concentran alrededor de un tercio de todas las víctimas publicadas del semestre.

En el caso español, el seguimiento del sector sitúa como más activos a **Qilin**, **The Gentlemen** —con un repunte apreciable en marzo— y **Nightspire**, con enero como uno de los meses de mayor actividad detectada. Los sectores más golpeados han sido la industria, el marketing y la comunicación, la construcción y el sector inmobiliario, la logística y el transporte, y las empresas de tecnología. España aparece en séptimo lugar entre los países con más víctimas publicadas del semestre, y representa en torno al 2 % del total mundial.

Circulan tres cifras españolas que no son comparables entre sí: los 392 incidentes de ransomware que registró el instituto nacional en 2025 cuentan incidentes gestionados, los rastreadores cuentan víctimas publicadas por los atacantes, y las estimaciones sectoriales usan perímetros propios. Ninguna es errónea; el error consiste en encadenarlas para construir una serie temporal.

3.4 Qué buscan los atacantes en cada fase

El marco ATT&CK ordena las técnicas por el objetivo que persigue el atacante en cada momento: entrar, ejecutar código, mantenerse, moverse, robar información. Ver cómo se reparte la actividad entre esas fases dice bastante sobre dónde pone el esfuerzo el adversario.

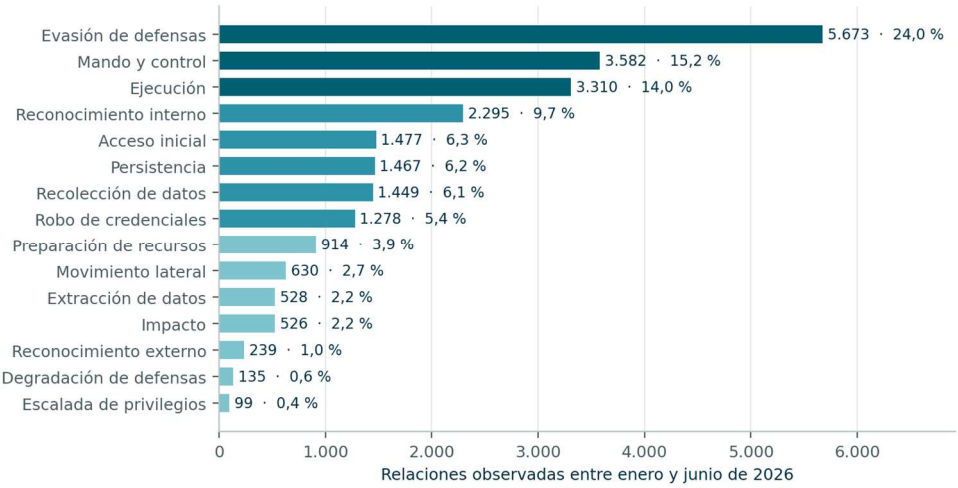

Figura 8. Reparto de la actividad observada por fase del ataque, enero-junio de 2026.

La **evasión de defensas** encabeza el reparto con 5.673 relaciones, el **24,0 %** del total. Casi una de cada cuatro. Le siguen el **mando y control** —la comunicación entre el equipo comprometido y el atacante— con 3.582 (15,2 %) y la **ejecución de código** con 3.310 (14,0 %).

Que la evasión encabece la lista con tanta ventaja tiene una lectura directa: el esfuerzo principal ya no se dedica a entrar ni a moverse, sino a **no ser visto mientras se hace**. Es el reflejo de que las herramientas de detección en el puesto de trabajo funcionan razonablemente bien, y de que los atacantes lo saben.

En el extremo opuesto, tres fases llaman la atención por su escasa presencia. El **impacto** —cifrar, destruir, interrumpir— reúne 526 relaciones (2,2 %) y la **extracción de datos** 528 (2,2 %). Son las fases que producen el daño visible, y su baja frecuencia recuerda que la mayor parte de la actividad catalogada corresponde a fases preparatorias. La **escalada de privilegios**, con 99 relaciones, refleja algo distinto: cuando se entra con credenciales válidas de nivel suficiente, sencillamente no hace falta escalar.

Tabla 4. Reparto de la actividad por fase del ataque, enero-junio de 2026.

Fase del ataque	Relaciones	% del total	Qué implica
Evasión de defensas	5.673	24,0 %	Prioridad absoluta del atacante
Mando y control	3.582	15,2 %	Canales cifrados y servicios legítimos
Ejecución de código	3.310	14,0 %	Uso de intérpretes del propio sistema
Reconocimiento interno	2.295	9,7 %	Explorar la red una vez dentro
Acceso inicial	1.477	6,3 %	Correo fraudulento y servicios expuestos
Persistencia	1.467	6,2 %	Asegurar el regreso tras un reinicio
Recolección de datos	1.449	6,1 %	Captura de teclado y ficheros locales
Robo de credenciales	1.278	5,4 %	La fase que más ha crecido
Preparación de recursos	914	3,9 %	Infraestructura previa al ataque
Movimiento lateral	630	2,7 %	Salto entre equipos con servicios legítimos
Extracción de datos	528	2,2 %	Fase final, poco representada
Impacto	526	2,2 %	Cifrado y destrucción
Reconocimiento externo	239	1,0 %	Actividad previa, difícil de observar

Merece la pena comparar este reparto con el del histórico acumulado, porque hay dos diferencias que importan. En el semestre, el **mando y control adelanta a la ejecución de código** y sube al

segundo puesto; y el **acceso inicial gana posiciones** hasta el quinto, por delante de la persistencia. Ambos movimientos apuntan en la misma dirección: campañas más cortas, más centradas en entrar y comunicar, y menos en instalarse a largo plazo.

3.5 Las técnicas más usadas

Bajando de las fases a las técnicas concretas, el resultado confirma algo que hay que repetir ante cualquier comité que evalúe inversiones: **el repertorio básico del atacante es corto, estable y bien conocido**. Ninguna de las diez primeras técnicas es una novedad, y todas tienen contramedidas documentadas desde hace años.

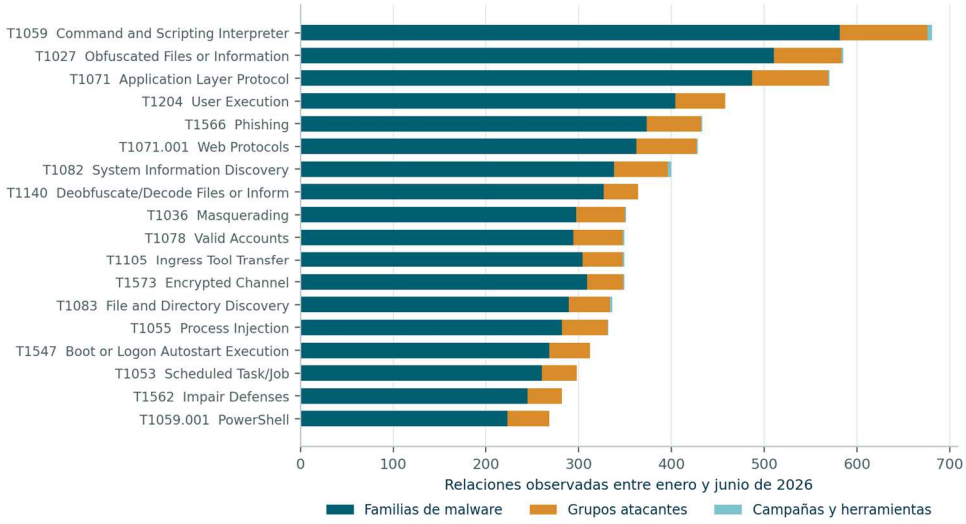

Figura 9. Técnicas más observadas entre enero y junio de 2026, con desglose por tipo de entidad hostil.

Encabeza la lista **T1059**, que describe el uso de los intérpretes de comandos ya presentes en el sistema —PowerShell, la consola de Windows, *bash*— para ejecutar la carga dañina, con 681 relaciones. Le siguen **T1027**, la ofuscación del código para dificultar su análisis (585), y **T1071**, el uso de protocolos ordinarios de internet como canal de comunicación con el atacante (570).

El cuarto puesto lo ocupa **T1204**, que describe la necesidad de que alguien haga clic (458), y el quinto **T1566**, el correo fraudulento (433). Aparecen también dos técnicas que, juntas, dicen bastante: **T1140**, la desofuscación en tiempo de ejecución (364), y **T1078**, el uso de cuentas legítimas (349). La primera indica que el código llega cifrado y se descifra ya dentro; la segunda, que buena parte de la actividad se ejecuta con credenciales que el sistema considera válidas.

3.6 Lo que más ha crecido

La comparación entre los últimos noventa días y los noventa anteriores es donde el análisis aporta más valor, porque señala hacia dónde se mueve el adversario. De las 618 técnicas de la matriz empresarial con seguimiento de tendencia —368 con actividad reciente—, **89 han triplicado o más su frecuencia**, y 33 de ellas con volumen suficiente para descartar el ruido estadístico.

