Estudio de mercado

La voz de los CISOs españoles

Ciberseguridad extendida: del control a la resiliencia

eraneos

Enero 2026

Prólogo

Eduvigis Ortiz
Cybersecurity Head Iberia
eduvigis.ortiz@eraneos.com

Contexto y tendencias globales que condicionan la ciberseguridad en 2026

Desde el punto de vista de Eraneos, el entorno de amenaza combina tres aceleradores que se retroalimentan para generar más riesgos para las organizaciones en el corto y medio plazo:

1. La industrialización del cibercrimen y la extorsión.

2. La centralidad de la identidad como vector de entrada dominante (phishing, robo y reutilización de credenciales).

3. La dependencia de ecosistemas y cadenas de suministro digitales cada vez más complejas.

Los principales informes internacionales coinciden en que la resiliencia y el control de riesgos de terceros están pasando a ser focos centrales de la agenda de los CISOs, en paralelo a la adopción masiva de la IA generativa por atacantes y defensores.

Implicaciones para los CISOs

- Elevar el gobierno de ciberseguridad al comité ejecutivo y al consejo, con métricas orientadas a continuidad, impacto y riesgo residual.
- Reducir exposición y complejidad: consolidar, integrar y automatizar; priorizar capacidades que cierren brechas operativas reales.
- Gestionar a los proveedores como un programa continuo (no como un proceso de compra): evaluación, contratos, integración, monitorización y planes de salida.
- Preparar la transición a criptografía post-cuántica mediante agilidad criptográfica, inventario criptográfico y planificación por criticidad.

Índice

Análisis estratégico y sourcing de ciberseguridad 2026

1. Resumen ejecutivo

Los resultados de este documento recogen las principales prioridades y reflexiones de los CISOs de grandes compañías españolas durante su participación en el primer Eraneos Cybersecurity Summit. Dichas conclusiones se canalizaron a través de una encuesta sobre el estado de la ciberseguridad en sus organizaciones. El análisis revela un alto grado de madurez estratégica y una gestión cada vez más compleja de la ciberdefensa, caracterizada por el uso de modelos híbridos y la colaboración con múltiples proveedores especializados. De estas respuestas se han extraído las siguientes conclusiones:

- Los CISOs españoles participantes en el informe muestran una alta madurez estratégica: la ciberseguridad se gobierna como un riesgo de negocio y cuenta, en la mayoría de los casos, con aprobación explícita de la alta dirección.

- El riesgo de terceros emerge como la principal preocupación: la dependencia de múltiples proveedores incrementa la complejidad operativa, la superficie de ataque y la exposición a fallos de control en la cadena de suministro.

- El presupuesto de 2026 se orienta a proyectos de gestión de identidades (IAM/PAM) y a la consolidación/optimización de capacidades existentes, más que a una proliferación de herramientas. Se prioriza la eficiencia y la reducción de la complejidad.

- La IA se percibe como una palanca para escalar la defensa y optimizar las operaciones (automatización), mientras crecen los riesgos de ingeniería social avanzada (deepfakes / ultrafalsos) y de abuso de credenciales robadas. El foco se desplaza de “evitar el ataque” a “recuperarse antes y mejor”.

- El cumplimiento normativo evoluciona hacia la resiliencia operativa y continuidad de negocio (NIS2 y DORA). La privacidad se considera interiorizada, la exigencia del día a día es demostrar la preparación, la gestión de crisis y la capacidad de recuperación de la organización frente a ciberataques.

2. Contexto y metodología de la encuesta

El informe se basa en una muestra de más de 30 CISOs de grandes compañías españolas, pertenecientes a diversos sectores y con diferentes tamaños, que participaron en el primer Eraneos Cybersecurity Summit, celebrado a finales de 2025.

Estos CISOs son profesionales con una amplia experiencia en el ámbito de la ciberseguridad, lo que aporta un elevado nivel de criterio a las perspectivas recogidas sobre el futuro del sector.

