
Observatorio TAI
Ciberresiliencia
PATROCINADORES
CHECK POINT
Silverfort
SOPHOS
TAI
ciberseguridadTIC
directorTIC

Introducción

Ciberresiliencia: el nuevo indicador de madurez empresarial

La ciberresiliencia se ha convertido en uno de los pilares estratégicos de las organizaciones modernas. En un entorno en el que las amenazas evolucionan con la misma rapidez que la innovación tecnológica, la diferencia entre una empresa vulnerable y otra preparada radica en su capacidad para anticipar, adaptarse y mantener la continuidad del negocio ante cualquier incidente. Así lo subraya el World Economic Forum, que sitúa los ciberataques entre los cinco mayores riesgos globales para la próxima década, junto con los conflictos geopolíticos y la crisis climática.

El concepto de resiliencia digital, impulsado desde la Unión Europea a través de marcos regulatorios como NIS2 o DORA, ha pasado de ser una aspiración a convertirse en una obligación. Según la Agencia de Ciberseguridad de la Unión Europea (ENISA), el 62 % de las organizaciones europeas ha sufrido al menos un incidente grave en los últimos doce meses, y más de la mitad reconoce que su capacidad de respuesta sigue siendo limitada. La resiliencia, por tanto, se consolida como una métrica del grado de preparación y madurez organizativa: no se trata solo de prevenir, sino de asegurar la continuidad operativa ante cualquier contingencia.

Los datos globales refuerzan esta urgencia. El IBM X-Force Threat Intelligence Index 2025 señala que el coste medio de una brecha de seguridad se mantiene por encima de los 4,8 millones de dólares, mientras que el tiempo medio de detección y contención supera los 230 días. Más del 70 % de las organizaciones encuestadas por la consultora Ponemon Institute reconoce que, pese a haber incrementado sus presupuestos en ciberseguridad, no se siente preparada para responder a un ataque de gran escala. La diferencia, cada vez más, reside menos en las herramientas y más en la capacidad de anticipación, coordinación y aprendizaje organizativo.

En España, la ciberresiliencia avanza, aunque de manera desigual. El Informe Nacional de Ciberseguridad 2024, elaborado por el INCIBE, ci-

fra en más de 83.000 los incidentes gestionados durante el último año, un 14 % más que en 2023. La Oficina de Coordinación Cibernética (OCC) alerta de un incremento notable de los ataques dirigidos contra infraestructuras críticas y servicios esenciales, mientras que el Centro Criptológico Nacional (CCN-CERT) insiste en la necesidad de reforzar los planes de continuidad y respuesta. A pesar de estos datos, sólo un 38 % de las empresas españolas dispone de una estrategia formal de resiliencia digital, y apenas un 27 % ha realizado simulacros o pruebas de recuperación en el último año.

> La ciberresiliencia ha pasado de ser un objetivo técnico a convertirse en un requisito estratégico de supervivencia

La transformación digital, la adopción masiva del *cloud*, la inteligencia artificial y la interconexión de sistemas han incrementado la complejidad de las infraestructuras corporativas, haciendo más difícil mantener el control sobre los activos críticos y las cadenas de suministro. Como señalan numerosos analistas, la resiliencia no depende únicamente de la fortaleza tecnológica, sino de la coordinación entre áreas, la cultura organizativa y la capacidad de aprendizaje tras cada incidente.

Conscientes de este desafío, Ciberseguridad TIC lanza el primer Observatorio de Ciberresiliencia, un proyecto que combina el análisis cuantitativo de la realidad empresarial española con la visión de los líderes del sector. El estudio cuenta con la colaboración de Check Point Software, Mastercard, Silverfort y Sophos, y con las aportaciones de directivos de ciberseguridad y tecnología de algunos de los sectores más críticos de la economía nacional.

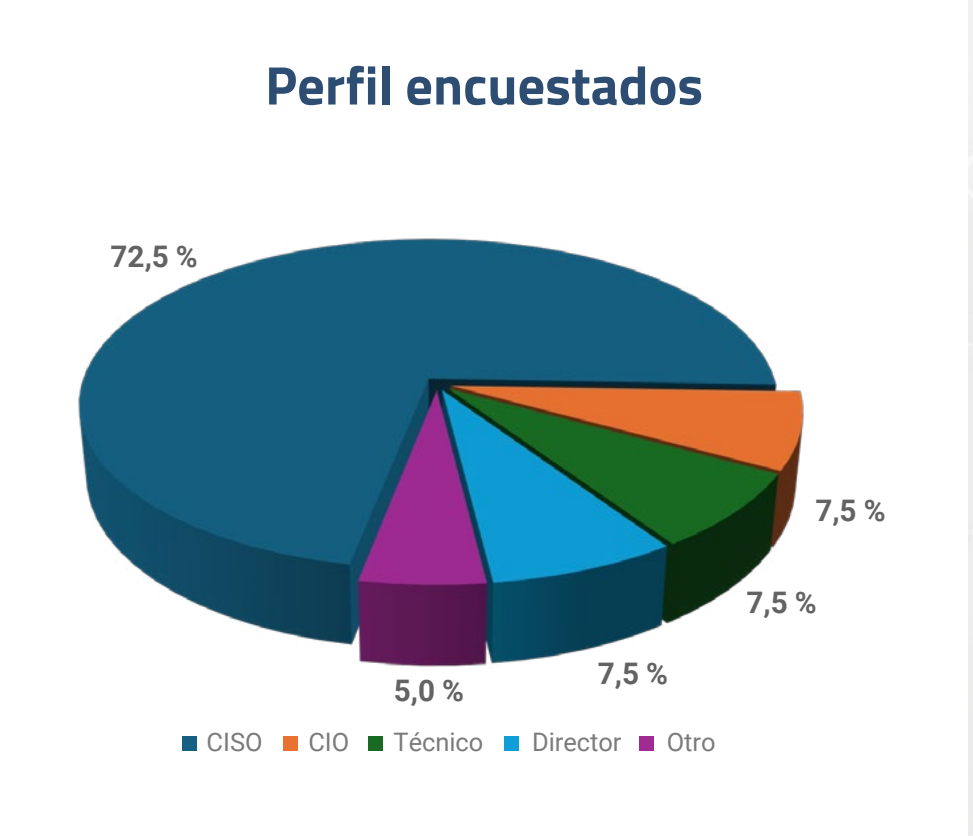
A través de este observatorio, se busca comprender cómo están abordando las empresas la resiliencia en un escenario de riesgos crecientes, qué barreras enfrentan y qué estrategias están demostrando ser más eficaces. Porque, más allá de la prevención, la pregunta clave hoy es otra: ¿está preparada la empresa española para resistir y recuperarse ante un ciberataque?

Tipología de la muestra

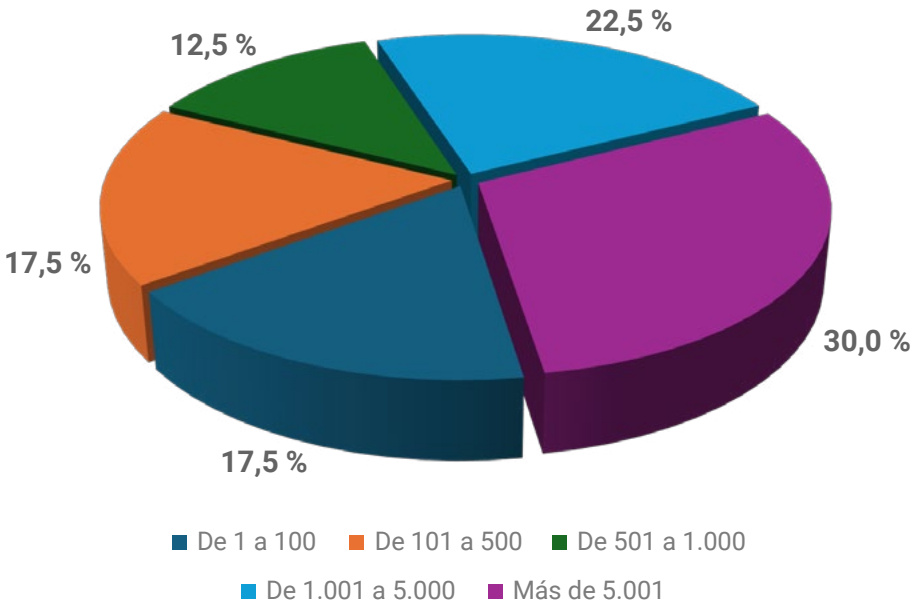
La composición de la muestra confiere al estudio una visión cualificada y representativa del tejido empresarial con mayor madurez en ciberseguridad. El 72,5 % de los participantes son CISO, lo que garantiza una lectura centrada en la práctica real de la resiliencia y en los desafíos estratégicos de seguridad. A ellos se suman CIO, directores y técnicos en proporciones equilibradas, aportando una perspectiva complementaria entre la gestión y la ejecución operativa.

En cuanto al tamaño empresarial, más de la mitad de las organizaciones (52,5 %) supera los 1.000 empleados, lo que refuerza la validez de los resultados en entornos complejos y distribuidos. Sin embargo, la presencia de pymes (35 %) añade contraste y permite identificar diferencias en recursos y enfoques.

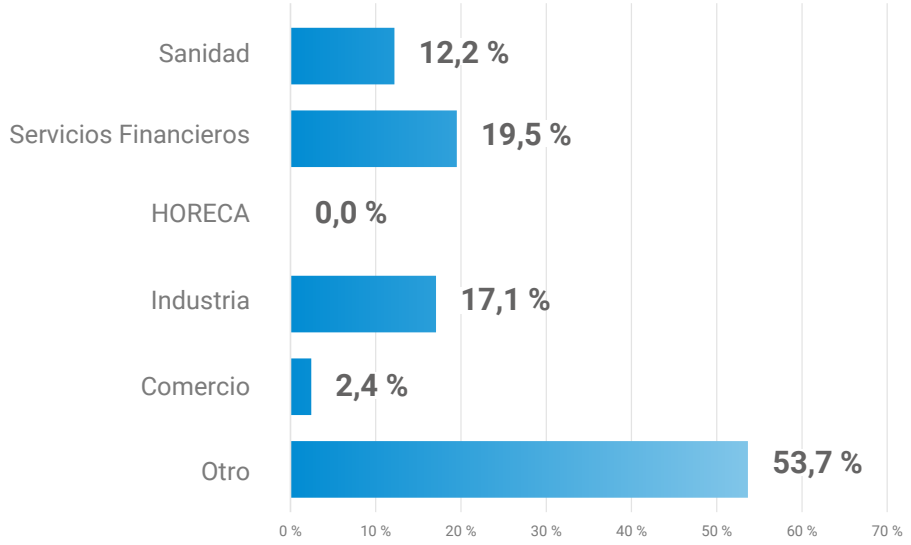
Por sectores, predominan servicios financieros, industria y sanidad, junto a un 53,7 % catalogado como “otros”, que incluye ámbitos tecnológicos, educativos y de servicios profesionales, aportando diversidad y amplitud de visión sobre el estado de la ciberresiliencia en España.