Figura 10. Técnicas con mayor crecimiento. Comparación entre los últimos noventa días y los noventa anteriores, con el multiplicador de crecimiento.

Estas técnicas no forman una lista suelta: se agrupan en tres bloques que describen tres decisiones distintas del atacante.

Borrar el rastro ya es rutina

T1070, que agrupa el borrado de indicadores de la actividad, pasa de 89 a 398 observaciones: se multiplica por 4,5 y es la técnica que más crece en términos absolutos. Su variante específica de borrado de los registros de eventos de Windows, **T1070.001**, se multiplica por 9,5. En paralelo, **T1564**, ocultar ficheros y procesos para que no aparezcan en las herramientas habituales, crece por 5,9.

Se lee sin dificultad: limpiar detrás de uno ha dejado de ser la firma de un atacante sofisticado para incorporarse al manual estándar. Y no solo dificulta la investigación posterior: **degrada la señal de la que depende toda la detección basada en registros**, justo cuando muchas organizaciones han desplazado su estrategia precisamente hacia ahí.

> **CONTRAMEDIDA PRIORITARIA**
>
> El reenvío de registros debe ser **inmediato y hacia un destino que el equipo de origen no pueda modificar**. Si el borrado local no impide que la copia remota ya exista, la técnica pierde su efecto.
>
> Y algo que casi nadie vigila: **la ausencia de registros debe generar alerta por sí misma**. Un servidor que deja de enviar eventos es una señal tan relevante como un evento anómalo.

Buscar contraseñas guardadas sin protección

T1552 se multiplica por 8,9, de 20 a 178 observaciones. Describe algo muy concreto: rebuscar credenciales almacenadas en claro allí donde suelen quedarse olvidadas —ficheros de configuración, variables de entorno, repositorios de código, historiales de consola—. Su variante **T1552.007**, que busca esas credenciales a través de la interfaz de gestión de contenedores, se multiplica por diez.

A su alrededor crece todo un bloque. **T1555.003**, el robo de contraseñas guardadas en el navegador, se triplica hasta 143 observaciones. **T1558.003** —conocida como *Kerberoasting*, que permite obtener contraseñas de cuentas de servicio del directorio activo— se multiplica por once, y su prima **T1558.004** aparece como técnica emergente. En conjunto describen a un atacante que, una vez dentro, dedica su primer esfuerzo a acumular más credenciales antes de moverse.

Que estas dos últimas crezcan a la vez es especialmente significativo. Ambas aprovechan configuraciones débiles del directorio activo que llevan años documentadas y que tienen contramedidas conocidas: contraseñas largas y aleatorias en las cuentas de servicio, cifrado

moderno y preautenticación obligatoria. Su reaparición indica que el atacante ha comprobado que siguen siendo comunes.

Instalarse en los equipos de red

El tercer bloque es el más novedoso y el peor cubierto por los controles habituales. **T1482**, que consiste en mapear las relaciones de confianza entre dominios para saber hasta dónde se puede llegar, se multiplica por 25,5 —el mayor crecimiento relativo del semestre—. **T1568.002**, la generación automática de nombres de dominio para que la infraestructura del atacante sea difícil de bloquear, se multiplica por 19. El uso del **DNS como canal de comunicación** (T1071.004) crece por 4,1, y el encadenamiento de servidores intermedios para ocultar el origen (T1090.003) por 3,1.

Entre las técnicas emergentes destaca un grupo que apunta al mismo territorio: **T1601** y sus variantes, que describen la modificación del firmware de los equipos de red, incluida la instalación deliberada de una versión antigua y vulnerable; y **T1602.002**, la extracción de la configuración de esos equipos. Seamos explícitos con el volumen: hablamos de tres observaciones en la ventana reciente frente a ninguna en la anterior. No es una tendencia consolidada, sino una señal débil. La recogemos porque coincide con lo que muestran las vulnerabilidades del semestre y porque, de confirmarse, describe una capacidad para la que la mayoría de las organizaciones no tiene ninguna detección.

Dos indicadores propios acompañan a la figura. El **impulso** compara la frecuencia de una técnica en los últimos noventa días con la de los noventa anteriores: es una derivada, no un nivel. La **novedad** mide su rareza en el corpus histórico. Novedad alta más actividad reciente identifica candidatas a convertirse en tendencia.

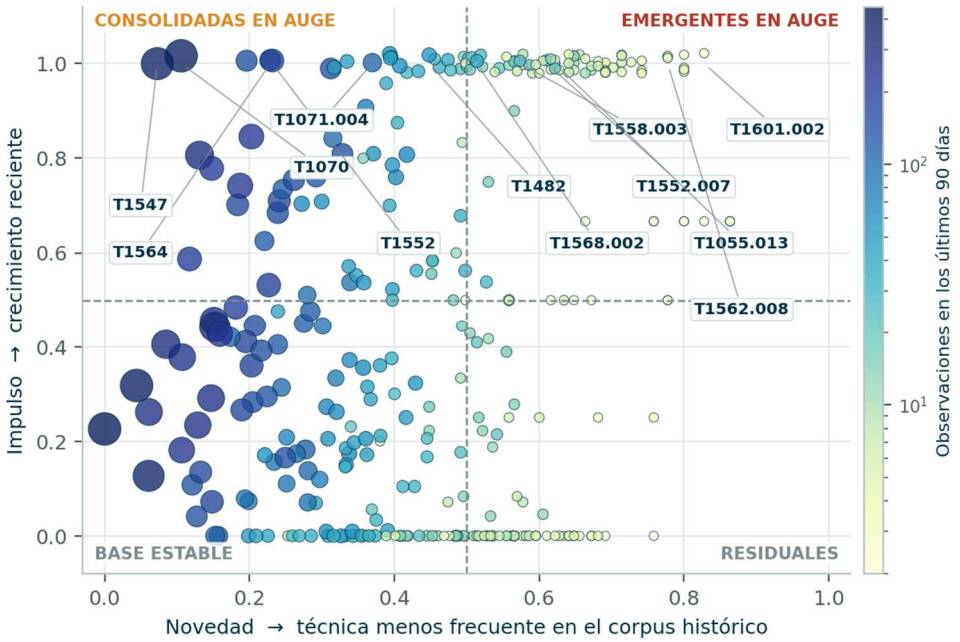

Figura 11. Cada punto es una técnica. El eje horizontal mide lo poco frecuente que es en el histórico; el vertical, cuánto ha crecido recientemente. El cuadrante superior derecho reúne las técnicas poco habituales que están despegando.

La coincidencia de estos dos últimos bloques —abuso del DNS y manipulación de equipos de red— con lo que hemos visto en el capítulo de vulnerabilidades no es casual. Describe a un atacante que trata la infraestructura de red no como un obstáculo que atravesar, sino como un lugar donde instalarse. Un equipo de red comprometido ofrece una permanencia que sobrevive a la reinstalación de los servidores, visibilidad sobre todo el tráfico y una salida a internet que la monitorización perimetral considera de confianza.

3.7 Ataques sin malware

Todo lo anterior desemboca en un cambio que hay que decir sin rodeos: la proporción de operaciones que no emplean malware en sentido clásico ha alcanzado niveles que invalidan buena parte del diseño defensivo heredado. Las mediciones del sector sitúan las detecciones sin malware en torno al **82 %**, frente al 51 % de hace cinco años. Herramientas que durante una década fueron sinónimo de intrusión avanzada han caído a posiciones marginales, desplazadas por utilidades de administración legítimas.

El abuso de herramientas de gestión y control remoto ha crecido de forma muy acusada, mientras las puertas traseras tradicionales retroceden. Es un intercambio racional desde el punto de vista del atacante: la herramienta legítima está firmada, el antivirus la conoce, genera tráfico hacia dominios de buena reputación y, con frecuencia, **ya está instalada y autorizada** en la organización objetivo.

> **QUÉ SIGNIFICA PARA LA DETECCIÓN**
>
> Si el atacante usa credenciales válidas, programas firmados y herramientas autorizadas, la detección no puede apoyarse en identificar el artefacto. Tiene que apoyarse en la **anomalía del comportamiento**: qué cuenta ejecuta qué proceso, en qué equipo, a qué hora, con qué frecuencia y hacia dónde envía datos.
>
> En la práctica esto exige tres cosas que muchas organizaciones no tienen: un inventario fiable de qué herramientas de administración remota están autorizadas y en qué equipos; una referencia de comportamiento normal por cuenta y por servicio; y capacidad de cruzar identidad, equipo y red en una misma consulta. Sin las tres, la búsqueda proactiva de amenazas se queda en revisar alertas.

3.8 Inteligencia artificial en el ataque

Pocos asuntos han generado tanta literatura y tan poca evidencia contrastada. Desde PERSEUS hemos mantenido durante el semestre una posición deliberadamente escéptica, comprobando cada afirmación antes de darla por buena. El resultado se resume en una frase: la inteligencia artificial es hoy **un acelerador comprobado y una capacidad ofensiva nueva todavía incipiente**, pero este semestre se han producido los dos primeros casos que obligan a matizar la segunda mitad.