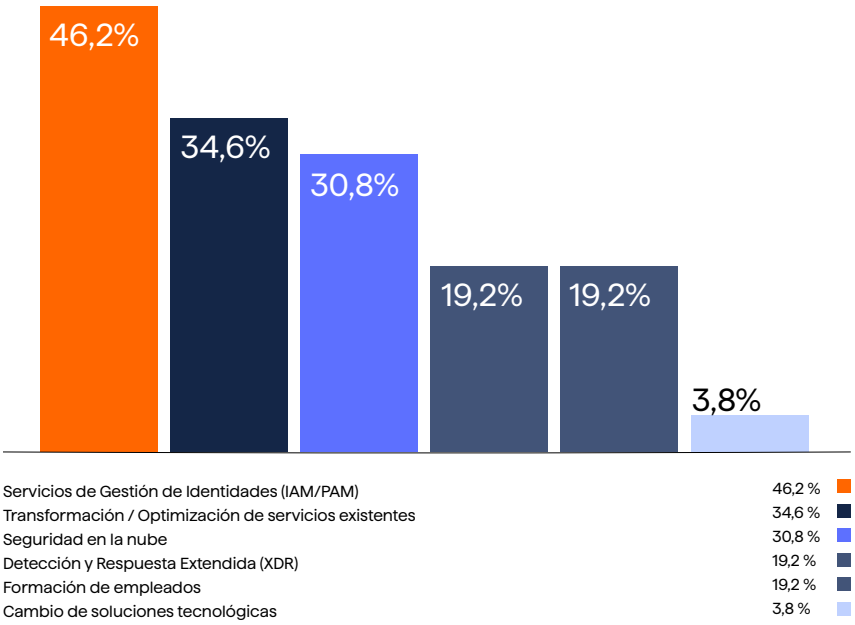
Las conclusiones del informe reflejan así la visión y las prioridades de los principales responsables de ciberseguridad en organizaciones de referencia, las cuales gestionan entornos tecnológicos complejos y dependen de cadenas de suministro muy variadas, desde proveedores altamente especializados hasta otros menos sofisticados.

Esta diversidad sectorial y de perfiles garantiza que los resultados de la encuesta sean especialmente relevantes para comprender las principales tendencias y desafíos compartidos en la gestión de la ciberseguridad en España.

3. Agenda del CISO para 2026: prioridades de inversión

Aquí exploramos cómo priorizan los CISOs la asignación de presupuesto cuando existe margen adicional de inversión. Más allá de los presupuestos recurrentes, este escenario permite identificar qué capacidades se consideran más críticas para reducir exposición al riesgo, mejorar la resiliencia y acelerar la madurez de la ciberseguridad en la organización. Las respuestas ofrecen una fotografía clara de las áreas donde se percibe mayor brecha o mayor retorno en términos de protección y continuidad, y ayudan a entender hacia dónde se orienta el mercado cuando la decisión es “dónde reforzar primero”.

Si tuvieras que destinar una inversión extra significativa en ciberseguridad este año, ¿cuáles de las siguientes áreas requieren una mayor inversión en tu compañía? Selecciona hasta dos respuestas.



El foco principal es quién accede, identidad como prioridad (46,2%). La inversión se concentra en IAM/PAM para implementar estrategias de Zero Trust y frenar el robo de credenciales.

No se busca comprar herramientas nuevas, sino optimizar las existentes. Hay una clara fatiga tecnológica; el CISO prefiere que lo que ya tiene funcione mejor. Eficiencia sobre Novedad (34,6% vs. 3,8%).

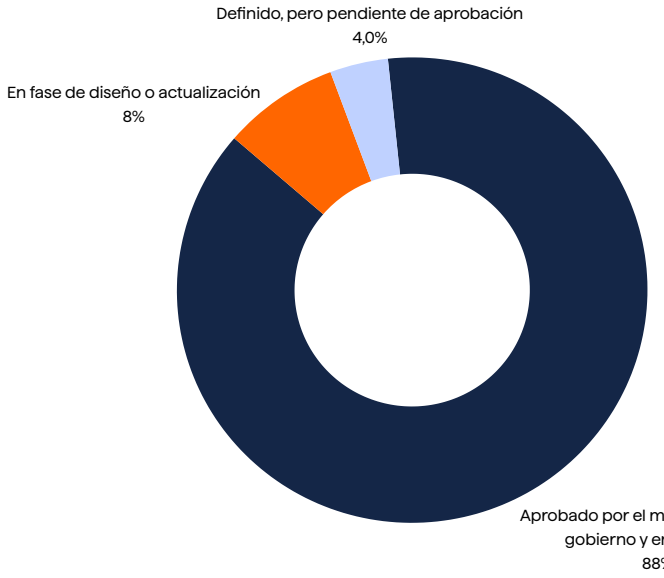
La seguridad en la nube sigue siendo una inversión estructural necesaria, mientras que la detección (XDR) se mantiene como un pilar de mantenimiento, pero no de crecimiento crítico.