Tamaño de empresa

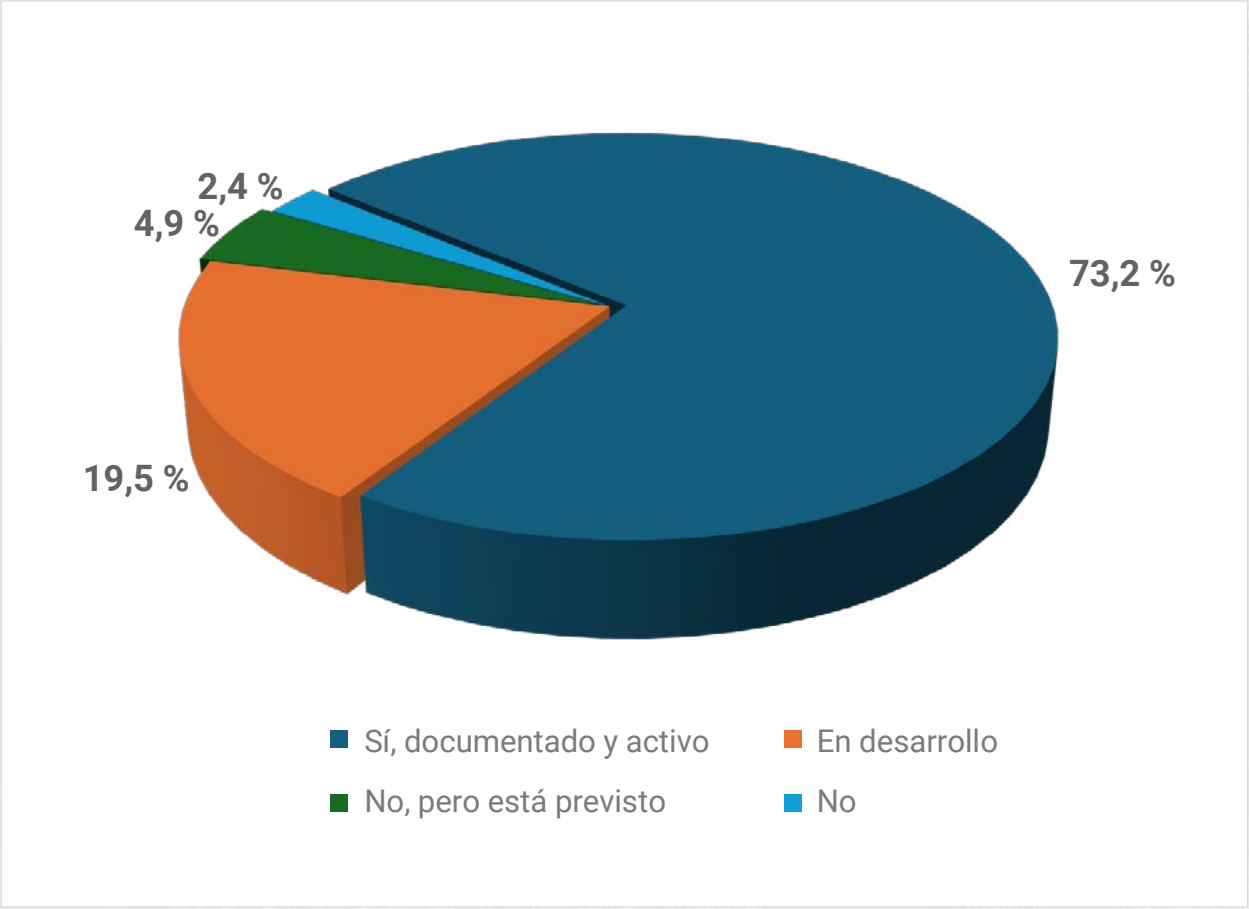


Sector de actividad



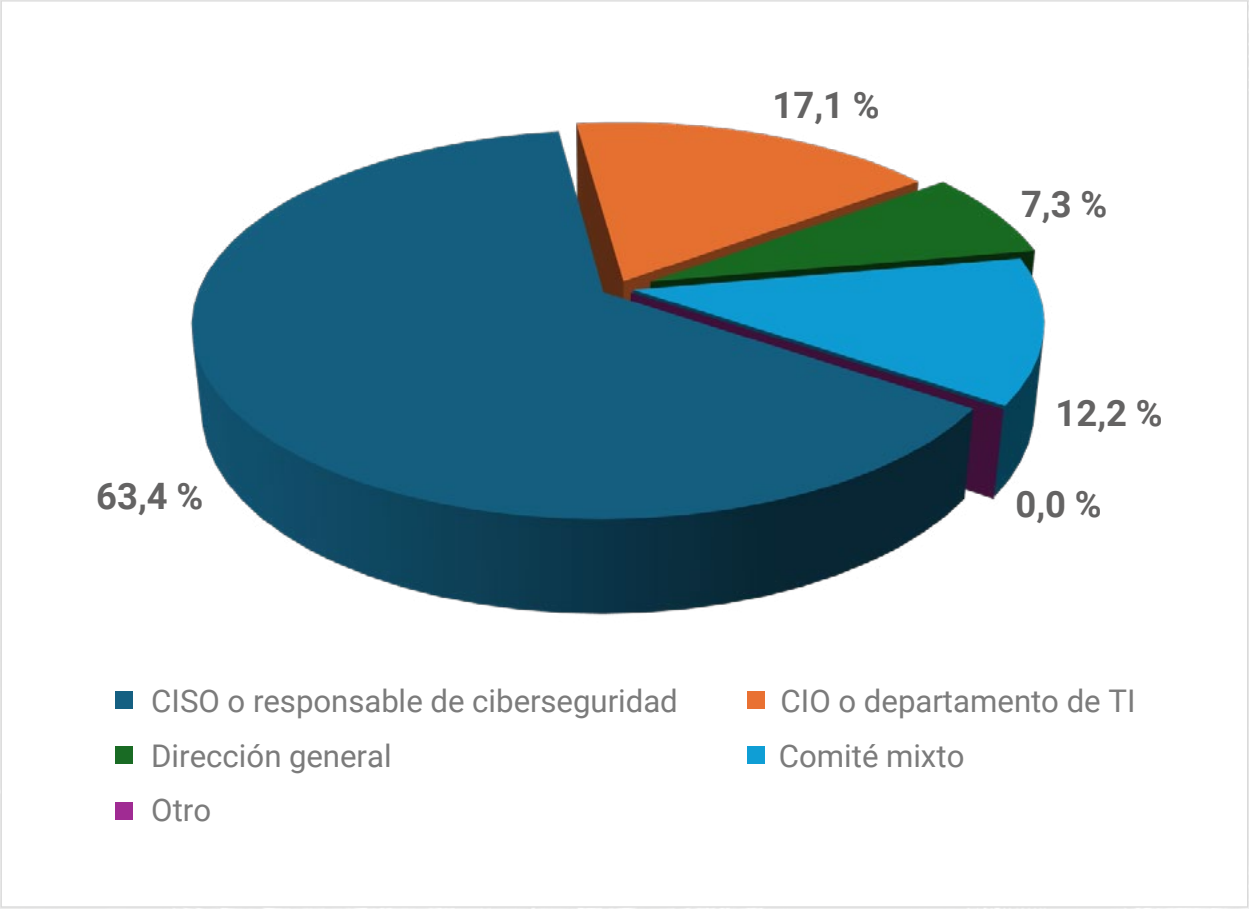
Resultados del estudio

1. ¿Tiene su organización un plan formal de ciberresiliencia?



El 73,2 % de las organizaciones dispone de un plan formal de ciberresiliencia documentado y activo, mientras que un
19,5 % lo tiene en desarrollo. Solo un 7,3 % carece aún de estrategia, aunque la mayoría prevé implantarla a corto plazo.
Este dato refleja un salto de madurez: la ciberresiliencia ha pasado de ser un concepto aspiracional a integrarse en la gestión operativa. La presión regulatoria —con marcos como NIS2 o DORA— y la frecuencia de incidentes disruptivos han impulsado esta evolución. El desafío ahora no es disponer de un documento, sino mantenerlo vivo, con revisiones, simulacros y métricas que garanticen su eficacia ante un ataque real y aseguren que la continuidad del negocio sea una responsabilidad compartida por toda la organización.

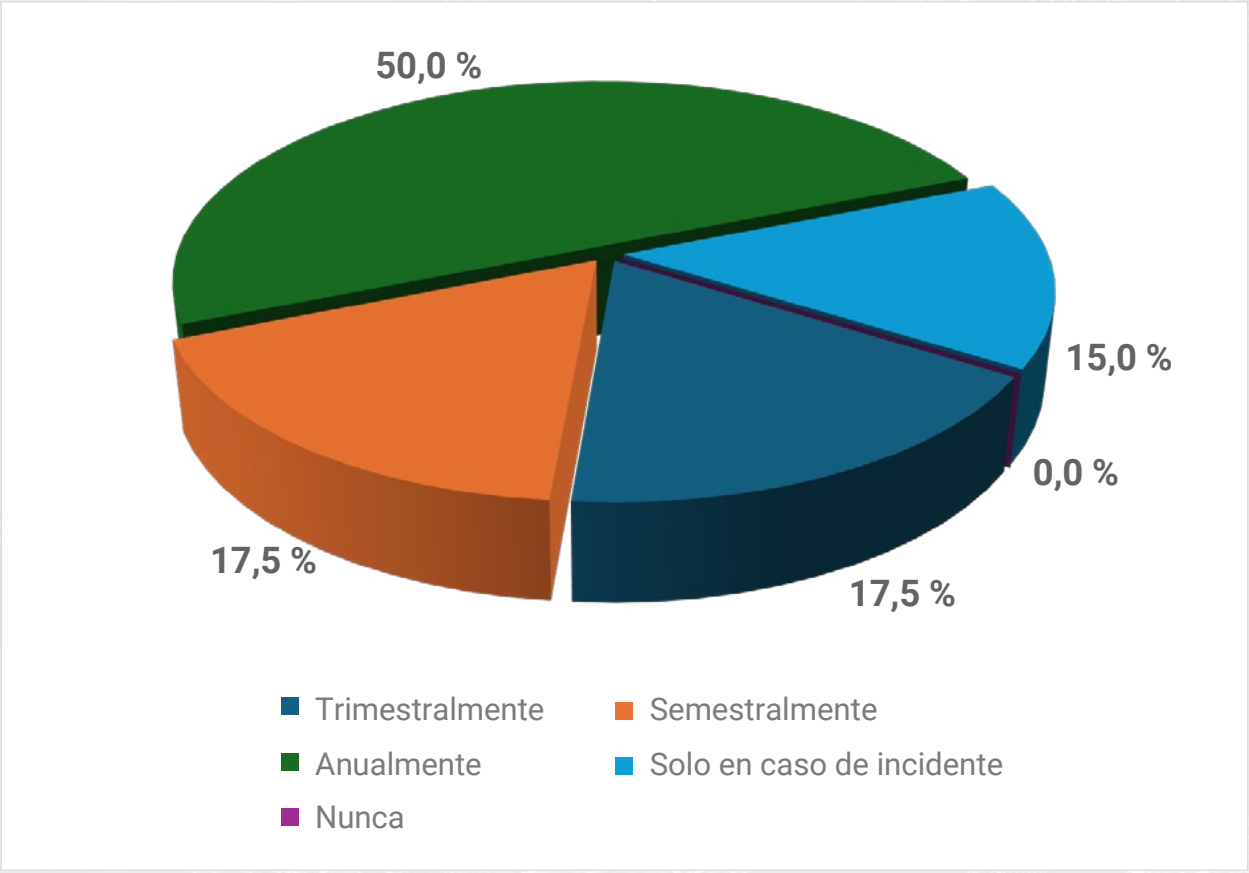
2. ¿Quién lidera la estrategia de ciberresiliencia en su organización?



En la mayoría de las empresas, la ciberresiliencia está liderada por el CISO o responsable de ciberseguridad (63,4 %), lo que evidencia su consolidación como una función estratégica dentro del ámbito de seguridad. Un 17,1 % mantiene esta responsabilidad bajo el CIO o departamento de TI, mientras que sólo un 7,3 % depende directamente de la dirección general. Por su parte, un 12,2 % ha optado por comités mixtos, reflejando un modelo más colaborativo.

