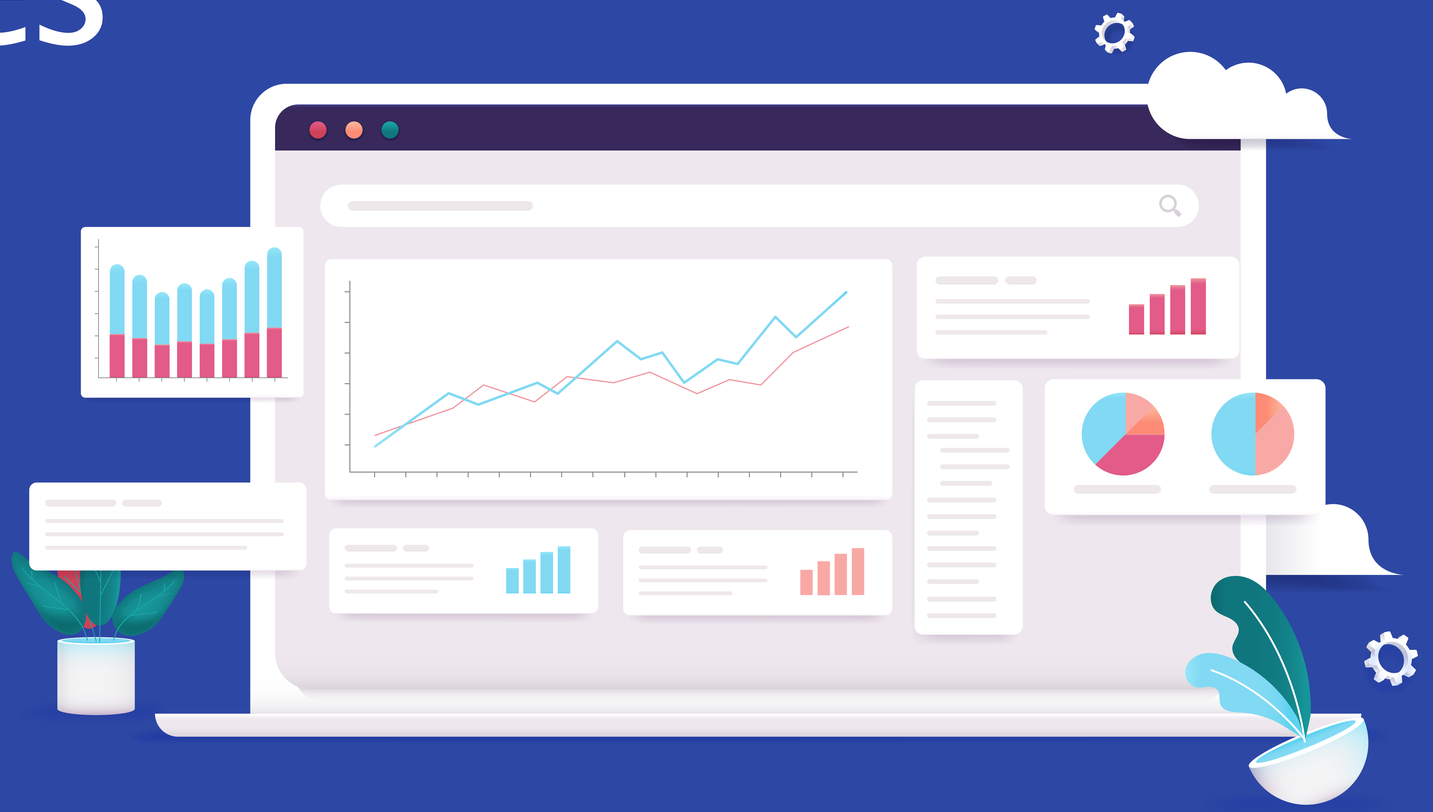
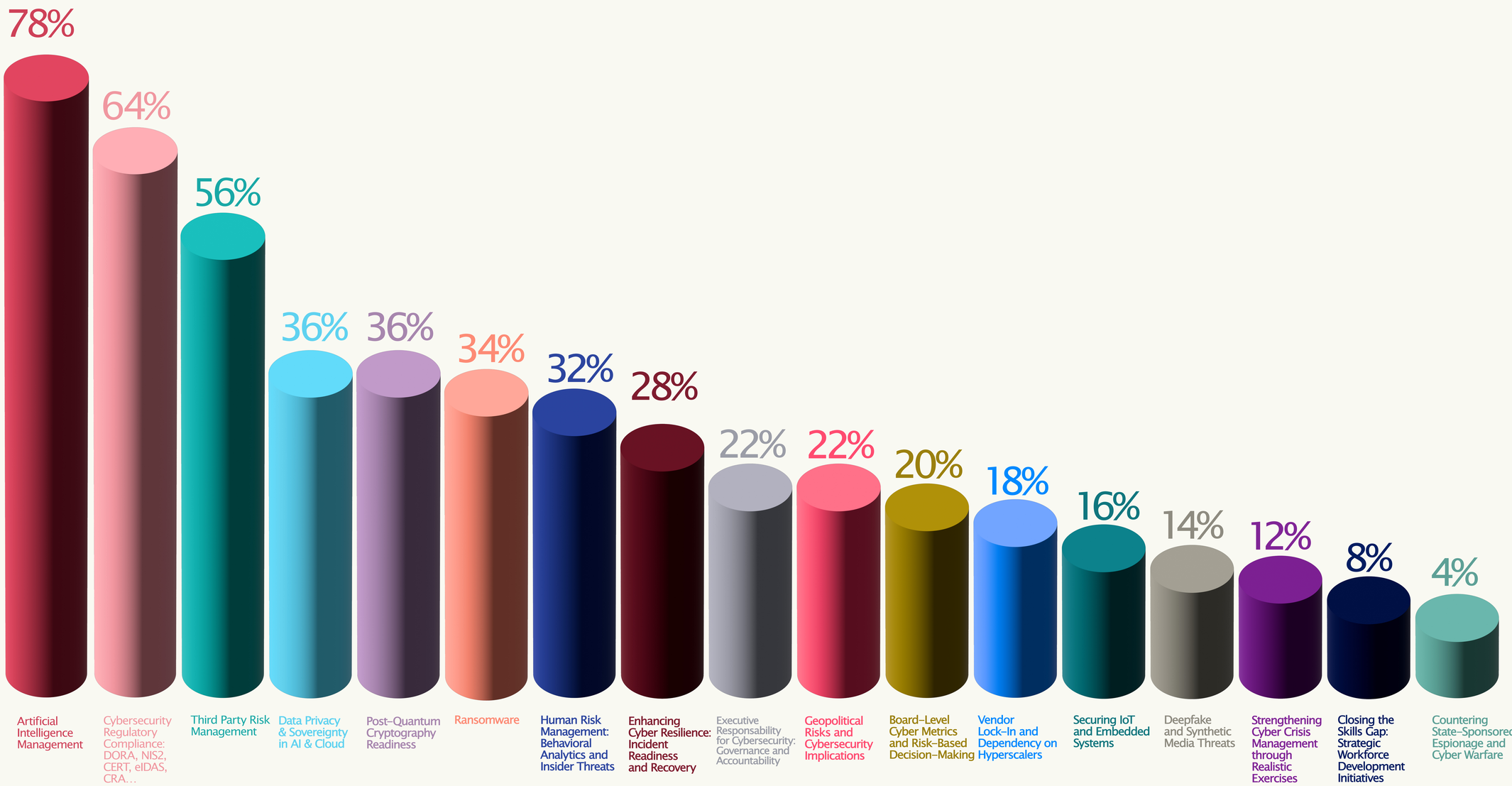
Cyber Security and Data Protection Challenges 26'