Los equipos que investigan incidentes reales coinciden de forma llamativa. En una muestra de seiscientas sesenta y una investigaciones publicada este año se documentó **un único caso verificado** de uso de inteligencia artificial generativa por parte del atacante: un vídeo manipulado recibido por redes sociales. El patrón dominante es que el adversario incorpora modelos a manuales que ya funcionaban para ir más rápido —mejores señuelos, traducción sin errores, reconocimiento automatizado, desarrollo acelerado—, no para hacer cosas que antes no podía hacer.

En el terreno del código dañino se ha consolidado una categoría que apenas existía hace un año: familias que **consultan un modelo de lenguaje en tiempo de ejecución** para generar los comandos que ejecutan, en lugar de llevarlos embebidos. La primera de ellas, empleada operativamente por un actor con nexo estatal contra objetivos ucranianos, consulta un modelo de código a través de una interfaz pública. Tiene una implicación directa para la detección: si los comandos se generan en el momento, las reglas basadas en cadenas concretas dejan de servir.

Existe además una segunda categoría, probablemente más relevante a medio plazo: el código dañino *escrito* con asistencia de modelos. El caso mejor documentado del semestre es un entorno de ataque completo para sistemas Linux que pasó de documento de planificación a más de ochenta y ocho mil líneas funcionales **en una semana**. No introduce técnicas nuevas: comprime radicalmente el tiempo de desarrollo.

Donde el efecto sí es medible y muy acusado es en el fraude de identidad. Las pérdidas documentadas por suplantación sintética pasaron de 335 millones de dólares en 2024 a alrededor de **2.500 millones en 2025**, y el primer semestre de 2026 acumula ya 764 millones. Alrededor de uno de cada cinco intentos de fraude biométrico incorpora hoy material sintético.

Para una organización todo esto se concreta en un procedimiento que casi todas tienen mal resuelto: **la verificación de identidad en el servicio de atención al usuario**. Si restablecer una contraseña puede pedirse por teléfono y la verificación consiste en reconocer una voz, el control ha dejado de existir. Los incidentes más costosos documentados en Europa en los últimos dos años empezaron exactamente así.

Los responsables de los principales repositorios han desplegado durante el semestre un conjunto de medidas —publicación en dos fases, desactivación por defecto de los guiones de instalación, protección preventiva de cuentas de alto impacto, periodos de enfriamiento antes de proponer actualizaciones— que representan el cambio más profundo en años. Su propia evaluación reconoce, no obstante, una limitación relevante: varias campañas del semestre eludieron la desactivación de guiones ejecutándose al importar el módulo.

4 Qué sectores reciben más ataques

La distribución de la actividad hostil por sector de actividad refleja tanto el atractivo del objetivo como su exposición estructural. Entre enero y junio de 2026 hemos registrado **3.456 relaciones** entre una entidad hostil y un sector económico, repartidas entre 74 categorías distintas. Los diez primeros sectores concentran el 68,1 % de esa actividad.

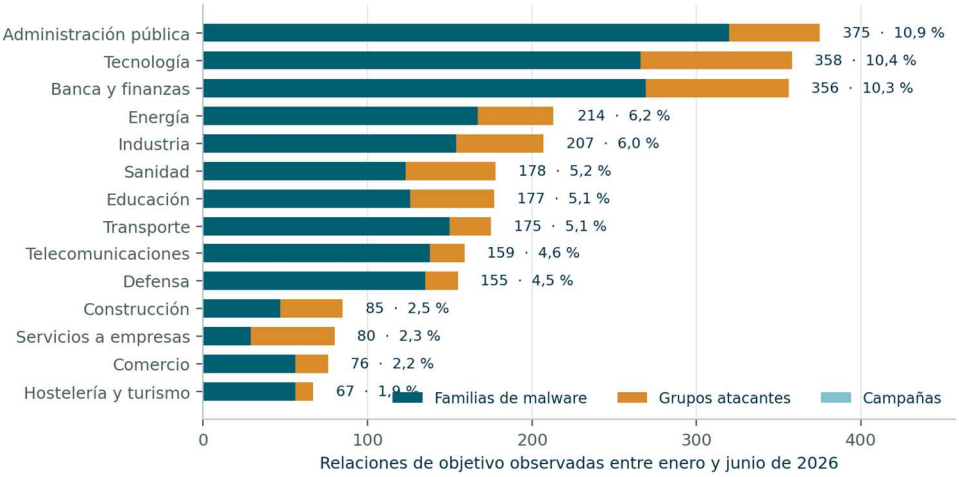

Figura 12. Sectores con mayor volumen de actividad hostil dirigida, con desglose por tipo de entidad.

4.1 Perfil de los seis sectores más atacados

4.1.1 Administración pública

Encabeza el reparto con **375 relaciones (10,9 %)**. La cifra es coherente con lo que reportan los organismos de referencia europeos, que sitúan a la administración pública como el sector más afectado de la Unión, con el 38,2 % de los incidentes registrados; dentro de ese sector, seis de cada diez son de denegación de servicio. La combinación que explica esta posición es conocida: superficie enorme y heterogénea, ciclos de renovación tecnológica largos, restricciones presupuestarias, y un valor simultáneo para tres tipos de adversario distintos —espionaje estatal, hacktivismo y ransomware oportunista—.

La administración local española es un caso aparte. Concentra servicios esenciales para el ciudadano, custodia datos personales de alto valor y opera con equipos de seguridad muy reducidos o inexistentes. Los mecanismos de apoyo nacionales han crecido mucho, pero la asimetría entre la superficie a proteger y los recursos disponibles sigue siendo el factor determinante del riesgo en este segmento.

4.1.2 Tecnología y proveedores de servicios

Segundo con **358 relaciones (10,4 %)**, y con una particularidad que lo hace especialmente relevante: es el sector con mayor proporción de actividad atribuible a grupos identificados y a campañas concretas, frente al predominio del malware genérico en otros sectores. Dicho de otro modo, es donde el atacante elige antes de atacar.

La razón es el efecto multiplicador. Comprometer a un proveedor de servicios gestionados, a un fabricante de software o a un integrador da acceso a decenas o cientos de organizaciones cliente con una sola operación. Las campañas de espionaje más persistentes del semestre han seguido exactamente esta lógica, y la métrica que mejor la resume es que la proporción de brechas con implicación de terceros se ha situado en torno al 48 %, tras haberse duplicado el año anterior.

4.1.3 Sector financiero

Tercero, prácticamente empatado, con **356 relaciones (10,3 %)**. Es, junto con las telecomunicaciones y la electricidad, uno de los sectores con mayor madurez de seguridad reconocida en las evaluaciones europeas, y esa madurez se nota en los resultados: pese a ser uno de los objetivos más atacados, la proporción de incidentes con impacto operativo real es comparativamente baja.

El marco regulatorio ha contribuido de forma medible. El primer informe agregado de incidentes graves bajo el reglamento europeo de resiliencia operativa digital, publicado en junio de 2026, recoge 3.383 incidentes notificados durante 2025 por las **entidades financieras de la Unión sujetas al reglamento** —no por el conjunto de la economía—, con una media de 0,18 por entidad. El dato más interesante para un CISO financiero es otro: **solo el 10 % de esos incidentes tuvo origen en ciberseguridad**. La mayor parte fueron fallos de sistema y eventos externos, y cerca de un tercio se originaron en terceros. La resiliencia operativa no es un subconjunto de la ciberseguridad, y la regulación lo ha entendido antes que muchas organizaciones.

4.1.4 Industria y entornos industriales

La industria reúne **207 relaciones (6,0 %)**, pero el dato que cambia respecto a semestres anteriores es el de **energía, que sube al cuarto puesto con 214 (6,2 %)**, por delante de la propia industria. Sumando el transporte (175), el bloque industrial y de infraestructuras se sitúa entre los más presionados del semestre. Es el sector donde la distancia entre la exposición y la capacidad de detección es mayor.

Los datos del sector que contrastamos son elocuentes: solo alrededor del 30 % de las redes de operación cuentan con visibilidad suficiente, más de la mitad de las organizaciones industriales no ve lo que ocurre por debajo de la frontera entre tecnología de la información y tecnología de operación, y cerca de nueve de cada diez reconocen dificultades de detección y respuesta en ese entorno. En el primer trimestre de 2026 se contabilizaron más de mil incidentes de ransomware industrial, con la manufactura como sector más golpeado.

Un matiz importante para no alimentar alarmismo: los especialistas en el dominio han sido claros al señalar que **no se han observado variantes de ransomware diseñadas específicamente para manipular protocolos de control industrial**. El daño en planta se produce por propagación desde la red corporativa y por paradas preventivas, no por manipulación directa del proceso. Eso no reduce el impacto —una parada de producción cuesta lo mismo sea cual sea su causa—, pero sí orienta dónde invertir: la segmentación entre dominios sigue siendo el control de mayor rendimiento.