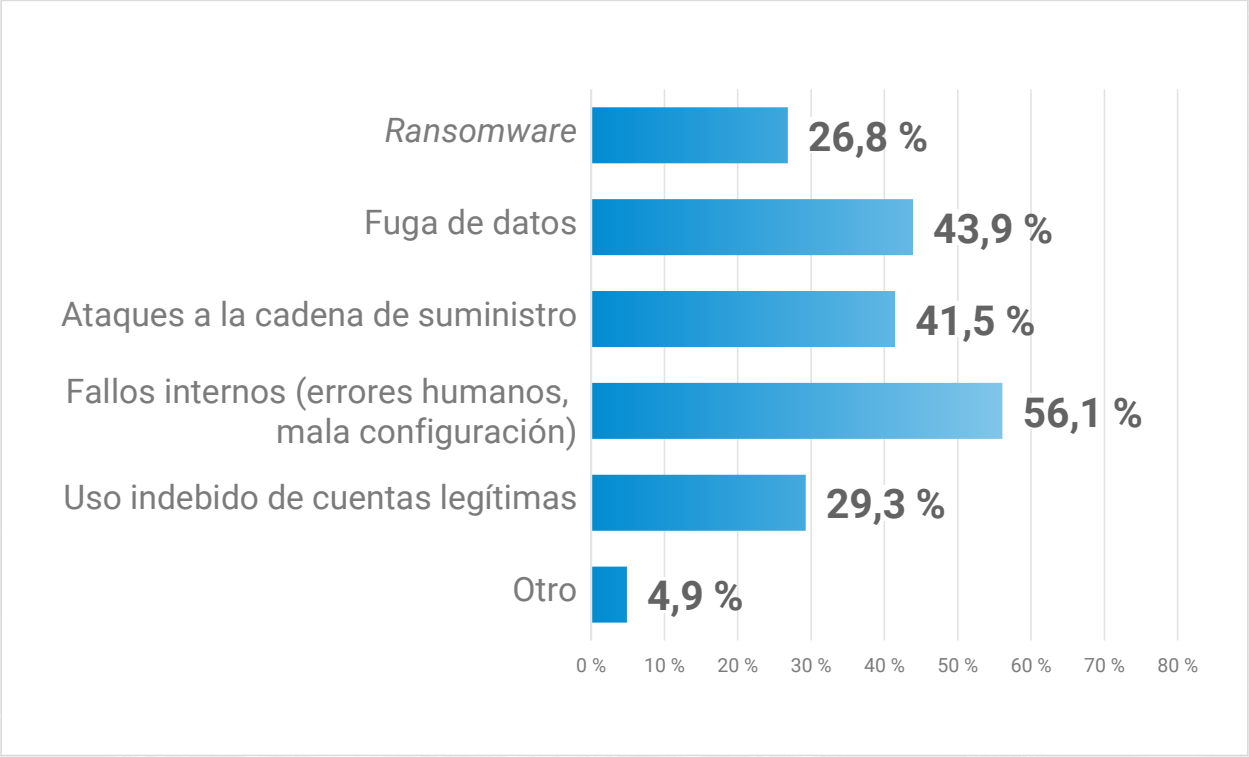
Estos datos confirman que la resiliencia se percibe principalmente como un asunto técnico, aunque la tendencia apunta a un enfoque más transversal, donde negocio, riesgos y tecnología comparten responsabilidades. A medida que crece la exposición digital, el liderazgo efectivo exige integrar la resiliencia en la estrategia corporativa, con una gobernanza que trascienda el ámbito puramente tecnológico.

3. ¿Con qué frecuencia realiza su organización simulacros o pruebas de recuperación frente a incidentes críticos?



La mitad de las organizaciones (50 %) realiza simulacros o pruebas de recuperación una vez al año, mientras que un 35 % lo hace con mayor frecuencia —17,5 % trimestralmente y 17,5 % semestralmente—. Un 15 % solo ejecuta estas pruebas tras sufrir un incidente, y ninguna reconoce no haberlas hecho nunca. Las pruebas anuales resultan útiles, pero no siempre bastan para validar la agilidad de los equipos ni la coordinación interdepartamental. La tendencia más avanzada pasa por incorporar simulacros periódicos y realistas, incluyendo escenarios de *ransomware*, fallo de proveedor o pérdida de datos críticos, que permitan medir y mejorar los tiempos de detección, respuesta y recuperación.

4. ¿Qué tipo de incidente considera más probable que afecte a su organización en los próximos 12 meses?

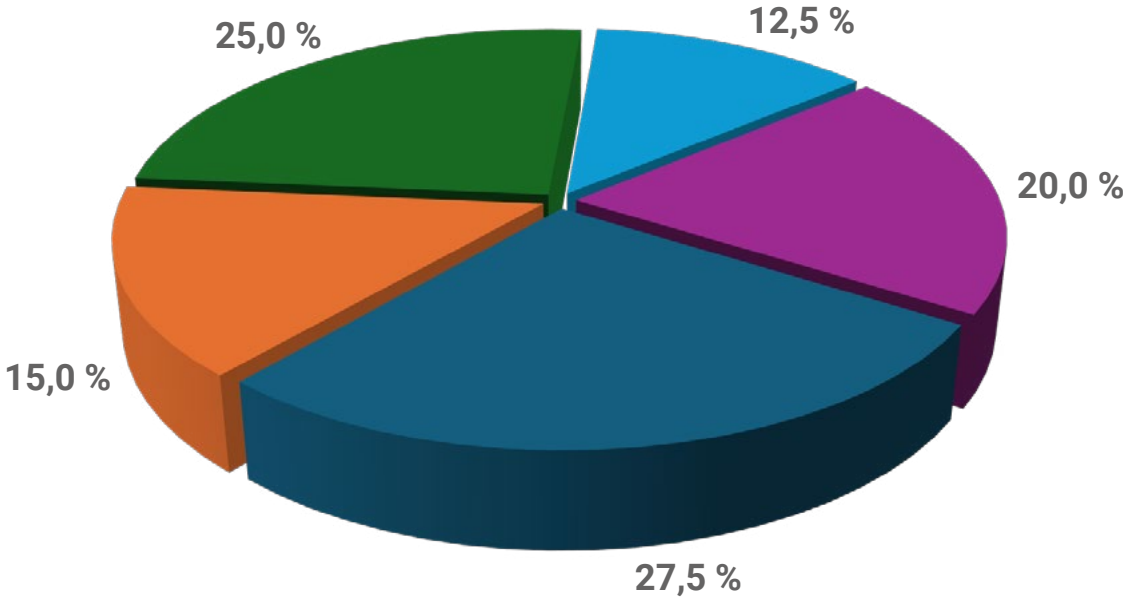


Los fallos internos, derivados de errores humanos o configuraciones inadecuadas, son percibidos como la principal amenaza por el 56,1% de los encuestados. Le siguen las fugas de datos (43,9 %) y los ataques a la cadena de suministro (41,5 %), dos riesgos cada vez más frecuentes en entornos interconectados.

El *ransomware* (26,8 %) y el uso indebido de cuentas legítimas (29,3 %) aparecen en segundo plano, aunque siguen siendo vectores críticos.

Este reparto sugiere una visión más realista y madura: las organizaciones identifican los riesgos internos y la complejidad del ecosistema digital como las fuentes principales de vulnerabilidad. La prevención ya no se centra únicamente en el ataque externo, sino también en la gestión del error y la exposición interna, elementos clave para lograr una resiliencia efectiva.

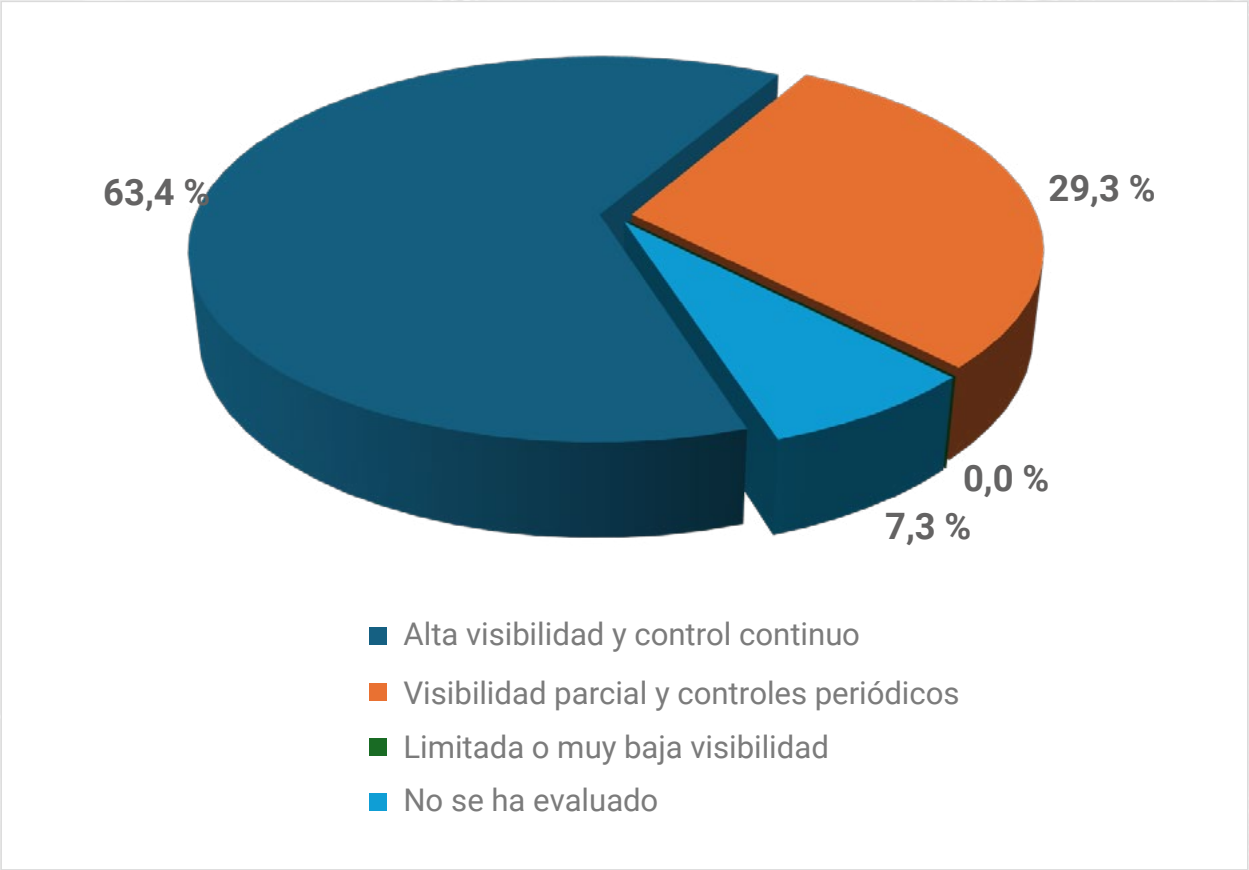
5. ¿Cuál de las siguientes áreas considera más crítica para su resiliencia operativa?



La gestión de accesos e identidades (27,5 %) se sitúa como el pilar más crítico para garantizar la resiliencia operativa, seguida de la detección y respuesta ante amenazas (25 %) y la formación del personal (20 %). Por detrás quedan la protección del dato (15 %) y la automatización de la respuesta (12,5 %), todavía en fases incipientes de adopción.

La lectura es clara: las organizaciones son conscientes de que la identidad se ha convertido en el nuevo perímetro de seguridad, y que un control deficiente puede comprometer todo el ecosistema digital. Al mismo tiempo, la atención a la formación subraya la importancia del factor humano en la resiliencia. El reto inmediato será avanzar hacia una resiliencia automatizada, capaz de reducir tiempos de detección y respuesta sin depender exclusivamente de la intervención manual.

6. ¿Qué grado de visibilidad y control tiene su organización sobre los activos y accesos críticos (incluidas identidades humanas y no humanas)?