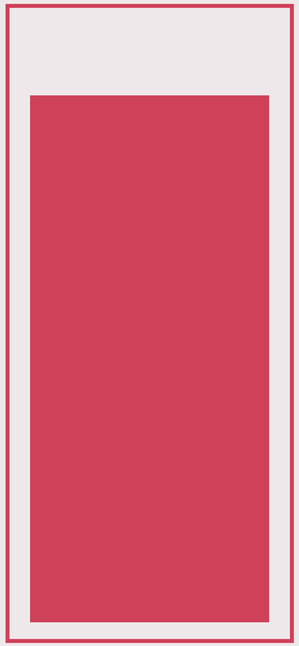

78%
Artificial Intelligence Management
64%
Cybersecurity Regulatory Compliance: DORA, NIS2, CERT, eIDAS, CRA…
56%
Third Party Risk Management
36%
Data Privacy & Sovereignty in AI & Cloud
36%
Post–Quantum Cryptography Readiness
34%
Ransomware
32%
Human Risk Management: Behavioral Analytics and Insider Threats
28%
Enhancing Cyber Resilience: Incident Readiness and Recovery
22%
Executive Responsability for Cybersecurity: Governance and Accountability
22%
Geopolitical Risks and Cybersecurity Implications
20%
Board–Level Cyber Metrics and Risk–Based Decision–Making
18%
Vendor Lock–In and Dependency on Hyperscalers
16%
Securing IoT and Embedded Systems
14%
Deepfake and Synthetic Media Threats
12%
Strengthening Cyber Crisis Management through Realistic Exercises
8%
Closing the Skills Gap: Strategic Workforce Development Initiatives
4%
Countering State–Sponsored Espionage and Cyber Warfare

Cybersecurity & Data Protection Challenges 2026

El año 2026 comienza con un panorama de ciberseguridad marcado por la aceleración tecnológica y la presión regulatoria.

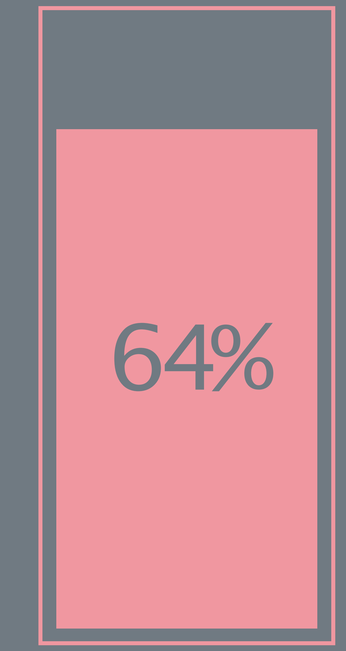
Las respuestas de los CISOs españoles reflejan una clara evolución respecto a años anteriores: la prioridad ya no se limita a contener amenazas tradicionales, sino a anticipar riesgos derivados de la innovación y la hiperconectividad.

La gestión de la inteligencia artificial **se sitúa en primer lugar, con un 78% de los encuestados considerándola el desafío más crítico.** No es casualidad, la IA se ha convertido en el motor de la transformación digital, pero también en una fuente de vulnerabilidades inéditas. Los CISOs son conscientes de que los modelos generativos pueden filtrar información sensible, amplificar sesgos y ser utilizados para ataques sofisticados. Además, la AI Act europea obliga a establecer controles sobre algoritmos y transparencia, lo que convierte la gobernanza de la IA en una prioridad estratégica.



78%

Artificial Intelligence Management

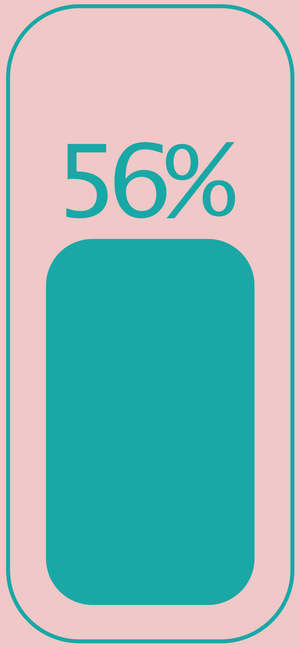


64%

Cybersecurity Regulatory Compliance: DORA, NIS2, CERT, eIDAS, CRA…

En segundo lugar, con un 64%, aparece el cumplimiento normativo en ciberseguridad. Normativas como DORA, NIS2, CERT, eIDAS y CRA están redefiniendo las reglas del juego. Las organizaciones ya no pueden limitarse a cumplir de forma reactiva; deben integrar la regulación en su ADN operativo. El impacto es directo: sanciones elevadas, pérdida de confianza y exigencia de métricas claras en los consejos de administración. La ciberseguridad se consolida como un factor de competitividad.