La excepción a esa tranquilidad relativa está en el preposicionamiento. Durante el semestre se han catalogado grupos especializados en obtener y mantener acceso a entornos industriales sin ejecutar acción destructiva: sustraen configuraciones de autómatas programables, datos de interfaces de operación y lógica de alarmas. Es reconocimiento para una acción futura, y su detección requiere precisamente la visibilidad que la mayoría no tiene.

4.1.5 Sanidad

Con **178 relaciones (5,2 %)**, la sanidad no lidera el ranking de volumen pero sí el de consecuencias. Las evaluaciones sectoriales europeas la sitúan de forma consistente en la zona de riesgo, donde la criticidad del servicio supera a la madurez de la protección. La combinación de equipamiento médico con ciclos de vida de quince años, imposibilidad práctica de detener servicios para mantenimiento y datos de altísimo valor en el mercado criminal la convierte en un objetivo estructuralmente vulnerable.

4.1.6 Transporte y logística

El transporte reúne **175 relaciones (5,1 %)**, y es el sector con mayor peso relativo en los incidentes de operadores críticos españoles, donde supera el 42 % del total. Los incidentes de mayor visibilidad del último año en Europa —la interrupción de sistemas de facturación en varios aeropuertos importantes por el compromiso de un proveedor común, o el ataque a instalaciones portuarias— comparten un patrón: el impacto no se produjo en el operador, sino en el proveedor de un servicio compartido por muchos operadores.

4.2 Por dónde entran y cuánto cuesta, sector a sector

Saber cuántos ataques recibe cada sector dice poco si no se sabe **cómo** entran y **qué cuesta** cuando entran. Los datos públicos del sector permiten completar las dos cosas con una metodología homogénea, lo que hace la comparación entre sectores mucho más útil que cualquier recuento.

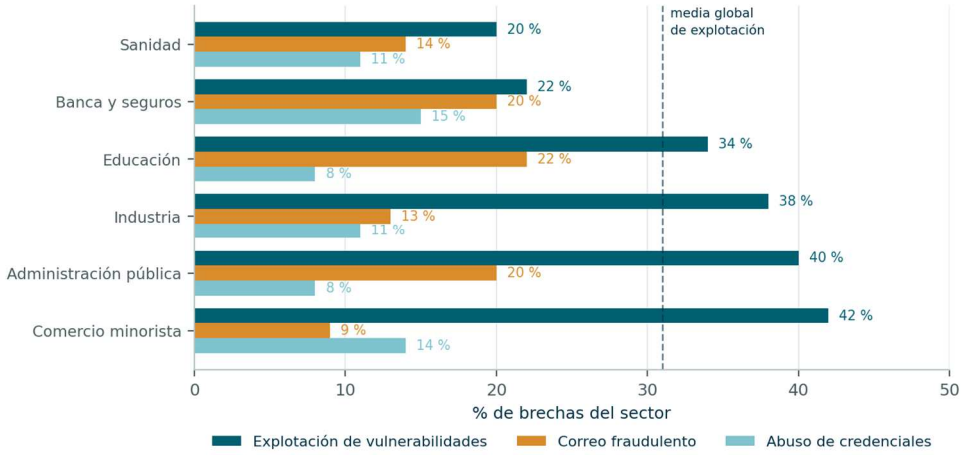

Figura 13. Vector de entrada por sector, en porcentaje de las brechas del sector. La línea discontinua marca la media global de explotación de vulnerabilidades.

El reparto desmonta la idea de que todos los sectores se atacan igual. El **comercio minorista** y la **administración pública** son los que más sufren la explotación directa de vulnerabilidades —42 % y 40 % de sus brechas—, muy por encima de la media global del 31 %. La **sanidad**, en cambio, se queda en el 20 %: allí pesan más el correo fraudulento y el error humano. Y la **banca** es el sector con mayor abuso de credenciales, un 15 %.

Hay dos cifras que cambian la conversación sobre proveedores. En el **comercio minorista, el 68 % de las brechas implica a un tercero**; en la **industria, el 61 %**. Frente a una media global ya muy alta del 48 %, estos dos sectores tienen un problema de cadena de suministro que no se resuelve con controles propios.

4.3 Quién ataca y por qué, según el sector

La motivación del atacante también varía, y en un caso lo hace de forma radical. En casi todos los sectores el móvil es económico en más del 85 % de los casos. En **utilities y suministros, el espionaje supera al lucro: 71 % frente al 36 %**. Es el único sector donde ocurre, y describe una realidad distinta: allí el adversario no busca dinero, busca conocimiento y posición.

La **administración pública** presenta otra anomalía: el **44 % de sus brechas tiene origen interno**, muy por encima del resto, y el espionaje pesa un 33 %. Buena parte de ese componente interno son errores —el envío de información a destinatario equivocado supone el 88 % de los errores del sector,

y en nueve de cada diez casos por simple descuido—. Hay que matizar el dato: las obligaciones de notificación son más estrictas en el sector público, así que los errores afloran más que en el privado.

Tabla 5. Perfil del atacante por sector. El factor humano incluye error, uso indebido y engaño.

Sector	Actor externo	Motivación económica	Espionaje	Factor humano
Comercio minorista	99 %	85 %	19 %	58 %
Transporte	99 %	89 %	15 %	—
Utilities y suministros	97 %	36 %	**71 %**	—
Industria	95 %	87 %	15 %	56 %
Banca y seguros	88 %	98 %	3 %	65 %
Sanidad	81 %	99 %	2 %	54 %
Educación	78 %	78 %	21 %	68 %
Administración pública	56 %	69 %	33 %	69 %

4.4 Lo que cuesta una brecha

El coste medio de una brecha se ha situado este año en **4,99 millones de dólares**, un récord y un 12 % más que el ejercicio anterior. Pero la media esconde diferencias de casi un 35 % entre sectores.

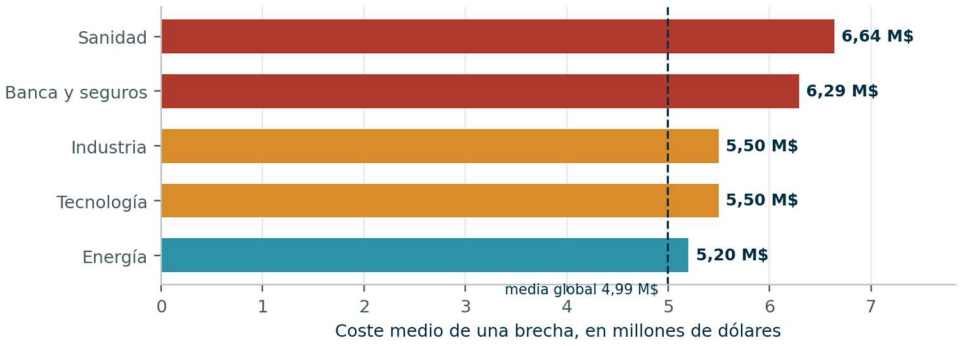

Figura 14. Coste medio de una brecha por sector, en millones de dólares.

La **sanidad encabeza la lista por decimotercer año consecutivo** con 6,64 millones, aunque baja un 10,5 % respecto al año pasado. Le siguen la **banca** con 6,29 y, empatados, **tecnología e industria** con 5,50. La **energía** cierra el grupo de cabeza con 5,20.

Dos factores explican buena parte de esas diferencias y ninguno es sectorial en sentido estricto. El primero es el **tiempo**: las brechas que tardan más de doscientos días en contenerse cuestan 5,65 millones frente a 4,32 las que se resuelven antes, y el ciclo medio global ha subido a **247 días**, la primera subida en cinco años. El segundo es la **cadena de suministro**, que encabeza la lista de factores que encarecen un incidente y produce además las brechas más lentas de detectar.

4.5 Con qué frecuencia ocurre

El recuento por sector responde a cuántos ataques hay en total, no a cuántos le tocan a cada organización. Ese segundo dato, cuando existe, es mucho más útil para dimensionar un equipo.

El caso mejor documentado es el sanitario: **el 93 % de las organizaciones sanitarias sufrió al menos un ciberataque en doce meses, con una media de 43 ataques por organización**, frente a los 40 del año anterior. No se trata de un incidente ocasional, sino de una media de casi cuatro al mes por

entidad. En administración pública, el ransomware contra entidades gubernamentales alcanzó las **187 víctimas en el semestre a escala mundial**, un 13 % más: **una entidad pública atacada cada día**.

Y una particularidad que rara vez se menciona: **la administración local y autonómica es el sector que más paga**. El 72 % de las que sufrieron ransomware pagó el rescate, la tasa más alta de los catorce sectores medidos, frente al 32 % del comercio minorista, que es la más baja. La explicación probable es la combinación de servicios que no pueden interrumpirse con capacidad de recuperación limitada.

5 Europa y España

5.1 Dónde se concentra la actividad

La actividad hostil registrada por PERSEUS sitúa a **Europa como la segunda región del mundo por volumen**, con 2.045 asociaciones de objetivo, por detrás de Asia (2.285) y por delante del conjunto americano (1.807). Dentro de Europa, la subregión más apuntada es Europa del Este con 1.419 asociaciones, seguida de Europa Occidental (918), Europa Meridional (781) y Europa del Norte (698).