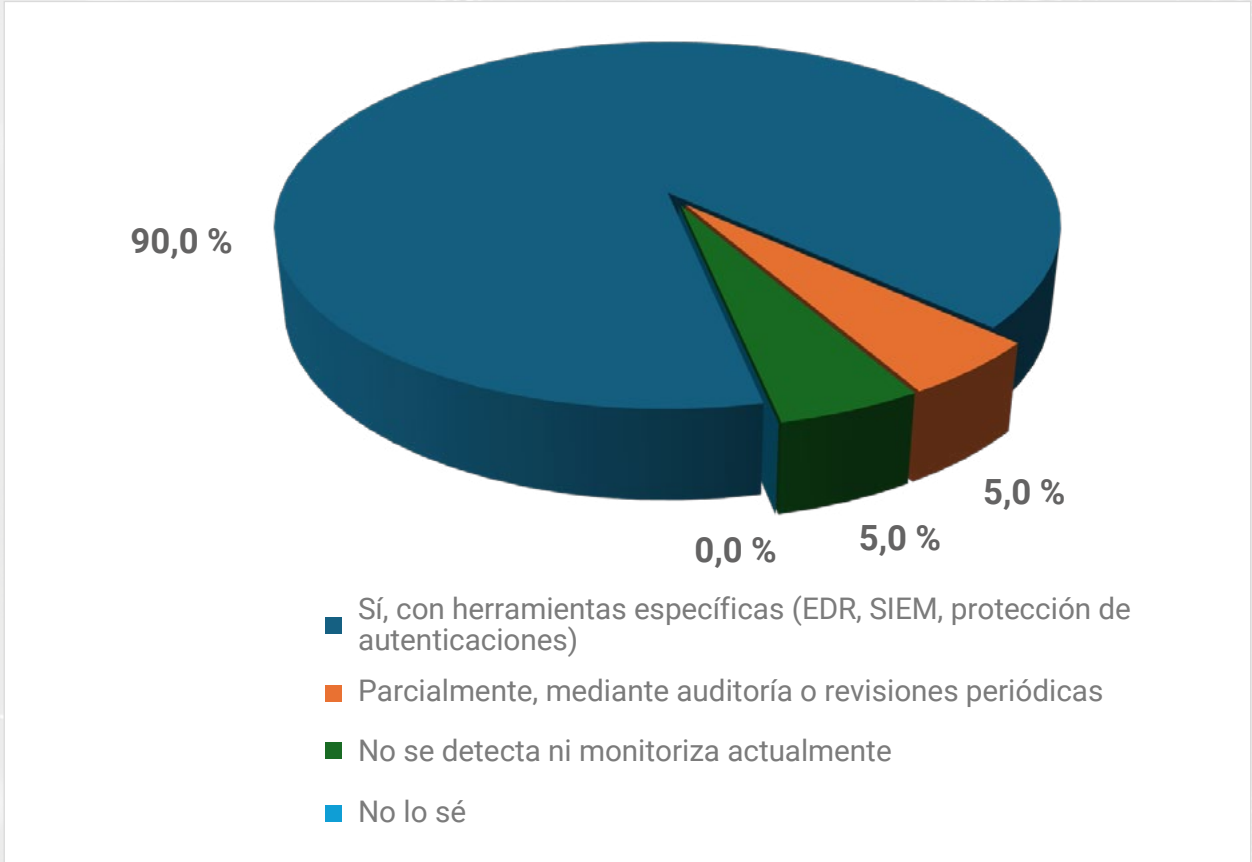


Un 63,4 % de las organizaciones declara contar con una alta visibilidad y control continuo sobre sus activos y accesos críticos, mientras que un 29,3 % reconoce disponer solo de una visión parcial. Un 7,3 % admite no haber evaluado aún este aspecto, y ninguna afirma tener visibilidad baja. Los resultados transmiten una confianza generalizada, aunque posiblemente más percibida que real.

En entornos cada vez más híbridos, con múltiples identidades no humanas (servicios, API, máquinas), mantener un control completo sigue siendo un desafío. El avance hacia una gestión unificada de identidades y activos es clave para reducir la superficie de exposición.

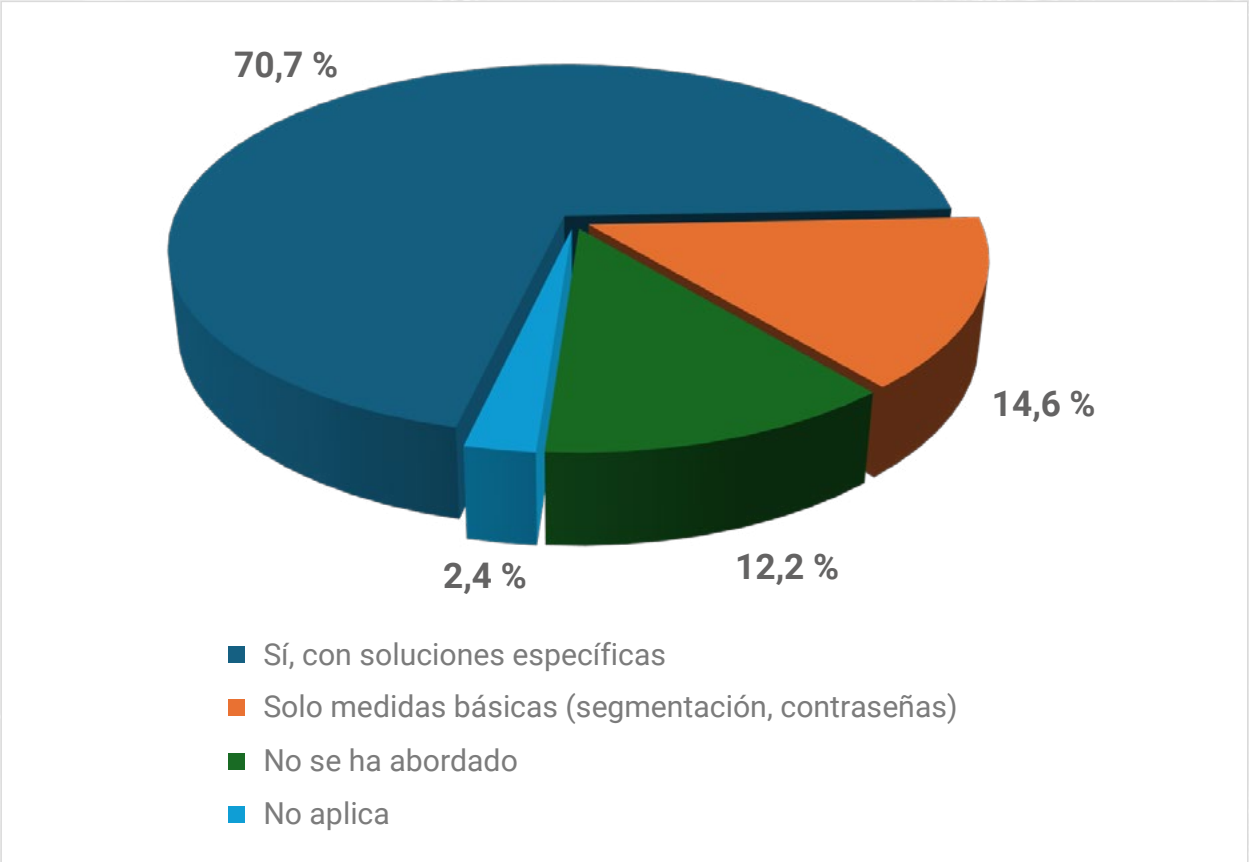
El siguiente paso pasa por consolidar la supervisión continua y automatizada, que permita detectar anomalías en tiempo real y asegurar la trazabilidad de todos los accesos.

7. ¿Su organización cuenta con medidas específicas para detectar y responder ante movimientos laterales y abuso de cuentas válidas?



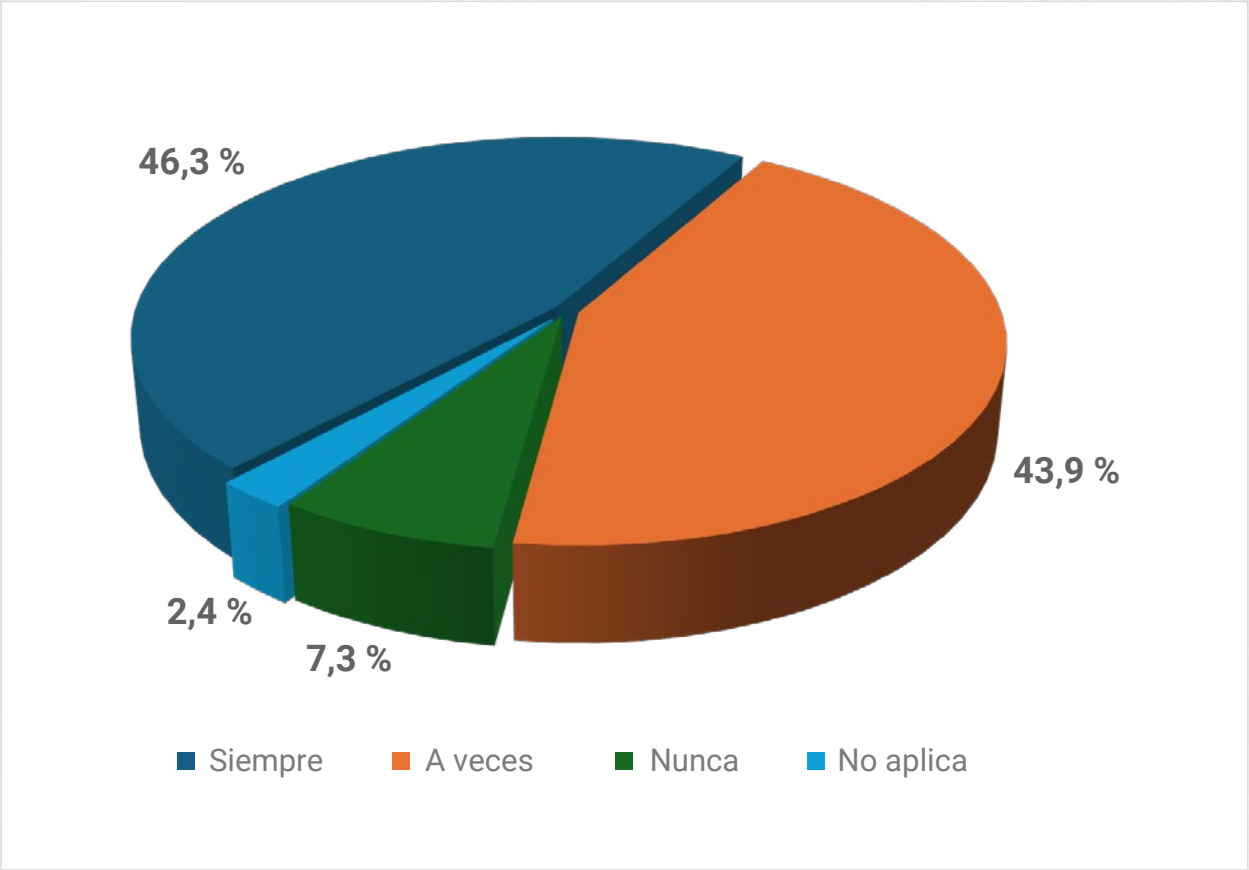
Un 90 % de las organizaciones afirma disponer de herramientas específicas —como EDR, SIEM o sistemas de protección de autenticaciones— para detectar y responder ante movimientos laterales o uso indebido de cuentas válidas. Sólo un 5 % lo hace de forma parcial y otro 5 % reconoce no monitorizar este tipo de actividades. Estos datos reflejan un grado de preparación elevado, impulsado por la adopción de tecnologías avanzadas y por la creciente conciencia sobre ataques que explotan credenciales legítimas. Sin embargo, la mera presencia de herramientas no garantiza eficacia: la detección de patrones anómalos requiere configuración, correlación y respuesta automatizada. El reto para las organizaciones será evolucionar hacia una gestión inteligente de identidades y comportamientos, capaz de anticipar movimientos laterales antes de que se materialicen.