En definitiva, el presupuesto de 2026 es pragmático. Se invierte en el control de accesos y en la consolidación de lo que ya se tiene para reducir la complejidad operativa.

4. Madurez de la ciberseguridad en organizaciones españolas

Se refleja en la encuesta una alta madurez en estrategia de ciberseguridad de las empresas participantes. Así como también la gestión de muchos planes e iniciativas en curso, con la continua actualización y revisión de estos para ir acomodando y adaptando la legislación que va llegando, los riesgos que surgen, y adoptando la innovación tecnológica.

¿En qué situación se encuentra el plan director/estrategia de ciberseguridad de tu organización?

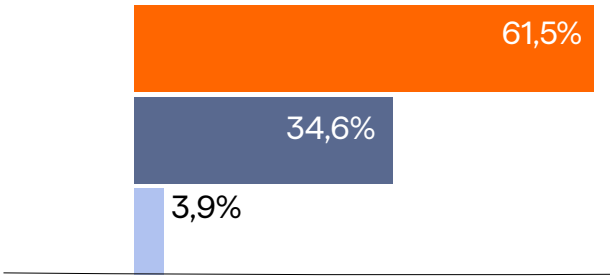


Aprobado por el máximo órgano de gobierno y en ejecución	88,0 %
En fase de diseño o actualización	8,0 %
Definido, pero pendiente de aprobación	4,0 %
Solo existen iniciativas aisladas sin plan director formal	0 %
No disponemos de un plan director o estrategia formal de ciberseguridad	0 %

5. Modelo operativo: internalización vs. externalización (sourcing)

Gestionar terceros se ha convertido en uno de los mayores desafíos para los CISOs: una gran parte opera con un modelo híbrido y con más de seis proveedores de ciberseguridad, lo que eleva la complejidad y hace aflorar nuevos riesgos en la cadena de suministro. Por esto es tan importante seleccionar bien a los proveedores y establecer un gobierno continuo. Para alcanzar los objetivos de ciberseguridad es crítico el acompañamiento experto e independiente para asegurar que los contratos y servicios prestados por terceros protejan la operación y mejoren la resiliencia de la organización.

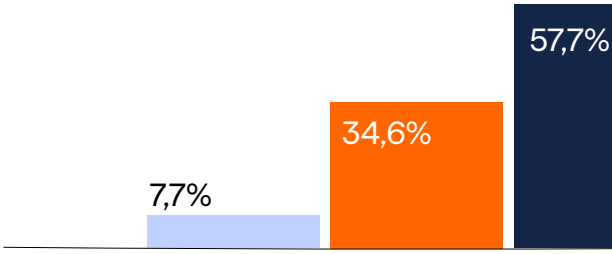
¿La gestión de la ciberseguridad la realiza un equipo interno dedicado o se han contratado servicios externos?



Modelo híbrido	61,5 %
La realiza un equipo interno dedicado	34,6 %
Se han contratado servicios externos	3,9 %

Una de las reflexiones comentadas en el evento fue internalizar las funciones más estratégicas y externalizar aquellas que requieren más especialización, aunque esta decisión puede variar en función del sector y de los recursos internos. Una conclusión que fue ampliamente respaldada durante el evento es la recomendación de **“Solo externalizar procesos que ya se encuentran maduros internamente en la organización”** ya que, de lo contrario, el servicio sería muy complejo de gobernar y aumentaríamos la dependencia del conocimiento en nuestro proveedor.