La gestión del riesgo de terceros, con un 56%, sigue siendo un pilar fundamental. En un ecosistema interconectado, la seguridad de la cadena de suministro es tan crítica como la propia infraestructura interna. Los ataques a proveedores estratégicos han demostrado que vulnerar un eslabón puede comprometer a cientos de organizaciones. Por ello, los CISOs demandan auditorías continuas y controles robustos para mitigar este riesgo.



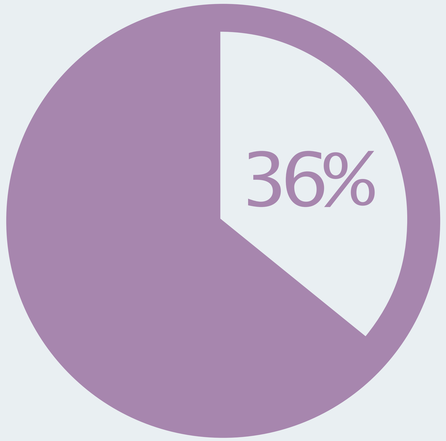
Third Party Risk Management

Data Privacy & Sovereignty in AI & Cloud

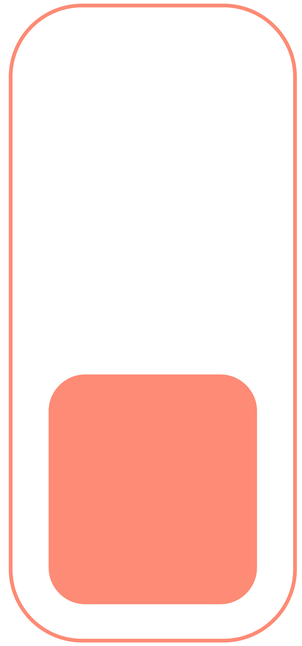
36%

Otro aspecto que gana relevancia es la privacidad y soberanía de datos en entornos de IA y Cloud, con un 36%. La combinación de inteligencia artificial y nube plantea retos sobre dónde se almacenan y procesan los datos, y cómo garantizar su confidencialidad. Las regulaciones de soberanía digital y la presión por mantener la confianza del cliente obligan a diseñar arquitecturas seguras y transparentes.

En paralelo, la preparación para la criptografía post-cuántica también alcanza un 36%. Aunque la computación cuántica aún no es una amenaza inmediata, los CISOs saben que el riesgo de “harvest now, decrypt later” es real. Los datos cifrados hoy pueden ser descifrados en el futuro. Migrar hacia algoritmos resistentes no es una tarea sencilla, pero la planificación anticipada es clave para evitar vulnerabilidades críticas.



Post–Quantum Cryptography Readiness



34%

Ransomware

Finalmente, el ransomware, con un 34%, sigue presente en la agenda. Aunque pierde peso frente a desafíos emergentes, continúa siendo una amenaza persistente que paraliza operaciones y genera pérdidas millonarias. Los CISOs lo saben: la resiliencia ante incidentes y la capacidad de recuperación son imprescindibles para garantizar la continuidad del negocio.

La gestión del riesgo humano, con un 32%, se posiciona como un desafío estratégico que no puede ignorarse. Las organizaciones reconocen que los incidentes no siempre provienen de actores externos; los comportamientos negligentes o malintencionados dentro de la empresa representan una amenaza latente. La aplicación de analítica conductual permite identificar patrones anómalos y anticipar posibles fugas de información o sabotajes. En este contexto, la combinación de tecnología y cultura corporativa es esencial: programas de concienciación, controles de acceso dinámicos y sistemas de monitorización avanzada son pilares para mitigar el riesgo interno sin comprometer la productividad.

Human Risk Management: Behavioral Analytics and Insider Threats

En definitiva, las respuestas de los CISOs revelan una tendencia clara: la ciberseguridad deja de ser reactiva para convertirse en un pilar estratégico. La gestión de la inteligencia artificial y la preparación para la era post-cuántica marcan el futuro, mientras que la regulación y la protección de la cadena de suministro consolidan la base sobre la que se construirá la confianza digital en 2026.

isms forum

Cyber Security and Data Protection Challenges 26’