8. ¿Dispone su organización de medidas concretas para proteger Active Directory u otros servicios de identidad críticos?



El 70,7 % de las organizaciones cuenta con soluciones específicas para proteger Active Directory u otros servicios de identidad, mientras que un 14,6 % se limita a medidas básicas, como contraseñas reforzadas o segmentación. Un 12,2 % admite no haber abordado aún esta protección y un 2,4 % considera que no le aplica. Dado que los servicios de directorio son el corazón de la infraestructura de identidades, estos datos reflejan una madurez significativa, aunque con margen de mejora. Los ataques dirigidos a AD siguen siendo una de las principales vías de movimiento lateral y escalado de privilegios. Protegerlo implica aplicar controles específicos —auditoría continua, separación de privilegios, autenticación multifactor y alertas en tiempo real—. La prioridad ahora debe ser reforzar la monitorización y segmentar entornos administrativos para reducir el impacto potencial de una intrusión.

9. ¿Incluye su organización criterios de ciberresiliencia en la selección y evaluación de terceros (proveedores, *partners*)?

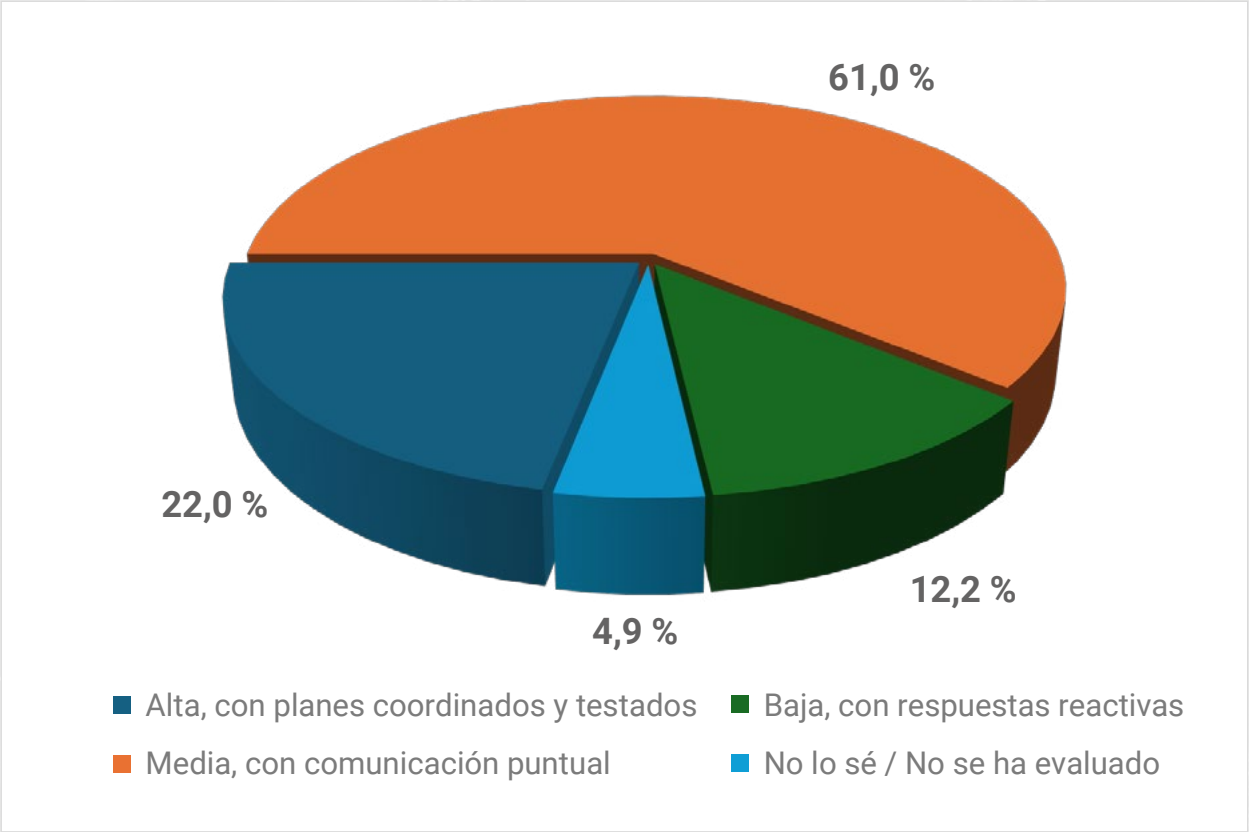


Casi la mitad de las organizaciones (46,3 %) afirma incluir siempre criterios de ciberresiliencia en la evaluación de sus proveedores o socios, mientras que un 43,9 % lo hace solo en algunos casos.
Un 7,3 % reconoce no considerarlo nunca y un 2,4 % señala que no aplica.
Los resultados reflejan una conciencia creciente sobre los riesgos de la cadena de suministro, aunque la práctica aún no es universal. La dependencia de terceros convierte la resiliencia compartida en un componente esencial de la seguridad corporativa. Sin embargo, la aplicación irregular de estos criterios muestra que muchas organizaciones aún no integran la ciberresiliencia en los procesos de compra u homologación. Avanzar hacia un modelo maduro exigirá estandarizar exigencias, incluir métricas de cumplimiento y realizar simulacros conjuntos que prueben la continuidad ante incidentes interconectados.

10. ¿Tiene en cuenta los riesgos asociados a la IA generativa en su estrategia de continuidad y seguridad?

Un 35 % de las organizaciones afirma haber integrado ya los riesgos de la IA generativa en sus análisis de seguridad y continuidad, mientras que un 55 % se encuentra en fase de evaluación. Sólo un 10 % reconoce no haberlo considerado todavía. Los datos recogidos en el estudio muestran que la mayoría de las empresas está comenzando a incorporar la IA generativa en su marco de riesgos, impulsada por su rápida adopción en procesos de negocio. El foco no se limita al uso de modelos públicos, sino también a la exposición de datos sensibles y a la manipulación de resultados generados por IA. La tendencia apunta hacia una gobernanza progresiva, donde la gestión de riesgos de IA se integre con la ciberseguridad tradicional, estableciendo políticas claras, controles técnicos y formación específica para empleados y desarrolladores.

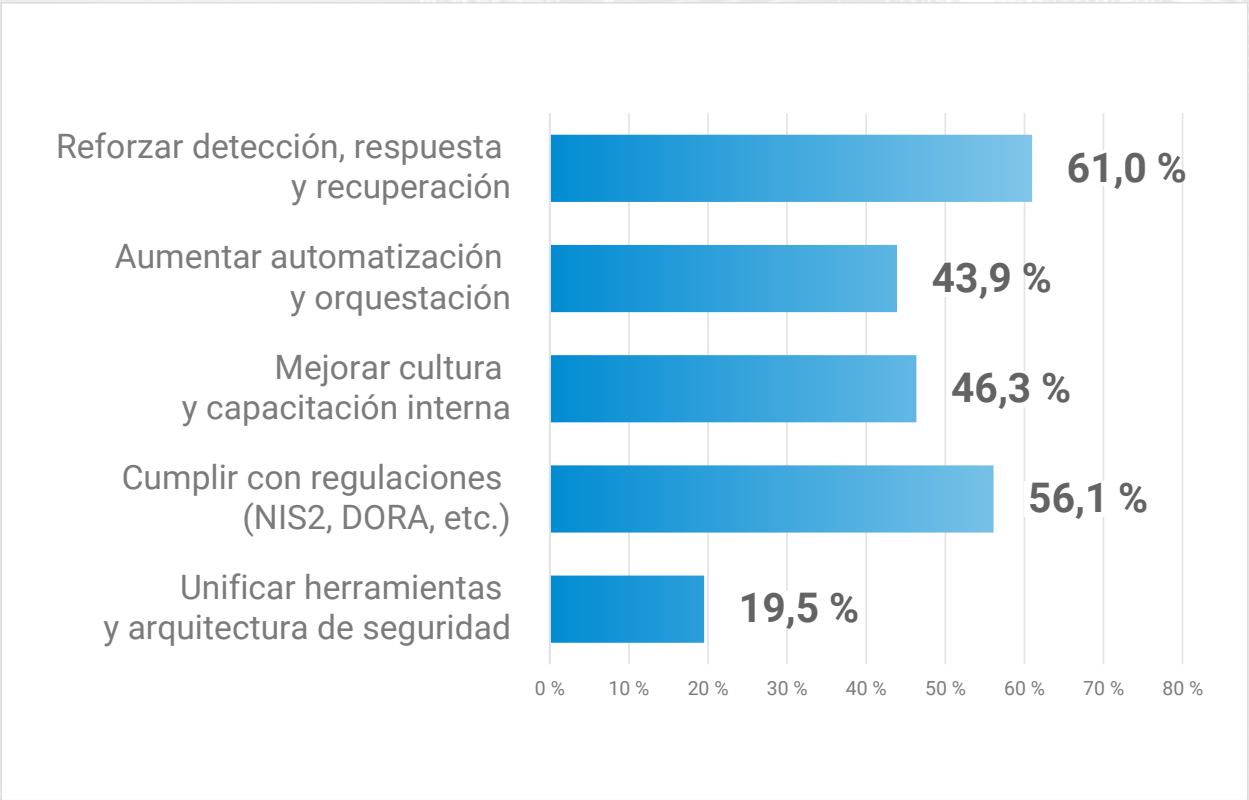
11. ¿Cómo evalúa la preparación de su sector ante un incidente que afecte a múltiples actores interconectados (clientes, proveedores, *partners*)?



Sólo un 22 % de las organizaciones considera que su sector está bien preparado ante un incidente que afecte de forma simultánea a varios actores, con planes coordinados y probados. La mayoría (61 %) valora su preparación como media, limitada a comunicaciones puntuales, mientras que un 12,2 % la percibe baja y reactiva. Un 4,9% admite no haberlo evaluado.

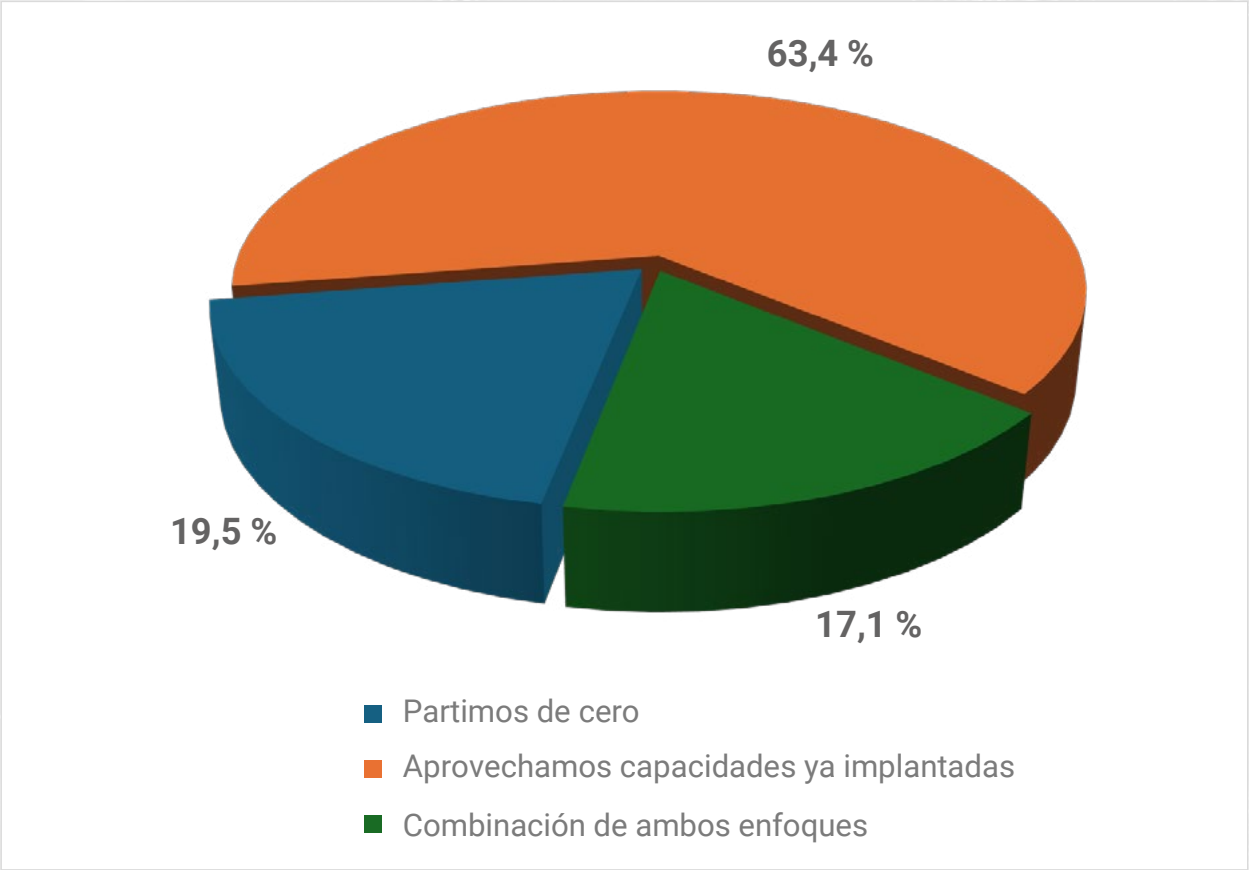
Este resultado evidencia que, aunque las empresas refuerzan su propia resiliencia, la coordinación intersectorial sigue siendo una asignatura pendiente. Los ciberataques con efecto dominó, como los sufridos en cadenas logísticas o proveedores de servicios críticos, han demostrado la importancia de contar con mecanismos conjuntos de respuesta y comunicación. El desafío inmediato pasa por establecer canales colaborativos y protocolos sectoriales que garanticen una reacción sincronizada ante incidentes de gran impacto.