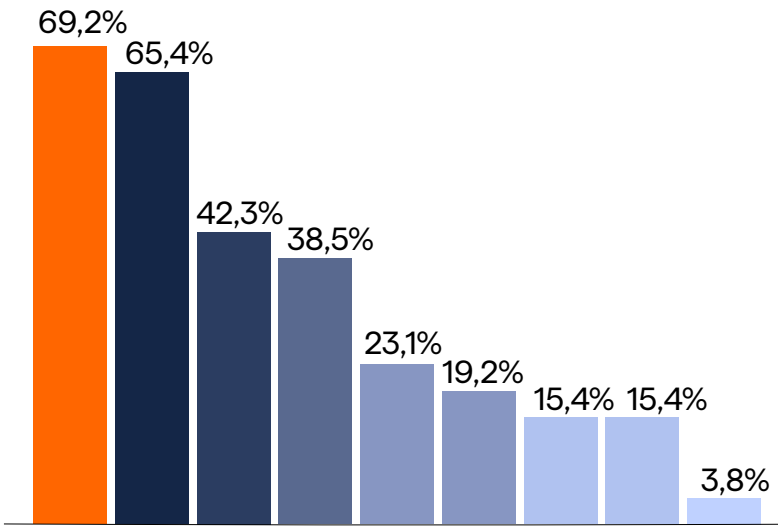
¿Cuántos proveedores de ciberseguridad gestionáis actualmente? (aproximadamente)



1-3	7,7 %
4-6	34,6 %
Más de 6	57,7 %

En el primer **Cybersecurity Summit de Eraneos** quedó claro que el coste dejó de ser el principal factor decisivo al seleccionar a un proveedor. Con funciones cada vez más críticas en juego y el nivel de especialización requerido por los CISOs, ahora es prioritario que el proveedor cuente con un alto nivel de madurez en el servicio, así como excelentes referencias, reputación y capacidad técnica en el equipo contratado.

¿Qué factores pesan más en la selección de un proveedor de ciberseguridad? Selecciona hasta tres respuestas.

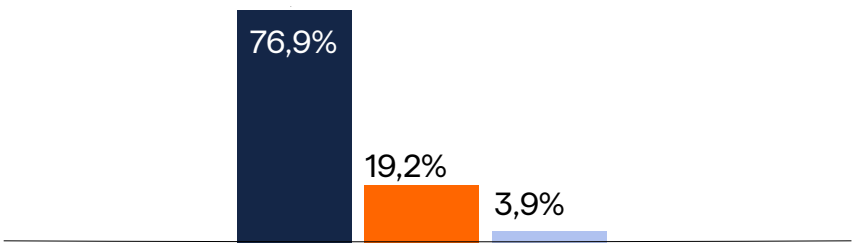


Reputación y referencias	69,2%
Capacidad técnica	65,4%
Nivel de talento y especialización	42,3%
Coste	38,5%
Cumplimiento normativo (NIS2, ENS, ISO. 27001, etc.)	23,1%
Enfoque innovador / usos de IA	19,2%
Capacidad de integración con sistemas existentes	15,4%
Capacidad de respuesta ante incidentes	15,4%
Cercanía y soporte local	3,8%

6. Riesgo de terceros y cadena de suministro

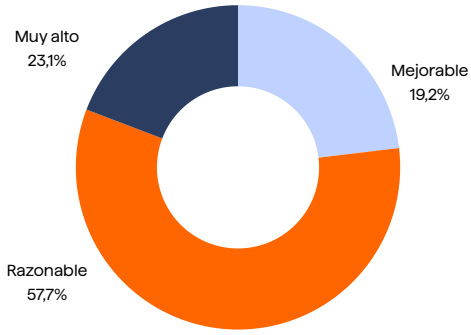
A pesar de que muchos servicios son externalizados, solo el 23,1% de los CISOs confían en un nivel “muy alto” en sus proveedores de ciberseguridad.

¿Cómo medís el desempeño de vuestros proveedores actuales?