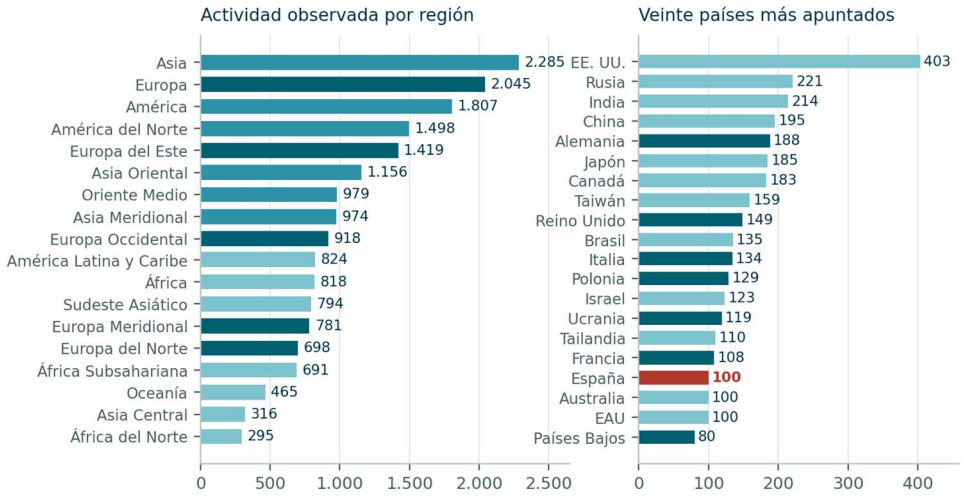

Figura 15. A la izquierda, actividad observada por región. A la derecha, los veinte países más apuntados; España aparece destacada.

El peso de Europa del Este se explica en su mayor parte por el conflicto en Ucrania y por la actividad asociada a él, tanto de espionaje como de perturbación. Europa Meridional —donde se encuadra España— reúne 781 asociaciones, por delante de Europa del Norte y a poca distancia de Europa Occidental, lo que sitúa al arco mediterráneo en un nivel de exposición comparable al de los países del centro y norte del continente.

5.2 España en nuestros datos

España aparece en el semestre con **100 asociaciones de objetivo**, lo que la sitúa en la decimoséptima posición mundial, empatada con Emiratos Árabes Unidos y Australia. Entre los países de la Unión Europea y su entorno inmediato ocupa el séptimo lugar, por detrás de Alemania (188), Reino Unido (149), Italia (134), Polonia (129), Ucrania (119) y Francia (108).

Esta posición hay que leerla con cuidado. En términos de tamaño económico, España está sistemáticamente por debajo de lo que su peso relativo haría esperar cuando se la compara con Alemania o Reino Unido. Nuestra valoración, con confianza media, es que esa diferencia refleja en buena medida un **sesgo de reporte** más que una exposición menor: la actividad dirigida contra organizaciones españolas se documenta y se comparte con menos frecuencia en las fuentes abiertas internacionales, en parte por el idioma y en parte por una cultura de notificación más reservada. Recomendamos por tanto no leer esta cifra como un indicador de menor riesgo.

5.3 España comparada con sus vecinos

Comparar países en ciberseguridad es traicionero: cada agencia nacional cuenta cosas distintas y las cifras no son intercambiables. Hay, sin embargo, dos fuentes que sí permiten una comparación homogénea, y juntas dibujan un cuadro que contradice la percepción habitual.

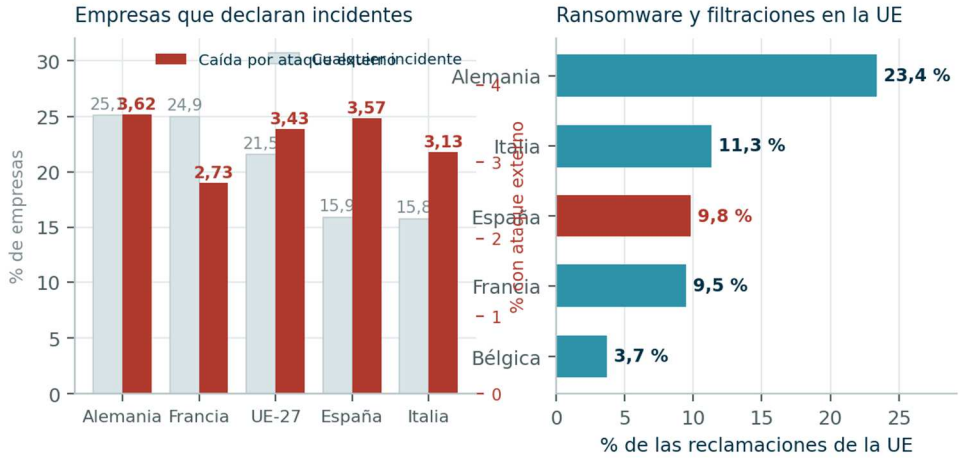

Figura 16. A la izquierda, empresas que declaran haber sufrido incidentes, según la encuesta europea armonizada. A la derecha, reparto de las reclamaciones de ransomware y filtraciones entre países de la Unión.

La primera es la estadística europea armonizada, que pregunta lo mismo a empresas de los veintisiete Estados. Según ella, el **15,88 % de las empresas españolas** declaró algún incidente, frente al 21,54 % de la media europea, el 25,07 % de Alemania y el 24,95 % de Francia. Leído sin más, España parecería un país tranquilo. Es una lectura equivocada.

EL DATO QUE CAMBIA LA LECTURA

Si se mira solo el indicador agregado, España queda 5,7 puntos por debajo de la media europea. Pero al separar los incidentes **maliciosos** de los **accidentales**, el cuadro se invierte: en caídas provocadas por un ataque externo España registra un **3,57 %**, por encima de la media europea (3,43 %) y de Italia y Francia. Y en destrucción de datos por intrusión o código dañino, un **2,47 %** frente al 1,89 % europeo.

Toda la diferencia entre España y Europa se explica por los **fallos de hardware y software no maliciosos**: 11,97 % frente a 17,97 %. Dicho de otro modo: **España no recibe menos ataques que Europa; tiene menos averías**. Cualquier conclusión del tipo «aquí nos atacan menos» apoyada en el dato agregado es incorrecta.

Queda una cautela: el indicador mide incidentes **detectados y declarados**. Solo el 29 % de las pequeñas empresas europeas hace evaluaciones de riesgo, frente al 76 % de las grandes. Quien menos declara suele ser quien menos mira.

La segunda fuente es el reparto europeo de reclamaciones de ransomware y filtraciones de datos, donde **España ocupa el tercer puesto con el 9,8 %**, por detrás de Alemania (23,4 %) e Italia (11,33 %) y prácticamente empatada con Francia (9,5 %). Las familias más activas contra objetivos españoles son Qilin, Akira y FOG, y el sector más golpeado es la industria, seguido de los servicios a empresas y la administración pública.

Hay una asimetría más que merece señalarse. España **no aparece en los diez países más atacados por denegación de servicio** a escala mundial, donde Alemania es tercera y Reino Unido sexto. Pero sí figura en **segundo lugar mundial como objetivo del hacktivismo prorruso**. Son dos formas distintas de presión: una busca volumen y la otra, visibilidad política.

5.4 Qué tipo de ataques recibe España

El desglose nacional permite bajar del recuento agregado al tipo concreto de incidente, y el reparto es revelador: **el fraude y el código dañino se reparten prácticamente todo el volumen**, mientras que el ransomware, que domina la conversación pública, representa una fracción mínima del recuento aunque concentre la mayor parte del impacto.

Tabla 6. Incidentes gestionados en España durante 2025 por tipo.

Tipo de incidente	Casos en 2025	% del total	Comentario
Código dañino	55.411	45,3 %	De ellos, 392 de ransomware
Fraude en línea	45.445	37,2 %	25.133 corresponden a suplantación por correo
Robo de información	3.849	3,1 %	Credenciales y datos personales
Resto de tipologías	17.518	14,3 %	Intrusiones, disponibilidad y otros
Total gestionado	**122.223**	**100 %**	Un 26 % más que en 2024

Dos cifras del reparto merecen comentario. La primera es que **el 85 % de los sistemas identificados como parte de redes de equipos comprometidos son dispositivos del internet de las cosas**: cámaras, grabadores, routers domésticos y equipamiento industrial conectado sin mantenimiento. Es el punto ciego más grande del parque nacional. La segunda es que **el 59 % de los incidentes se detectó de forma proactiva** y no por aviso de la víctima, lo que indica una capacidad de vigilancia razonablemente madura.

En el terreno de los operadores esenciales, los 401 incidentes registrados se concentran en **banca (34 %), transporte (14 %) y energía (8 %)**. Ese reparto coincide con lo que muestra nuestra propia telemetría a escala global, con una salvedad: en España el peso del transporte es notablemente superior a la media internacional.