12. ¿Qué prioridad principal guiará su estrategia en los próximos 12 meses?



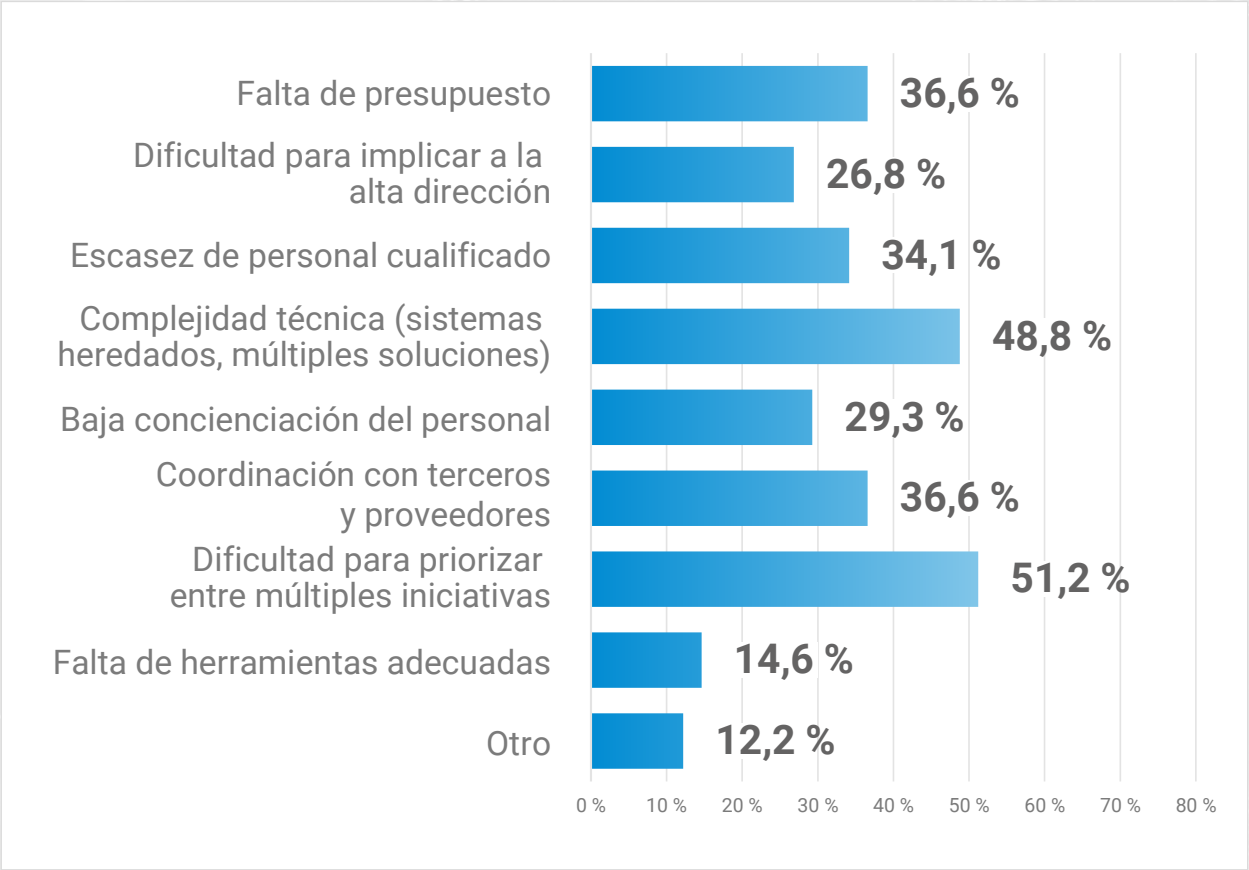
De cara al próximo año, las prioridades estratégicas se concentran en reforzar la detección, respuesta y recuperación ante incidentes (61 %) y en cumplir con las nuevas regulaciones, como NIS2 o DORA (56,1 %). También destaca la intención de mejorar la cultura y la capacitación interna (46,3 %), mientras que solo una minoría prioriza la unificación de herramientas (19,5 %) o la automatización y orquestación (13,9 %). Este reparto evidencia que las organizaciones están centradas en consolidar sus capacidades básicas y cumplir con los requisitos normativos, más que en transformaciones tecnológicas profundas. Sin embargo, el avance hacia una resiliencia real exigirá integrar automatización, orquestación y optimización de arquitecturas, reduciendo complejidad y dependencia de la intervención manual. La madurez regulatoria es el motor actual, pero la eficiencia operativa marcará el siguiente paso.

13. Para diseñar su estrategia de resiliencia, ¿partieron de cero o aprovecharon capacidades existentes?



La mayoría de las organizaciones (63,4 %) afirma haber aprovechado capacidades ya implantadas al diseñar su estrategia de resiliencia, mientras que un 19,5 % partió desde cero y un 17,1 % combinó ambos enfoques. Estos resultados reflejan una tendencia pragmática: las empresas buscan consolidar inversiones previas en seguridad, continuidad o infraestructura antes de iniciar nuevos proyectos. Esta integración permite avanzar con rapidez y contener costes, pero también puede heredar limitaciones si las soluciones existentes no fueron concebidas para entornos modernos o distribuidos. La clave está en evaluar la madurez real de esas capacidades y alinearlas con los nuevos requisitos de gobernanza y automatización. La resiliencia, más que un punto de partida, debe concebirse como un proceso evolutivo, que combine experiencia previa con innovación y mejora continua.

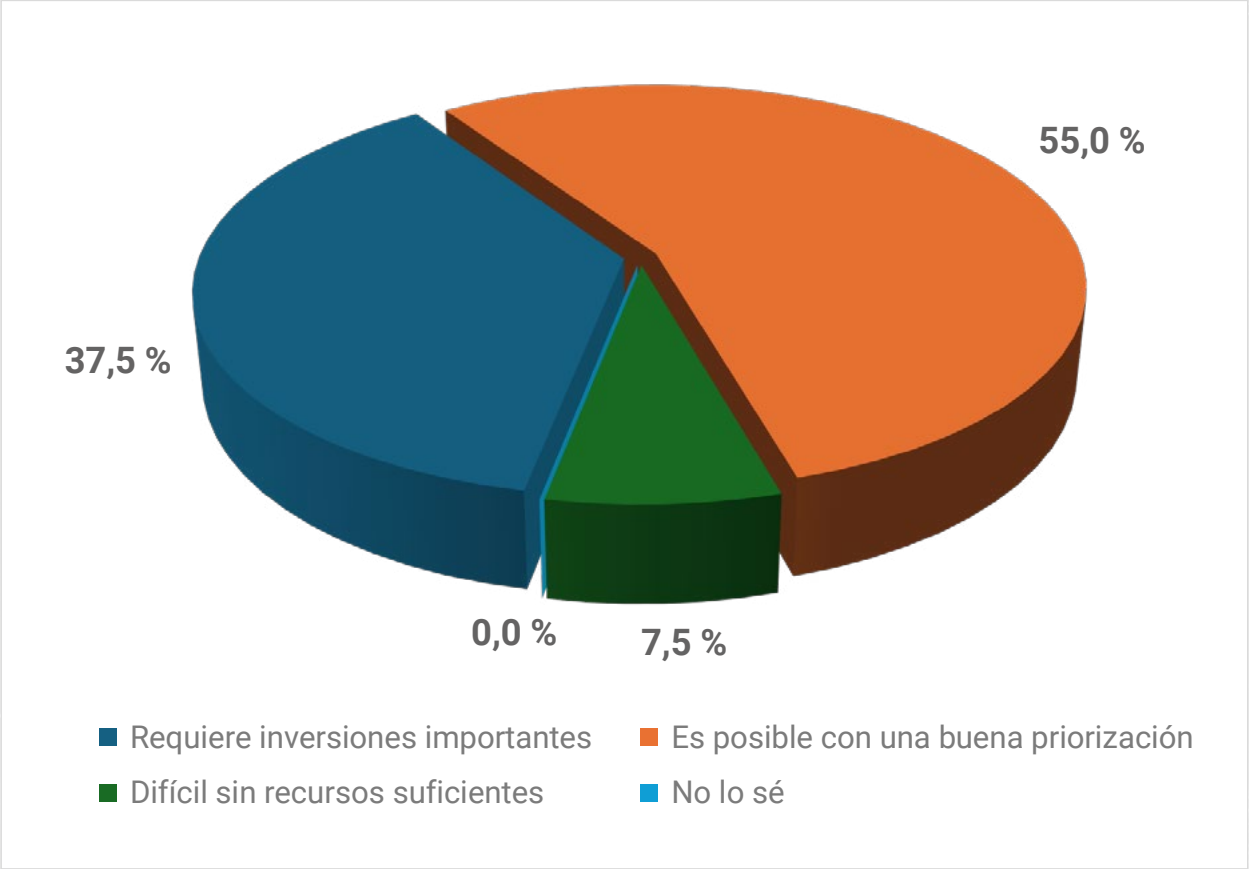
14. ¿Cuáles han sido las principales dificultades en la implantación de su estrategia de resiliencia?



La dificultad para priorizar entre múltiples iniciativas (51,2 %) y la complejidad técnica de entornos heredados y múltiples soluciones (48,8 %) son los principales obstáculos para consolidar la resiliencia. Les siguen la falta de presupuesto (36,6 %), la coordinación con terceros (36,6 %) y la escasez de personal cualificado (34,1 %), que reflejan limitaciones tanto operativas como de gestión. También influyen la baja concienciación del personal (29,3 %) y la escasa implicación de la alta dirección (26,8 %), factores que evidencian una madurez desigual entre las áreas técnicas y de negocio. Un 14,6 % señala la falta de herramientas adecuadas y un 12,2 % otros motivos.

En conjunto, los resultados muestran que el reto no es sólo económico o tecnológico, sino organizativo, y requiere liderazgo, foco y gobernanza clara para avanzar de forma sostenida.