KPIs técnicos y/o niveles de servicio acordados: 76,9%	76,9%
Auditorías periódicas: 19,2%	19,2%
No hay un sistema formalizado	3,9%
Evaluación cualitativa (satisfacción interna)	0,0%

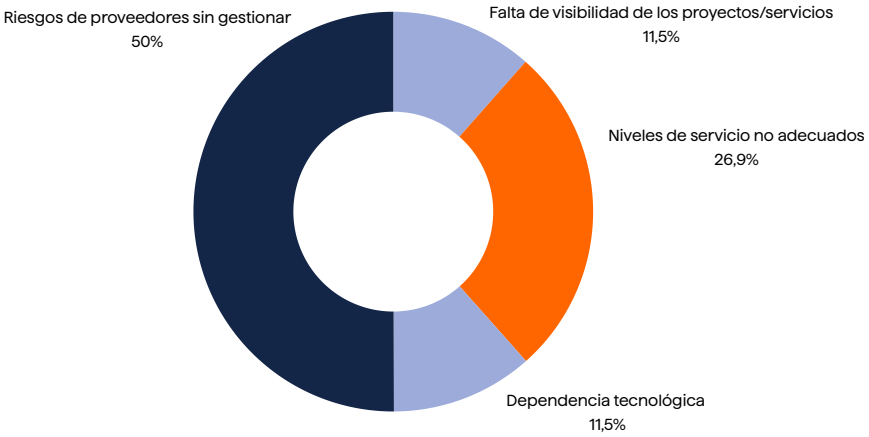
¿Cómo describirías el nivel de confianza actual en tus proveedores de ciberseguridad?



Muy alto	23,1%
Razonable	57,7%
Mejorable	19,2%

Además, la principal preocupación radica en los riesgos de proveedores sin gestionar. Este desafío va más allá de una simple contratación de un servicio, ya que exige un gobierno continuo. La complejidad aumenta a medida que crece el número de proveedores y, con ello, las exigencias regulatorias derivadas del cumplimiento de NIS2, DORA o las normativas que sean relevantes para el contexto sectorial. Aunque los CISOs suelen seleccionar a sus proveedores por su reputación y capacidades técnicas, esto no garantiza una integración eficaz ni una operación óptima alineada con la estrategia del negocio.

¿Cuál consideras el principal riesgo de depender de terceros en ciberseguridad?



Riesgos de proveedores sin gestionar	50 %
Niveles de servicio no adecuados	26,9%
Falta de visibilidad de los proyectos/servicios	11,5%
Dependencia tecnológica	11,5%

7. IA y automatización: de capacidad a ventaja operativa

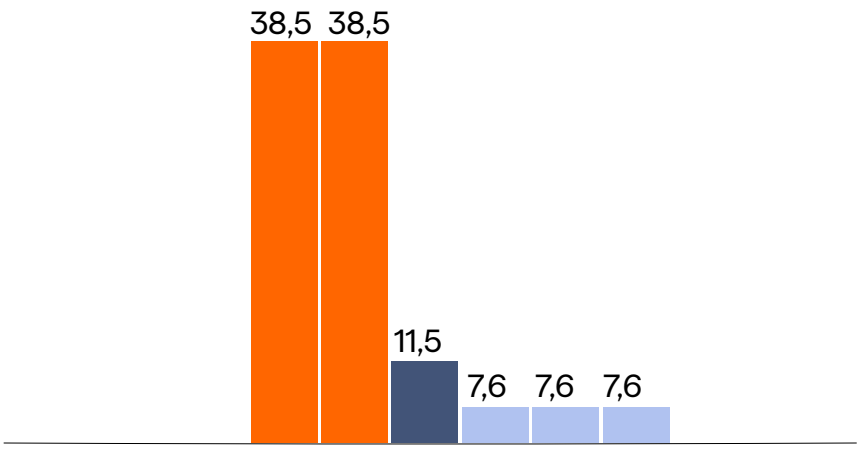
Los CISOs dan una prioridad significativa a la automatización (73,1%). La IA ya no es opcional, es percibida como la única forma de combatir ataques de última generación y suplir la falta de personal. Es la herramienta principal para escalar sus defensas.

Por otro lado, hay un cambio de mentalidad: el foco se desplaza de “evitar el ataque“ a “saber recuperarse“. Preocupa tanto la respuesta ante crisis propias como la seguridad de los proveedores (cadena de suministro).

Los sistemas de monitorización y detección se consideran un espacio menos prioritario. No porque no sean importantes, sino porque se toman en cuenta capacidades básicas ya instaladas, la inversión ahora busca capas de inteligencia más complejas e incluso plataformas que se retroalimenten entre sí.