5.5 Cifras nacionales de incidentes

Las series oficiales españolas ofrecen la contrapartida necesaria a la telemetría internacional y dibujan un panorama considerablemente más intenso.

Tabla 7. Principales indicadores nacionales de ciberseguridad, España.

Indicador nacional	2024	2025	Variación
Incidentes gestionados por INCIBE-CERT	97.348	122.223	+25,6 %
Incidentes gestionados por CCN-CERT	177.098	~200.000	—
Incidentes en operadores esenciales e importantes	341	401	+17,6 %
Sistemas vulnerables notificados	183.851	237.028	+28,9 %
Consultas a la línea de ayuda 017	98.546	142.767	+44,9 %
Ciberdelitos registrados	464.801	488.426	+5,1 %
Ciberincidentes en operadores críticos	160	90	−43,8 %

De esta tabla salen tres cosas. La primera es que el crecimiento es generalizado y sostenido en todas las series salvo una. La segunda es que la excepción —la caída del 43,8 % en incidentes de operadores críticos— debe interpretarse con prudencia: revierte un pico anómalo, ya que los 160 casos de 2024 supusieron a su vez un aumento del 97,5 % sobre 2023. Procede además de un universo pequeño y muy sensible a cambios de criterio de notificación, y contrasta con el aumento del 17,6 % en operadores esenciales e importantes registrado por otra vía. La tercera es que los ciberdelitos representan ya el **19,8 % de toda la criminalidad registrada en España**, con casi nueve de cada diez correspondiendo a fraude informático.

Un dato del análisis nacional destaca por encima del resto: durante 2025 se registró un incremento cercano al **300 % en incidentes atribuibles a actores patrocinados por Estados** respecto al año anterior, junto con un mayor número de acciones coordinadas entre actores. Las campañas de ciberespionaje de origen ruso se identifican como las más numerosas y frecuentes, con un uso

creciente de técnicas asistidas por inteligencia artificial y, de forma llamativa, con colaboración operativa entre grupos tradicionalmente enfrentados.

6 Qué esperamos del segundo semestre

Este capítulo combina dos ejercicios distintos que no hay que confundir. El primero es una proyección cuantitativa de las series de PERSEUS, con su intervalo de confianza, que responde a la pregunta de cuánto. El segundo es un conjunto de escenarios cualitativos con probabilidad estimada e indicadores de alerta asociados, que responde a la pregunta de qué. El primero es más preciso; el segundo, más útil para tomar decisiones.

6.1 Cuántas vulnerabilidades esperamos

La proyección se apoya en supuestos explícitos de ritmo, no en un modelo estadístico cerrado. La razón es práctica: con una serie que ha cambiado de pendiente dos veces en dieciocho meses, un ajuste sobre el histórico largo se queda corto y uno sobre el corto se dispara. Un supuesto de ritmo tiene la ventaja de que cualquiera puede sustituirlo por el suyo y rehacer la cuenta.

El punto de partida son las **37.126 vulnerabilidades** registradas entre enero y junio de 2026 —contando los identificadores que después se rechazan, para mantener la serie homogénea—. Quedan seis meses de ejercicio y los tres escenarios se diferencian solo en el ritmo que se supone para ellos.

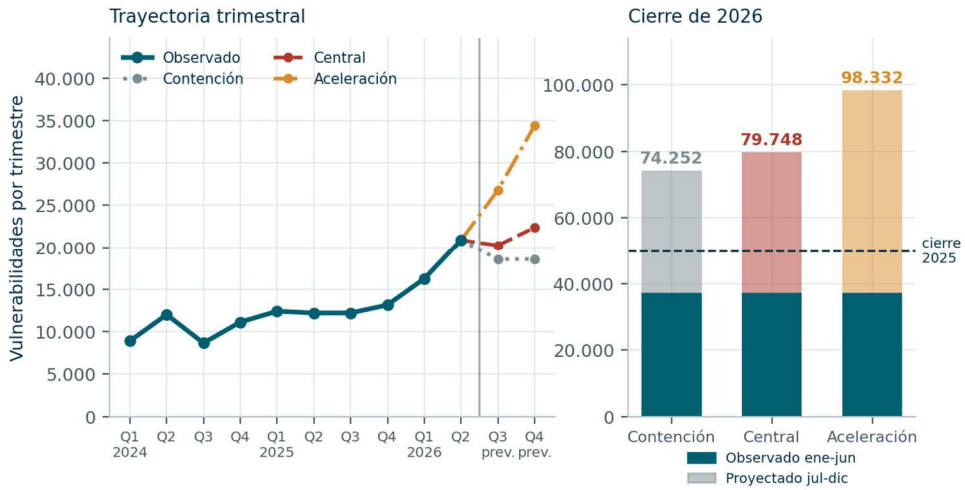

Figura 17. Proyección para el cierre de 2026. A la izquierda, trayectoria trimestral observada y proyectada; a la derecha, cierre de ejercicio en cada escenario.

Tabla 8. Escenarios de proyección. Cifras en la serie que incluye identificadores rechazados; descontados estos, el cierre equivaldría a 71.700, 77.000 y 95.000 respectivamente.

Escenario	Supuesto	Jul–dic	Cierre 2026	Var. 2025
Contención	El ritmo vuelve a la media del semestre (6.188 al mes)	37.126	**74.252**	+48,6 %
Central	Continúa la tendencia de los últimos seis trimestres (+10,6 % por trimestre)	42.622	**79.748**	+59,6 %
Aceleración	Se mantiene el salto entre trimestres de 2026 (+28,4 %)	61.206	**98.332**	+96,8 %

Nuestra estimación es que el escenario **central es probable** (55-74 %), con confianza media. Los dos factores que empujan al alza —más autoridades emisoras y herramientas de descubrimiento cada vez más baratas— siguen activos y no dan señales de agotarse. El que empuja a la baja es la capacidad de los organismos que mantienen los catálogos, que ya ha dado muestras de tensión y

puede acabar funcionando como cuello de botella administrativo: menos publicaciones, no menos fallos.

El escenario de **aceleración** lleva advertencia. Extrapola el salto de un solo trimestre, que es una base estrecha, y por eso lo damos como cota superior más que como pronóstico. Aun así no es descartable: encaja con el techo de los modelos de predicción que publican terceros.

Los tres escenarios encajan con el abanico que manejan otros analistas. Descontando los identificadores rechazados para poder compararlos, la **contención (71.700)** coincide casi exactamente con la extrapolación más citada del sector, que sitúa el cierre entre 71.000 y 72.000, y la **aceleración (95.000)** queda algo por encima del modelo de regresión más agresivo, que proyecta 90.831.

> **CÓMO USAR ESTA PROYECCIÓN**
>
> En el escenario central, el equipo de gestión de vulnerabilidades recibirá en el segundo semestre unas **42.600 entradas frente a las 37.126 del primero**: un **15 % más de carga**, y un ejercicio 2027 que arranca desde una base mucho mayor.
>
> La conclusión para el presupuesto no es ampliar la plantilla en proporción —no es viable—, sino invertir en **capacidad de descartar**: enriquecimiento automático con evidencia de explotación, cruce con el inventario real de activos y priorización por exposición. El objetivo es reducir cuántas vulnerabilidades llegan a un analista, no cuántos analistas hay.
>
> Y hay que anticipar el escenario contrario. Si se cumple la contención, la tentación será leerlo como una mejora. No lo sería: menos identificadores publicados por saturación de quienes los gestionan significa **menos visibilidad sobre los mismos fallos**.

6.2 Escenarios previstos

Los escenarios se expresan con la escala de estimación habitual en inteligencia: **casi seguro** (90-99 %), **muy probable** (75-89 %), **probable** (55-74 %), **posibilidad real** (40-54 %), **poco probable** (15-39 %) y **muy poco probable** (2-14 %). La **confianza** es cosa distinta de la probabilidad y va aparte: *alta* cuando el juicio se apoya en series consistentes y contrastadas, *media* cuando la evidencia es sólida pero parcial, *baja* cuando se construye sobre indicios y se ofrece por su valor de alerta.

Sobre la proyección cuantitativa construimos siete escenarios cualitativos. Cada uno lleva asociada una probabilidad estimada, un nivel de confianza y un conjunto de indicadores que permiten validarlo o descartarlo antes de que se materialice. Esos indicadores son la parte práctica: sirven para configurar la vigilancia de los próximos meses.

E1 · Un fallo en un equipo de red golpeará a varias organizaciones europeas a la vez

Probabilidad: muy probable (75-89 %). Confianza: alta. La combinación de tiempos de armamentización inferiores a una semana, ausencia de telemetría en estos equipos y concentración de la base instalada en un puñado de fabricantes hace prácticamente inevitable que al menos una vulnerabilidad crítica en un producto perimetral de amplia implantación derive en un incidente con impacto multiorganización antes de que acabe el año. El semestre analizado ya ha registrado varios episodios de este tipo; la previsión es de continuidad, no de novedad.

- **Vigilar:** publicación de una vulnerabilidad con puntuación superior a 9,0 en un producto de acceso remoto o cortafuegos de cuota alta; aparición de pruebas de concepto públicas en menos de 72 horas.