15. ¿Cree que una buena resiliencia requiere grandes inversiones o puede alcanzarse con presupuestos limitados?



Más de la mitad de las organizaciones (55 %) considera que la resiliencia puede alcanzarse con una buena priorización, mientras que un 37,5 % opina que requiere inversiones importantes y un 7,5 % la ve difícil sin recursos suficientes.

Estos resultados apuntan a una visión pragmática: la ciberresiliencia no depende únicamente del presupuesto, sino de cómo se planifican y asignan los recursos. La madurez en procesos, la automatización y el aprovechamiento de capacidades ya existentes son factores decisivos para optimizar la inversión. Este enfoque refuerza la idea de que la resiliencia es tanto una cuestión de gestión como de tecnología. Las organizaciones más avanzadas son aquellas que consiguen equilibrar la inversión con la priorización inteligente de riesgos, enfocando los esfuerzos donde el impacto potencial es mayor.

Sumario ejecutivo

Los resultados del Observatorio TAI de Ciberresiliencia reflejan un panorama maduro y en plena evolución. La mayoría de las organizaciones españolas ha pasado de la simple reacción ante incidentes a una gestión estructurada y proactiva de la resiliencia digital. Casi tres de cada cuatro empresas cuentan ya con un plan formal y activo, mientras el liderazgo del CISO se consolida como figura clave en la coordinación de las estrategias y la toma de decisiones.

El enfoque dominante es pragmático: las compañías priorizan reforzar capacidades existentes antes que iniciar proyectos desde cero, buscando equilibrio entre cumplimiento normativo, eficiencia operativa y sostenibilidad presupuestaria. Sin embargo, la práctica de simulacros regulares, la verificación de la eficacia de las defensas y la coordinación intersectorial siguen siendo áreas con margen de mejora. Aunque nueve de cada diez organizaciones disponen de herramientas para detectar movimientos laterales o abusos de identidad, la verdadera resiliencia exige validar su eficacia y entrenar de forma constante la respuesta humana.

La identidad y el dato se consolidan como los ejes de la resiliencia operativa, seguidos de la cultura corporativa y la formación del personal. También emerge un interés creciente por integrar la inteligencia artificial —incluida la generativa— en las evaluaciones de riesgo, lo que demuestra una sensibilidad cada vez mayor hacia los nuevos vectores de exposición.

Entre las principales dificultades, destacan la falta de priorización, la complejidad técnica y la coordinación con terceros, factores que revelan la necesidad de avanzar hacia una gobernanza más transversal y colaborativa. Aun así, la mayoría de los encuestados considera que la resiliencia no depende de grandes inversiones, sino de una planificación adecuada y del aprovechamiento inteligente de los recursos disponibles.

En conjunto, las organizaciones españolas están avanzando hacia una resiliencia inteligente y sostenible, basada en la anticipación, la colaboración y la mejora continua. El reto ahora es consolidar lo aprendido, medir el progreso y convertir la ciberresiliencia en un hábito operativo y no solo en una meta estratégica.

La resiliencia se consolida como un indicador de madurez digital en las empresas españolas

TAI Editorial ha presentado un nuevo estudio dentro de su serie de Observatorios, esta vez dedicado a la ciberresiliencia empresarial. Los resultados del informe, que analiza el grado de madurez de las organizaciones españolas ante los desafíos de seguridad, continuidad y cumplimiento normativo, fueron presentados por Javier Carvajal, CEO de Icraitas.

Rosalía Arroyo

Javier Carvajal, CEO y socio fundador de **Icraitas**

Durante la presentación de los resultados del Observatorio, Javier Carvajal, CEO de Icraitas, subrayó que el objetivo del estudio no es sólo "visibilizar", sino "observabilizar" lo que sucede, permitiendo a las organizaciones tener una visión estratégica, táctica y operativa de su madurez en ciberresiliencia.

El perfil de los participantes en el estudio refleja el interés creciente de las compañías por este ámbito: un alto porcentaje de CISOs y responsables de seguridad, junto a técnicos y directivos, lo que en palabras de Carvajal, muestra "una representación magnífica del interés de la ciberseguridad en las compañías". En cuanto al tamaño de las empresas, la mayoría supera los mil empleados, aunque también se incluyen pymes, lo que permite comparar recursos, madurez y capacidades. "La dificultad en las pequeñas no es

tecnológica", señaló el directivo, "sino de recursos humanos y económicos".

Sobre la resiliencia, recordó que "representa la capacidad de una organización para anticipar, resistir, adaptarse y recuperarse eficazmente ante una disrupción digital", algo que —dijo— "es esencial en la vida personal, profesional y empresarial". Según el estudio, el 74 % de las empresas cuenta ya con un plan formal de resiliencia, aunque Carvajal matizó que "muchas veces lo revisamos sólo cuando viene el auditor; tenemos que actuar sobre el esfuerzo que ya hemos empeñado".

El liderazgo de la estrategia de ciberresiliencia recae mayoritariamente en el CISO o responsable de seguridad (63 %), pero sólo un 7 % está directamente impulsado por la dirección general. Advirtió Javier Carvajal que esto debe cambiar: "NIS2 y DORA trasladan la responsabilidad a la alta dirección y a los consejeros. Este porcentaje crecerá porque la ley les obliga a implicarse".

En cuanto a la práctica, el 50 % de las organizaciones realiza simulacros periódicos. Admitiendo que tener un plan es bueno, puntualizó el CEO de Icraitas que "lo importante es probarlo, revisarlo y corregirlo". Los incidentes más probables siguen siendo ransomware, fugas de datos y abusos de identidad, con un papel cada vez más relevante del factor humano.

> Según Javier Carvajal, CEO de Icraitas, el objetivo del estudio no es sólo "visibilizar", sino "observabilizar" lo que sucede

Entre las áreas críticas, destaca la gestión de identidades y accesos (27,5 %), seguida de la protección del dato. El estudio también muestra que el 63 % de las empresas afirma tener alta visibilidad y control continuo, aunque el ponente distinguió entre ver y observar: "Una cosa es visibilizar y otra observabilizar. Puedo tener la información, pero si no la trato ni la interpreto, no sirve de nada", aseguró ante la audiencia.

Respecto a la gestión del riesgo con terceros, casi la mitad de las organizaciones afirma evaluar criterios de ciberresiliencia en sus proveedores, aunque Javier Carvajal cuestionó la profundidad real de ese análisis: “Nos piden cuestionarios declarativos, pero no siempre comprometen. Si tienes la ISO 27001 o el ENS, muéstralo; eso ya te acredita”.

El informe también aborda el impacto de la inteligencia artificial generativa, un terreno aún incierto. Reconociendo que es algo por descubrir, aseguró Javier Carvajal que “no deberíamos justificarnos en la falta de regulación: el reglamento de IA ya existe y exige cumplimiento”. Llamó a las empresas a crear marcos de uso claros antes de que la tecnología se descontrole porque “si dejas que se use sin límites, luego será muy difícil cortar”.

En cuanto a prioridades, las empresas planean reforzar detección, respuesta y recuperación, además de mejorar la cultura de seguridad. “¿De quién es la responsabilidad de mejorar la cultura?”, preguntó el CEO de Icraitas a la audiencia para luego responder: “De todos, pero tiene que motivarlo la dirección. Si no, no funciona”.

Finalmente, Carvajal insistió en que la resiliencia no siempre requiere grandes inversiones, y sí una buena priorización: “Hay que valorar qué nos interesa más: lo urgente o lo que genera más riesgo”.

Cerraba el directivo su intervención con una llamada a la acción: “Es el momento de que el liderazgo asuma la resiliencia como una decisión estratégica. Gobernarla desde el Consejo no sólo fortalece la defensa, sino que garantiza la continuidad, la reputación y la sostenibilidad del negocio”.

Y concluyó con un mensaje a los responsables de ciberseguridad: “Los CISOs tienen que subir a la capa de gestión. Tenemos que ser más visibles, y las normas nos ayudan a ello”.

Ciberresiliencia 360°: Seguridad, Identidad y Continuidad en la Era Digital

La ciberresiliencia se ha consolidado como uno de los grandes indicadores de madurez tecnológica y empresarial. Lo demuestran los debates que está impulsando TAI Editorial a través de sus eventos, donde CISOs y directivos analizan los retos reales de un entorno en el que ya no basta con proteger: hay que resistir, responder y recuperarse.

El encuentro, patrocinado por Check Point, Mastercard, Silverfort y Sophos, reunió a responsables de seguridad de organizaciones públicas y privadas de distintos sectores para abordar, desde la práctica, cómo se construye una resiliencia 360° frente a la complejidad tecnológica, el riesgo de terceros, la identidad digital y la gestión continua de incidentes.

Rosalía Arroyo

Complejidad tecnológica: el enemigo invisible

En el punto de partida del debate, los ponentes coincidieron en un hecho incuestionable: la complejidad tecnológica se ha convertido en uno de los principales obstáculos para la resiliencia. Sistemas heredados, entornos híbridos y una creciente dependencia de proveedores externos dibujan un escenario donde cada capa añade nuevos riesgos.

Carlos Juarros, CISO de FUNDAE, abrió el turno reconociendo que “la fragmentación tecnológica es un problema en sí mismo”, por lo que su estrategia ha pasado por reducir el número de proveedores y optimizar lo existente. “Intentamos que los proveedores se adapten a nosotros, no al revés. Cuantas más piezas, más difícil es mantener la coherencia y evaluar riesgos”, explicó.

> Si la identidad define el perímetro, la capacidad de anticipar define la resiliencia

Coincidió David Moreno, CISO de Tendam, en que la herencia tecnológica es uno de los grandes lastres para la resiliencia. Explicando que su compañúa cuenta con “un legado de sistemas complejo, sobre todo en procesos de negocio”, aseguró que su enfoque pasa por definir los sistemas críticos para la supervivencia básica de la compañía y priorizar los esfuerzos en torno a ellos.

En el sector telco, Alejandro Velilla, CTIO & Cybersecurity de Embou + Orange, puso el acento en la dependencia de terceros al asegurar que en muchos proyectos “trabajamos con plataformas IoT de otros proveedores. Todo puede estar certificado, pero la realidad es que no siempre se tiene el control sobre la custodia de los datos”.

> El concepto de resiliencia digital, impulsado desde la Unión Europea, ha pasado de ser una aspiración a convertirse en una obligación

Los fabricantes coincidieron en que la clave está en simplificar sin perder visibilidad. “La complejidad siempre es enemiga de la seguridad”, subrayó Eusebio Nieva, sales engineer manager Iberia y evangelista de Check Point, quien añadió que, “por eso apostamos por plataformas unificadas, automatización y APIs que permitan reducir el error humano y operar de forma más eficiente”.

Desde Sophos, Iván Mateos, sales engineer, de la compañía, añadió que el reto no es sólo técnico sino organizativo: “Muchas empresas no se dedican a la ciberseguridad, pero la sufren. Necesitan aliados que no sólo vendan tecnología, sino que acompañen en la operación”, aseguró el directivo.

> “Cuantas más piezas, más difícil es mantener la coherencia y evaluar riesgos”
>
> **Carlos Juarros,** CISO, **Fundae**

Terceros y continuidad: cuando el riesgo llega de fuera

En un ecosistema hiperconectado, la cadena de suministro digital es ya una extensión del perímetro corporativo. Los ataques a proveedores o socios se han convertido en una de las principales fuentes de incidentes, lo que obliga a las

"Definir qué sistemas son vitales para sobrevivir es clave para priorizar recursos"

David Moreno del Cerro, CISO, **Tendam**

organizaciones a elevar el control más allá de sus propias fronteras.

José Manuel Rivera, CISO de Iberia Cards, fue directo al asegurar que, por probabilidad, "el ataque vendrá antes de un tercero que de dentro". En su caso, la respuesta ha sido construir un registro de partners críticos y realizar evalua-

ciones de madurez "no tanto para excluir, sino para buscar soluciones conjuntas que permitan seguir trabajando con seguridad".