En definitiva, en 2026 se priorizan la eficiencia operativa mediante IA y la capacidad de recuperación por encima de la protección de datos pura o la detección tradicional.

¿Cuál es vuestro mayor desafío regulatorio en ciberseguridad actualmente?



La Resiliencia Operativa (77%), NIS2 y DORA son los grandes retos. Los CISOs están volcados en cumplir con los nuevos estándares de continuidad de negocio y gestión de crisis que exige Europa.

La privacidad pasa a un segundo plano (11,5%), el RGPD ya no es un desafío; es una norma interiorizada y madura. El foco ha pasado de “proteger el dato“ a “garantizar que el servicio no caiga“ primando la disponibilidad.

Lo emergente aún no presiona, la regulación sobre IA o computación cuántica todavía se percibe como algo lejano o secundario frente a la urgencia de las normativas de infraestructuras críticas.

En definitiva, el cumplimiento en 2026 es estratégico y operativo, no meramente legal. La prioridad es evitar sanciones por falta de resiliencia ante ataques que paralicen la actividad.

8. Principales retos para mejorar la ciberseguridad en las organizaciones encuestadas

Los CISOs consideran que los principales retos están asociados a la IA, la gestión de riesgos, especialmente con terceros y la resiliencia.

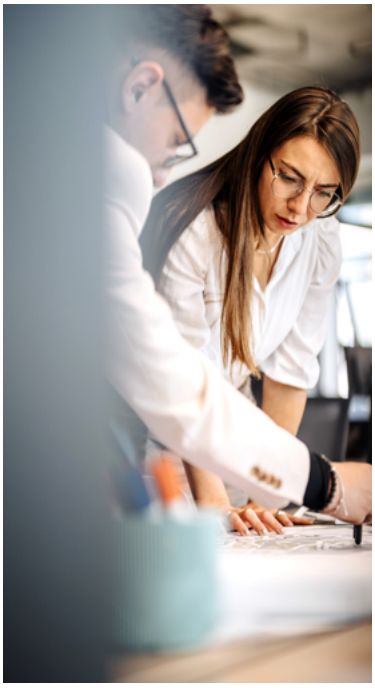
En la encuesta indican que es necesario priorizar la gestión de riesgos implicando a la alta dirección y fomentando una cultura donde nadie se salte los controles. También mencionan la importancia de elevar el discurso para ganar madurez y resiliencia para responder a la complejidad y a la velocidad de cambio.

Otros retos relevantes son: el refuerzo de capacidades con más presupuesto, recursos técnicos y talento; automatizar e integrar la operación (incluida OT), optimizar procesos conocidos por todas las áreas y asegurar las tecnologías emergentes (LLMs y plataformas de IA), la prevención de fuga de información y el riesgo de proveedores y cadena de suministro.

9. Ciberseguridad y alta dirección: el diálogo CEO–CISO

Vemos una gran sintonía de los CISOs participantes con la alta dirección de sus organizaciones. El 88% de los encuestados manifiestan tener su plan estratégico de ciberseguridad aprobado por la alta dirección de sus organizaciones. Esto nos deja un mensaje muy claro: la ciberseguridad ya no es un asunto técnico que se delega “a los de IT”, sino una palanca estratégica que se decide en los comités ejecutivos y en los consejos de administración.

Cuando se habla de riesgo reputacional, continuidad de negocio, experiencia de cliente o confianza de inversores, se está hablando también de ciberseguridad. Y hoy, los consejeros ya no pueden alegar desconocimiento: tienen una responsabilidad legal y fiduciaria explícita sobre la gestión de riesgos, entre ellos los de ciberseguridad, y sobre la supervisión de que la organización cuenta con los mecanismos adecuados de gobierno, control y respuesta para estar protegida. Integrar la ciberseguridad en la agenda del CEO, del comité ejecutivo y del consejo no va solo de aprobar presupuestos o políticas, va de tomar decisiones valientes sobre cómo queremos crecer, qué riesgos estamos dispuestos a asumir y qué nivel de resiliencia exigimos para que el negocio pueda seguir operando incluso en el peor escenario.