E2 · Robar datos ganará terreno frente a cifrarlos

Probabilidad: probable (55-74 %). Confianza: media. La proporción de casos con cifrado ha caído del 92 % al 78 % en dos años y la tasa de pago en operaciones de exfiltración pura es

sistemáticamente inferior, lo que en principio desincentivaría el modelo. Sin embargo, el menor coste operativo, el menor riesgo de detección y la menor exposición judicial compensan esa menor conversión. Esperamos que la tendencia continúe, aunque probablemente sin llegar a invertirse por completo dentro del ejercicio.

- **Vigilar:** aumento de reivindicaciones en sitios de filtración sin mención de cifrado; incremento de las demandas de rescate dirigidas a organizaciones de sectores con obligación de notificación reforzada.

E3 · Se documentará una campaña real dirigida en su mayor parte por una IA

Probabilidad: posibilidad real (40-54 %). Confianza: baja. Los dos umbrales cruzados en 2026 —desarrollo de exploits asistido y explotación autónoma en entorno de evaluación— establecen que la capacidad técnica existe. Lo que aún no se ha observado es su empleo sistemático en una campaña contra organizaciones reales, con el ciclo completo ejecutado de forma predominantemente autónoma. La barrera que queda no es de capacidad sino de fiabilidad: los análisis disponibles señalan que los modelos exageran hallazgos y fabrican datos con frecuencia suficiente para hacer poco práctica la autonomía completa.

- **Vigilar:** aparición de familias con lógica de decisión delegada a modelos externos en operaciones vivas; campañas con volumen de objetivos incompatible con dotación humana.

E4 · El ataque a un proveedor arrastrará a decenas de clientes

Probabilidad: muy probable (75-89 %). Confianza: alta. La proporción de brechas con implicación de terceros ronda ya el 48 % y la designación formal de proveedores tecnológicos críticos en el ámbito financiero es un reconocimiento institucional del riesgo de concentración. En el ámbito español, al menos uno de los seis incidentes destacados del semestre tuvo su origen declarado en un proveedor externo.

- **Vigilar:** incidentes reportados por proveedores de servicios gestionados; anomalías de acceso desde rangos de direcciones asociados a proveedores.

E5 · Cada vez costará más averiguar cómo entraron

Probabilidad: casi seguro (90-99 %). Confianza: alta. Es el escenario con menor incertidumbre de todo el capítulo. El crecimiento observado —factor 4,5 en el borrado de indicadores y 9,5 en el borrado de registros de eventos— es demasiado pronunciado y demasiado consistente entre familias distintas para ser un artefacto. La consecuencia esperable es un aumento del número de incidentes en los que la investigación no consigue determinar el vector de entrada.

- **Vigilar:** incremento de eventos de limpieza de registros; huecos temporales en la telemetría centralizada.

E6 · La ley española que traspone NIS2 entrará en el Congreso

Probabilidad: probable (55-74 %). Confianza: media. La remisión al Tribunal de Justicia con petición de sanciones económicas introduce una presión que no existía en los dieciocho meses anteriores. La experiencia con procedimientos similares sugiere que la tramitación se acelera notablemente tras este paso. Un plazo razonable situaría el inicio de la tramitación antes del cierre del ejercicio y la aprobación en 2027.

- **Vigilar:** publicación del dictamen definitivo del Consejo de Estado; aprobación del proyecto de ley en Consejo de Ministros.

E7 · Poco probables, pero de gran impacto

Se incluyen tres escenarios que consideramos **poco probables** dentro del ejercicio pero cuyo impacto justificaría una revisión de la planificación si llegaran a materializarse.

- **Un incidente destructivo con efecto físico sobre infraestructura crítica europea** *(poco probable, 15-39 %; confianza media).* Se han documentado ya casos de despliegue de código de

borrado contra instalaciones de generación en la Unión, y existen grupos especializados en preposicionamiento industrial. Lo que falta para el salto es la decisión política, no la capacidad técnica.

- **Un compromiso de la cadena de suministro que afecte a un componente criptográfico o de identidad de uso universal** *(poco probable, 15-39 %; confianza baja).* La demostración de que la procedencia criptográfica puede acreditar un artefacto malicioso abre la puerta a un incidente de este tipo, cuyo alcance sería difícil de acotar.
- **Un avance en computación cuántica que adelante materialmente el calendario de la amenaza** *(muy poco probable, 2-14 %; confianza baja).* Los tres trabajos publicados entre mayo de 2025 y marzo de 2026 han reducido las estimaciones de recursos en más de un orden de magnitud. Un cuarto avance de magnitud similar situaría el horizonte en un plazo incompatible con los calendarios de migración vigentes.

6.3 Qué amenazas pesan más

Como complemento a los escenarios, PERSEUS mantiene un modelo de 47 amenazas con probabilidad estructural asignada y un ajuste dinámico que incorpora la actividad observada en el periodo. El ajuste medio del semestre ha sido de **+24,8 puntos**, lo que refleja de forma agregada la intensidad del periodo.

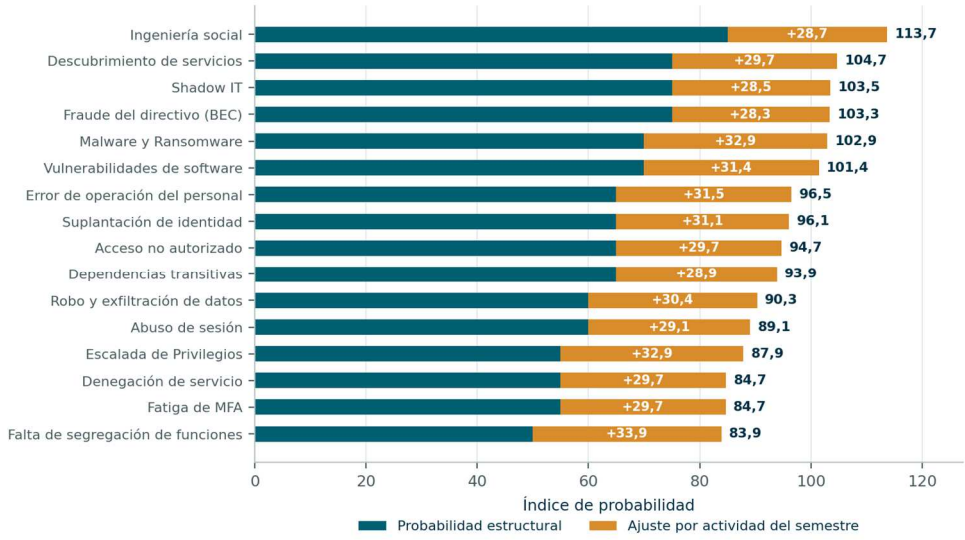

Figura 18. Modelo de amenazas de PERSEUS. Probabilidad estructural y ajuste por actividad observada durante el semestre, para las dieciocho amenazas de mayor puntuación.

Encabezan el modelo la **ingeniería social** (85 de base, +28,7 de ajuste), el **descubrimiento de servicios expuestos** (75 y +29,7), la **tecnología no gobernada o *shadow IT*** (75 y +28,5), el **fraude del directivo o compromiso del correo corporativo** (75 y +28,3) y el conjunto de **código dañino y ransomware** (70 y +32,9). Llama la atención que el mayor ajuste absoluto del semestre no corresponde a ninguna de estas: es el de las **sanciones por incumplimiento normativo** (+35,2), que refleja la presión regulatoria descrita en el capítulo anterior.

Del modelo se deducen dos cosas. La primera es que las seis amenazas principales se reparten a partes iguales entre las tres grandes familias: dos de ingeniería social, dos de ataque lógico y dos de fallo técnico. Ninguna categoría domina el cuadro. La segunda es que el *shadow IT* aparece en tercera posición: la tecnología que la organización desconoce que tiene es, en el modelo de PERSEUS, más probable como causa de incidente que la explotación de vulnerabilidades conocidas.

7 Recomendaciones

Las recomendaciones que siguen se ordenan por horizonte temporal y se han priorizado según el criterio de riesgo reducido por unidad de esfuerzo, tomando como referencia lo observado en el semestre. No pretenden ser exhaustivas: son las que, a juicio de los analistas de PERSEUS, tienen mayor rendimiento frente a las amenazas efectivamente activas.

7.1 Los próximos noventa días

Tabla 9. Prioridades inmediatas. La última columna indica qué capacidad hace falta para ejecutar cada acción, con independencia de que se resuelva con medios propios o externos.