Desde Informa D&B, David Cerrato, CISO de la compañía, subrayó la importancia del marco contractual y de las revisiones técnicas reales; "la parte de compliance ayuda, pero sin revisión técnica no hay garantías", aseguró.

Los patrocinadores coincidieron en la necesidad de convertir la visibilidad en acción. Explicó Alberto López, VP de Cyber & Intelligence Solutions Product Lead en Mastercard, que su compañía ha invertido más de 11.000 millones de dólares en soluciones de ciberseguridad e inteligencia pre-

"La complejidad no está solo en la tecnología, sino en la dependencia de terceros"

Alejandro Velilla, CTIO&Cybersecurity, **Embou +Orange**

cisamente para proteger un ecosistema donde interactúan 22.000 bancos. "La mejor forma de proteger el ecosistema es anticiparse. Por eso apostamos por la monitorización continua y la ciberinteligencia aplicada a terceros, como hace nuestra herramienta RiskRecon", comentó.

Por su parte, Javier Gómez, regional sales ma-

> “Prefiero invertir en detectar y responder rápido que en prevenir lo inevitable”
>
> **Félix Rodríguez,** CISO, **Triodos Bank**

nager de Silverfort, centró el discurso en la protección de identidades externas: “Podemos extender el doble factor a cualquier sistema, incluso a consolas de comandos. Se trata de establecer perímetros de autenticación y aplicar el mínimo privilegio también a proveedores y usuarios externos”, explicó.

La identidad, nuevo perímetro de seguridad

A medida que los entornos híbridos y la nube diluyen los límites tradicionales, la identidad se ha convertido en el auténtico perímetro de defensa. Si antes la seguridad se construía alrededor del perímetro físico o de la red, hoy todo gira en torno a quién accede, desde dónde y con qué legitimidad. La gestión de identidades, privilegios y comportamientos se ha transformado en un factor estratégico para mantener la continuidad operativa.

Félix Rodríguez, CISO de Triodos Bank, fue uno de los primeros en subrayarlo al asegurar que “todo acceso debe ser autenticado, autorizado y registrado”. En una entidad que combina entornos cloud, on-premise y APIs abiertas, aplicar esa regla de oro implica coordinar controles, centralizar accesos y desplegar herra-

"La seguridad total es una utopía; trabajamos para contener, no para idealizar"

Guillermo (Willy) Obispo,
Jefe Servicio Ciberseguridad, **IAM/Ayuntamiento de Madrid**

mientas de Identity and Access Management (IAM) capaces de ofrecer visibilidad transversal. "No siempre es posible aplicar multifactor a todo", reconoció, "pero la confianza cero nos obliga a controlar y monitorizar incluso los accesos legítimos".

Diego Durantes, CISO de Stratio BD, añadió un

La cadena de suministro digital es ya una extensión del perímetro corporativo

matiz cada vez más relevante: la inteligencia artificial como elemento de apoyo y riesgo a la vez. En su organización, la IA generativa se utiliza para gestionar la exposición de datos y para automatizar tareas, pero bajo una política clara de control. "Tenemos IA on-premise y en la nube; lo importante es que las personas estén concienciadas y formadas sobre cómo usarla y cómo acceder a ella", explicó. La gestión de identidades en Stratio DB incluye procesos de doble validación y flujos de aprobación para cada tipo de acceso, integrando la seguridad en el propio ciclo de uso de la IA.

La conversación dio paso al análisis de un tema más técnico: las cuentas no humanas o de servicio, que se han convertido en uno de los puntos ciegos más peligrosos dentro de las organizaciones.

"La diversificación de centros y proveedores nos ayuda a resistir mejor los incidentes"

Alejandro Expósito,
CIO/COO/CISO, **Servatrix Biomédica**

Javier Gómez explicó que "muchas empresas no saben ni cuántas cuentas de servicio tienen ni dónde operan". Silverfort propone un enfoque basado en visibilidad y contención: "Si no puedes rotar contraseñas sin romper procesos críticos, necesitas perimetrar y monitorizar comportamientos. La identidad, hu-

> “Cada permiso y cada dato deben pasar por un control: la automatización también debe auditarse”
>
> **Diego Durantes,** CISO, **STRATIO BD**

mana o no, debe estar bajo el mismo marco de control”.

Desde Sophos, Iván Mateos advirtió del riesgo de la complacencia tecnológica. “Hay clientes que siguen usando el mismo antivirus desde 2009”, comentó con ironía. Pero detrás del comentario hay un mensaje claro: la resiliencia

exige revisión continua y autocrítica. “Ser crítico con tus propias soluciones es el primer paso hacia la resiliencia”, insistió. También recordó que muchos incidentes parten de pequeños descuidos, como compartir dispositivos de autenticación o no revisar comportamientos anómalos. “El mejor malware es el que no hace ruido; lo peligroso es lo que no ves”, remató.

En conjunto, la identidad emergió como eje central de la ciberresiliencia: un punto de convergencia entre control técnico, cultura de uso y estrategia corporativa. Sin una gestión madura de identidades, el resto de capas —desde la red hasta el dato— pierden sentido.

> “Leerse el Esquema Nacional de Seguridad y aplicarlo con rigor da más resultados de los que parece”
>
> **Enrique Cervantes,** director Seguridad e Infraestructura Tecnológica, **CESCE**

Prevención, detección o anticipación: el nuevo equilibrio

Si la identidad define el perímetro, la capacidad de anticipar define la resiliencia. La siguiente pregunta que lanzó el moderador abrió un de-

> “La clave está en el compromiso de la dirección y en mantener viva la cultura de seguridad”
>
> **Luis Samper,**
> Jefe de Ciberseguridad, **Casa Real**

bate clásico pero esencial: ¿es más importante prevenir, detectar o anticiparse? Las respuestas reflejaron tanto las diferencias sectoriales como el nivel de madurez de cada organización.

Manuel Asenjo, CIO/CISO de Écija Abogados, defendió con convicción que la prevención sigue siendo la base de todo. “Podemos desplegar todas las herramientas del mundo, pero si el usuario se salta las normas, la brecha llega igual. La educación es la mejor barrera”, afirmó. En su opinión, formar al personal para identificar riesgos cotidianos tiene más impacto que cualquier inversión tecnológica.

Desde el ámbito financiero, Félix Rodríguez adoptó una visión complementaria. “Si tuviera 50 euros, pondría 40 en detectar y 10 en prevenir”, bromeó, aunque con un trasfondo serio. Para él, en un entorno con amenazas constantes y sistemas distribuidos, la detección temprana es la línea que separa una crisis controlada de una catástrofe. Por eso, en Triodos realizan simulacros periódicos de ransomware y de uso indebido de credenciales, no sólo para probar la tecnología, sino para entrenar la respuesta humana.

"Podemos tener todas las herramientas, pero sin conciencia, la brecha siempre llega"

Manuel Asenjo,
CIO/CISO, **Ecija Abogados**

David Cerrato y Alejandro Velilla coincidieron en una idea pragmática: "Entrar, entrarán", dijo este último. "El reto no es evitarlo, sino responder rápido y bien". Ambos defendieron que la inversión debe centrarse en reforzar la capacidad de recuperación y en reducir el tiempo de detección.

El concepto "nunca confíes, verifica siempre" ha pasado de eslogan a necesidad, pero llevarlo al terreno operativo exige estrategia

En el lado más humano del debate, Carlos Juarros compartió una anécdota que ilustró la filosofía preventiva: "Un amigo cirujano me dijo una vez: 'Yo no quiero curar, quiero prevenir'. En ciberseguridad debería ser igual".

El cierre del bloque trajo consenso. Alberto López sintetizó la nueva mentalidad: "No se trata solo de prevenir, sino de anticiparse. La ciberinteligencia es la diferencia entre reaccionar y adelantarse". Y Eusebio Nieva lo completó con un apunte técnico: "Con IA, los tiempos de detección se reducen de días a horas. Necesitamos que la prevención y la respuesta evolucionen al mismo ritmo que los atacantes".

"Sin revisión técnica no hay garantías; el papel por sí solo no protege nada"

David Cerrato,
CISO, **Informa DB**

La conclusión fue clara: la resiliencia moderna no elige entre prevenir o detectar; combina ambas con inteligencia y agilidad.

Zero Trust en entornos híbridos: del ideal a la práctica

En la última parte, el debate se centró en la im-

"Con IA, la prevención y la respuesta deben avanzar al mismo ritmo que los atacantes"

Eusebio Nieva,
Sales Engineering Manager Iberia, Evangelist,
Check Point Software

plementación real del modelo Zero Trust, una aspiración compartida por todos, pero que choca con la complejidad de los entornos heredados. El concepto —"nunca confíes, verifica siempre"— ha pasado de eslogan a necesidad, pero llevarlo al terreno operativo exige estrategia, segmentación y mucha paciencia.

David Moreno resumió su aproximación con una palabra: "segmentación". En su compañía, los sistemas más antiguos o incompatibles con Zero Trust se aíslan mediante políticas de red específicas, limitando su exposición. "A veces la mejor forma de proteger es no mezclar", señaló.

Alejandro Expósito, CIO/COO/CISO de Servatrix Biomédica, ofreció una visión inversa: la de quien debe conectarse a plataformas externas, como las de inteligencia artificial, bajo auditorías muy exigentes. "Para usar servicios públicos de IA tienes que pasar revisiones de seguridad que te gustaría tener en tu propia infraestructu-

"Ser crítico con tus propias soluciones es el primer paso hacia la resiliencia"

Ivan Mateos,
Sales Engineer, **Sophos**

ra", admitió con humor. Esa exigencia externa, reconoció, les ha servido para elevar su propio nivel de cumplimiento.

El testimonio de Guillermo Obispo, Jefe Servicio Ciberseguridad, IAM/Ayuntamiento de Madrid, aportó la mirada institucional: "En una organización con 30.000 equipos, la perfección no exis-

"La ciberinteligencia es la diferencia entre reaccionar y anticiparse"

Alberto López,
VP de Cyber & Intelligence Solutions Product Lead en, **Mastercard Europa**

te. Apostamos por segmentación y contención. La seguridad total es una utopía". Su intervención reflejó la realidad de las administraciones públicas, donde la coexistencia de tecnologías antiguas y modernas obliga a priorizar la visibilidad y el control más que la pureza conceptual del modelo.

Desde el lado de los fabricantes, Eusebio Nieva

El debate dejó clara una idea compartida por todos: Zero Trust no es un proyecto, sino un proceso

recordó que el verdadero reto es mantener una política de control coherente entre la nube y el entorno on-premise. "Si no lo ves, no lo puedes controlar, y si no lo controlas, no tienes seguridad", resumió.

Javier Gómez completó el argumento desde la capa de identidad: "Podemos extender el doble factor incluso a sistemas heredados. Es una forma de aplicar los principios de confianza cero sin necesidad de sustituirlo todo".

El bloque cerró con una idea compartida por todos: Zero Trust no es un proyecto, sino un proceso. Requiere equilibrio entre lo ideal y lo posible, y sobre todo, continuidad.

La ciberresiliencia, en definitiva, ya no es un destino, sino una forma de gestión continua. Las organizaciones que participaron en el Observatorio lo demostraron con una conclusión

"Proteger las cuentas de servicio es tan crítico como proteger a los usuarios humanos"

Javier Gómez,
Regional Sales Manager Iberia, **Silverfort**

compartida: no se trata de tener más tecnología, sino de construir cultura, visibilidad y capacidad de adaptación.

Como señaló uno de los ponentes, "no hay prevención perfecta, pero sí anticipación inteligente". Y esa es, quizá, la mejor definición posible de la resiliencia en 2025.


SOPHOS
Neutralize cyber threats, 24/7.
Stop breaches before they happen with Sophos Managed Detection and Response.
SOPHOS.COM


SALIDA