Al mismo tiempo, ha habido un gran consenso en la importancia de la cultura de ciberseguridad. Sin cultura y formación continua de los usuarios finales, no hay ciberseguridad sostenible. La mejor estrategia fracasa si la organización no la hace suya en el día a día: en la tienda, en el parque eólico, en la oficina, en el comité de dirección y en el propio consejo. La alta dirección y los consejeros marcan el tono desde arriba, con el ejemplo, con las preguntas que hacen y con las prioridades que fijan, aunque son las personas quienes convierten la cultura en realidad. El reto y la oportunidad está en pasar de "cumplir" a "creer". Pasar de ver la ciberseguridad como un coste necesario a verla como una ventaja competitiva y un compromiso con todos los que hacen posible el negocio: clientes, empleados, accionistas y sociedad. Cuando la ciberseguridad se entiende y se vive de esa forma, ya no es un freno, se convierte en el habilitador silencioso de todo lo que una organización construye y sostiene.

10. Conclusiones y recomendaciones de Eraneos

Esta encuesta que vemos como la Voz del CISO español nos confirma una realidad que ya percibimos en los comités ejecutivos: la ciberseguridad en las grandes organizaciones españolas ha alcanzado un alto grado de madurez estratégica y se gestiona como un activo de resiliencia del negocio, no como una función puramente técnica. El dato de que la mayoría cuenta con el plan estratégico aprobado por la alta dirección refuerza que el diálogo CEO-CISO está más alineado que nunca, impulsado por el peso de la regulación (NIS2/DORA) y por la prioridad clara de resiliencia operativa.

Nuestra recomendación es consolidar este avance formalizando un modelo de gobierno que conecte riesgos, continuidad, crisis y tecnología: métricas comprensibles para dirección y consejo, ejercicios de crisis periódicos y decisiones explícitas sobre apetito de riesgo y niveles mínimos de servicio.

El mensaje más contundente del estudio es que el principal riesgo ya no está "dentro", sino en el ecosistema donde hay terceros sin gestionar, exceso de proveedores y falta de visibilidad real sobre la cadena de suministro. Esto exige pasar de la evaluación puntual a una gestión continua de los terceros, basada en criticidad, controles verificables, monitorización, planes de contingencia y pruebas conjuntas.

En Eraneos recomendamos, además, reforzar la soberanía digital práctica: saber dónde están los datos y las dependencias críticas, reducir riesgos de concentración de proveedores, exigir transparencia sobre subcontrataciones y diseñar estrategias de salida para servicios esenciales.

En 2026, la pregunta no es "¿mi proveedor cumple con los controles mínimos para estar cubiertos?", sino "¿puedo operar y recuperarme si mi proveedor sufre una brecha o un ciberataque?".

En inversión y ejecución, las prioridades apuntan a lo que más reduce riesgo operativo con rapidez: gestión de identidades (IAM/PAM y Zero Trust), eficiencia y optimización de la tecnología existente, seguridad en la

nube y capacidades de detección y respuesta extendidas como base de resiliencia. La preferencia por la automatización evidencia la necesidad de escalar defensas, reducir tiempos de respuesta y mitigar la fatiga del talento.

Nuestra recomendación es una hoja de ruta pragmática:

1. Asegurar lo esencial (identidades, configuración segura, copias de seguridad / recuperación y respuesta).

2. Simplificar e integrar herramientas para ganar gobernabilidad.

3. Elevar la inteligencia operacional (casos de uso, detecciones, inteligencia de amenazas).

4. Abordar la innovación con control: seguridad de modelos / LLMs, protección frente a deepfakes / ultrafalsos y agilidad criptográfica como preparación realista a medio plazo. El objetivo no es acumular más tecnología, es tener más control, más visibilidad y mayor capacidad de recuperación en el corto, medio y largo plazo.

Autores

Eduvigis Ortiz
Cybersecurity Head Iberia
eduvigis.ortiz@eraneos.com

Pedro Navas
Sourcing & IT Advisory Manager
pedro.navas@eraneos.com

Valentina Morales
Cybersecurity Manager Iberia
valentina.morales@eraneos.com

Contacta con nosotros

Eraneos España
Eraneos Iberia S.L.U.
Av. de Europa, 24,
28108 Alcobendas,
Madrid
info.es@eraneos.com
+34 914 290 584