Acción	Riesgo que mitiga	Esfuerzo	Capacidad necesaria
Inventariar y clasificar todo activo expuesto a internet, con especial atención a equipamiento de red y appliances de seguridad	Explotación de perímetro	Medio	Superficie de exposición externa
Establecer un circuito de parcheo de menos de 72 horas para ese subconjunto, con verificación posterior a la aplicación	Ventana de exposición en el vector principal	Medio	Gestión de vulnerabilidades
Retirar de internet todo plano de administración y consola de gestión que no requiera exposición pública	Superficie de ataque directa	Bajo	Auditoría de seguridad
Garantizar el reenvío inmediato de registros a un destino que el origen no pueda modificar, y alertar sobre la ausencia de eventos esperados	Borrado de rastro	Medio	SOC 24×7
Revisar el procedimiento de verificación de identidad del servicio de atención al usuario, especialmente para restablecimientos y alta de segundo factor	Ingeniería social y suplantación	Bajo	Concienciación
Inventariar las herramientas de administración y monitorización remota autorizadas, y bloquear el resto por lista blanca	Abuso de utilidades legítimas	Medio	EDR y XDR
Auditar credenciales almacenadas en claro en repositorios, configuraciones, variables de entorno e interfaces de contenedores	Credenciales sin proteger	Medio	Auditoría y seguridad del desarrollo
Revisar la configuración de cuentas de servicio del directorio: contraseñas largas, cifrado moderno, preautenticación obligatoria	Robo de contraseñas de servicio	Bajo	Gestión de identidades
Vigilar la aparición de credenciales corporativas en fuentes de filtración y forzar su invalidación	Acceso con credenciales válidas	Bajo	Vigilancia digital

7.2 De aquí a fin de año

Tabla 10. Prioridades para el segundo semestre.

Acción	Riesgo que mitiga	Esfuerzo	Capacidad necesaria
Desplegar autenticación resistente a suplantación en administración, acceso remoto y cuentas privilegiadas	Interceptación de sesión	Alto	Gestión de identidades

Acción	Riesgo que mitiga	Esfuerzo	Capacidad necesaria
Implantar detección por anomalía de comportamiento, además de la detección por artefacto	Operaciones sin código dañino	Alto	SOC 24×7, NDR y XDR
Incorporar caza proactiva de amenazas sobre la telemetría ya disponible	Permanencia prolongada sin detección	Alto	Caza de amenazas
Ensayar la restauración empezando por los servicios de identidad, no por los datos	Denegación deliberada de recuperación	Medio	Continuidad y ciberejercicios
Desplegar control de movimiento de información hacia el exterior con umbrales calibrados por área	Extorsión por exfiltración	Alto	NDR y servicios gestionados
Endurecer la cadena de construcción: fijación de versiones, periodos de espera y desactivación de guiones de instalación	Compromiso de la cadena de suministro	Medio	Seguridad del desarrollo
Revisar el riesgo de los proveedores con acceso a sistemas o datos propios	Compromiso a través de terceros	Medio	Riesgo de terceros y GRC
Construir y ensayar el procedimiento de notificación en 24 y 72 horas exigido por el Reglamento de Ciberresiliencia	Incumplimiento normativo	Medio	GRC y cumplimiento
Extender la visibilidad a la frontera entre tecnología de información y de operación	Preposicionamiento en entornos industriales	Alto	Seguridad OT e industrial
Anticipar qué campañas y actores apuntan al propio sector y geografía	Ceguera ante amenazas dirigidas	Medio	Ciberinteligencia

7.3 Qué medir

Un plan de acción sin indicadores es una declaración de intenciones. Los siguientes son los que recomendamos seguir, elegidos porque son medibles con los datos que la mayoría de las organizaciones ya tiene y porque se mueven cuando las medidas funcionan.

- **Tiempo medio de aplicación de parches en activos expuestos a internet.** El objetivo razonable es inferior a 72 horas para vulnerabilidades con explotación confirmada. Medirlo por separado del parque general es imprescindible: la media global lo enmascara.
- **Porcentaje de vulnerabilidades con explotación confirmada remediadas a 7 y a 30 días.** Es el indicador que mejor correlaciona con el riesgo real y el que la regulación empieza a exigir.
- **Cobertura de autenticación resistente a phishing sobre cuentas privilegiadas.** Expresado en porcentaje de cuentas, no de usuarios, y desglosado por tipo de acceso.
- **Proporción de activos que reportan telemetría de forma continua**, y tiempo medio de detección de un cese de reporte. Este segundo dato es el que detecta el borrado de rastro.
- **Número de herramientas de administración remota distintas observadas en la red frente a las autorizadas.** La diferencia entre ambas cifras es superficie de ataque directa.
- **Tiempo desde la aparición de una credencial corporativa en fuentes de filtración hasta su invalidación.** Dado que tres de cada cuatro víctimas de ransomware tuvieron una fuga previa, este indicador es un anticipador de incidente.

8 Cómo trabajamos

Este informe describe problemas concretos. Esta última sección explica cómo los abordamos, ordenada por esos mismos problemas y no por catálogo de servicios. Si ya dispone de estas capacidades, le sobra y no pasa nada.

8.1 Anticipar lo que viene

El informe deja un dato difícil de ignorar: **tres de cada cuatro víctimas de ransomware habían sufrido una fuga de credenciales en el año anterior**, y la mitad en los noventa días previos. La información existía antes del incidente; lo que faltaba era mirarla. → **Ciberinteligencia**, **vigilancia digital** y **gestión de la superficie de exposición externa**.

8.2 Conocer y reducir la exposición

Con 35.364 vulnerabilidades publicadas en seis meses y la severidad ya inservible como criterio, el problema dejó de ser parchear y pasó a ser **decidir qué se parchea**. A eso se suma comprobar que lo desplegado resiste de verdad. → **Gestión de vulnerabilidades**, **auditorías y pruebas de intrusión**, **Red Team y simulación de adversario**, **seguridad en la nube**, **seguridad del ciclo de desarrollo** y **seguridad OT e industrial**.

8.3 Detectar y responder a tiempo

Aquí está el argumento central, y lo sostienen tres cifras del propio informe: el tiempo medio de propagación dentro de una red es de **29 minutos** —el más rápido observado, 27 segundos—, en el cuartil más veloz se llega a la extracción de datos en **72 minutos**, y automatizar la seguridad ahorra **1,93 millones por incidente y 65 días de ciclo**. Puestas juntas dicen algo incómodo: **un servicio de detección que responde en horas llega tarde por definición**. No es un problema de talento ni de herramientas, sino de tiempo de reacción, y el tiempo de reacción se gana automatizando lo que no requiere criterio humano para que el criterio humano se dedique a lo que sí lo requiere. → **SOC gestionado 24×7 con SIEM y SOAR**, **EDR, NDR y XDR**, **caza de amenazas**, **respuesta a incidentes y análisis forense** y **servicios gestionados de seguridad**.

8.4 Controlar el acceso y proteger el dato

La identidad es el hilo conductor de casi todas las cadenas de ataque reconstruidas este semestre, y la extorsión se ha desplazado del cifrado a la amenaza de publicar. → **Gestión de identidades y accesos privilegiados**, **seguridad del correo electrónico**, **continuidad, recuperación y ciberejercicios**.

8.5 Gobernar y sostener en el tiempo

El calendario normativo es exigente, casi la mitad de las brechas implica a un tercero y el factor humano interviene en el 62 %. Ninguna de las tres cosas se resuelve con tecnología. → **GRC y cumplimiento** frente a NIS2, DORA, el Reglamento de Ciberresiliencia y el Esquema Nacional de Seguridad, **riesgo de terceros y cadena de suministro** y **concienciación y formación**.

9 Anexos

9.1 Anexo A · Glosario

Tabla 11. Glosario de términos empleados en el informe.

Término	Definición
ATT&CK	Marco público de clasificación de tácticas y técnicas adversarias mantenido por MITRE. Este informe emplea la matriz empresarial en su versión más reciente.
Dispositivo de borde	Equipamiento situado en el límite de la red y expuesto a internet: cortafuegos, concentradores VPN, balanceadores, pasarelas de correo y consolas de gestión asociadas.
Explotación confirmada	Vulnerabilidad con evidencia pública de aprovechamiento real, no meramente teórico. Equivale a la inclusión en catálogos de vulnerabilidades explotadas conocidas.
Impulso	Indicador propio de PERSEUS. Mide el crecimiento de la frecuencia de una técnica en los últimos noventa días respecto a los noventa anteriores, normalizado entre 0 y 1.
Infostealer	Código dañino especializado en la extracción de credenciales, cookies de sesión y datos de autenticación del equipo comprometido.
Living off the land	Técnica consistente en emplear exclusivamente herramientas y binarios legítimos ya presentes en el sistema, evitando la introducción de artefactos detectables.
Novedad	Indicador propio de PERSEUS. Mide la rareza de una técnica en el corpus histórico, en escala logarítmica. Un valor alto indica una técnica poco frecuente.
Preposicionamiento	Obtención y mantenimiento de acceso a un entorno sin ejecutar acción hostil visible, con vistas a una acción futura.
Procedencia criptográfica	Mecanismo que acredita dónde y cómo se construyó un artefacto de software. Acredita el origen, no la ausencia de código dañino.
Tiempo hasta la explotación	Intervalo entre la publicación de una vulnerabilidad y su primer aprovechamiento observado. Un valor negativo indica que la explotación precedió a la disponibilidad del parche.