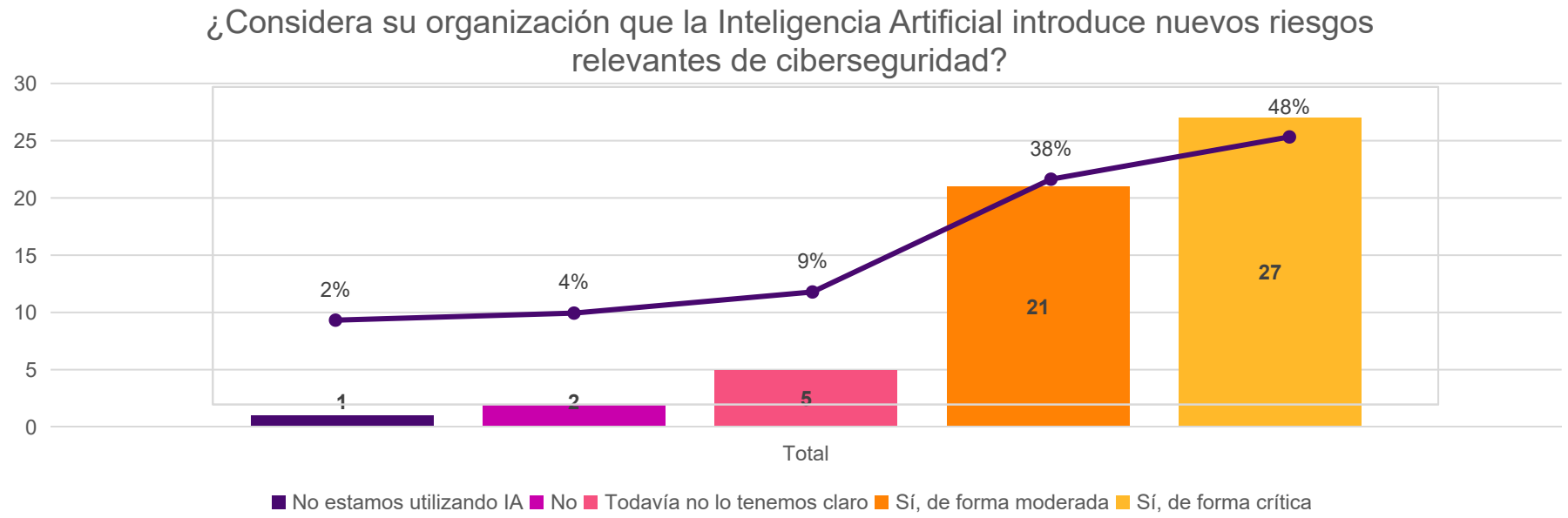
Resultados cuestionario ciberseguridad

FEHM & WTW

Febrero 2026

Relevancia de los riesgos de IA en ciberseguridad

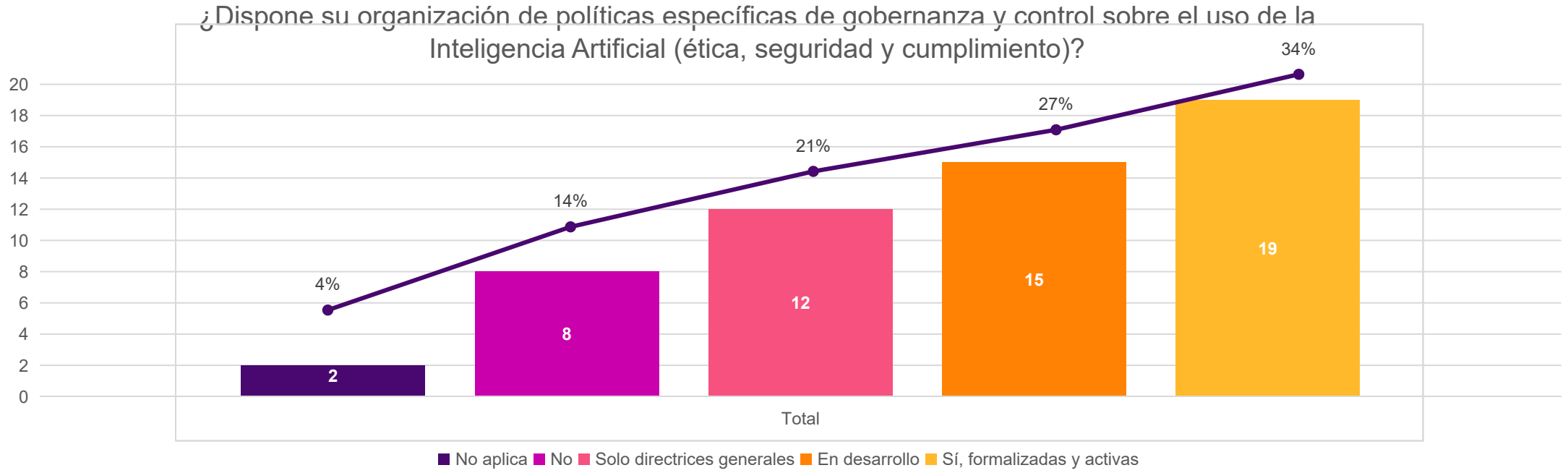
¿Considera su organización que la Inteligencia Artificial introduce nuevos riesgos relevantes de ciberseguridad?



56 compañías, han participado en el estudio

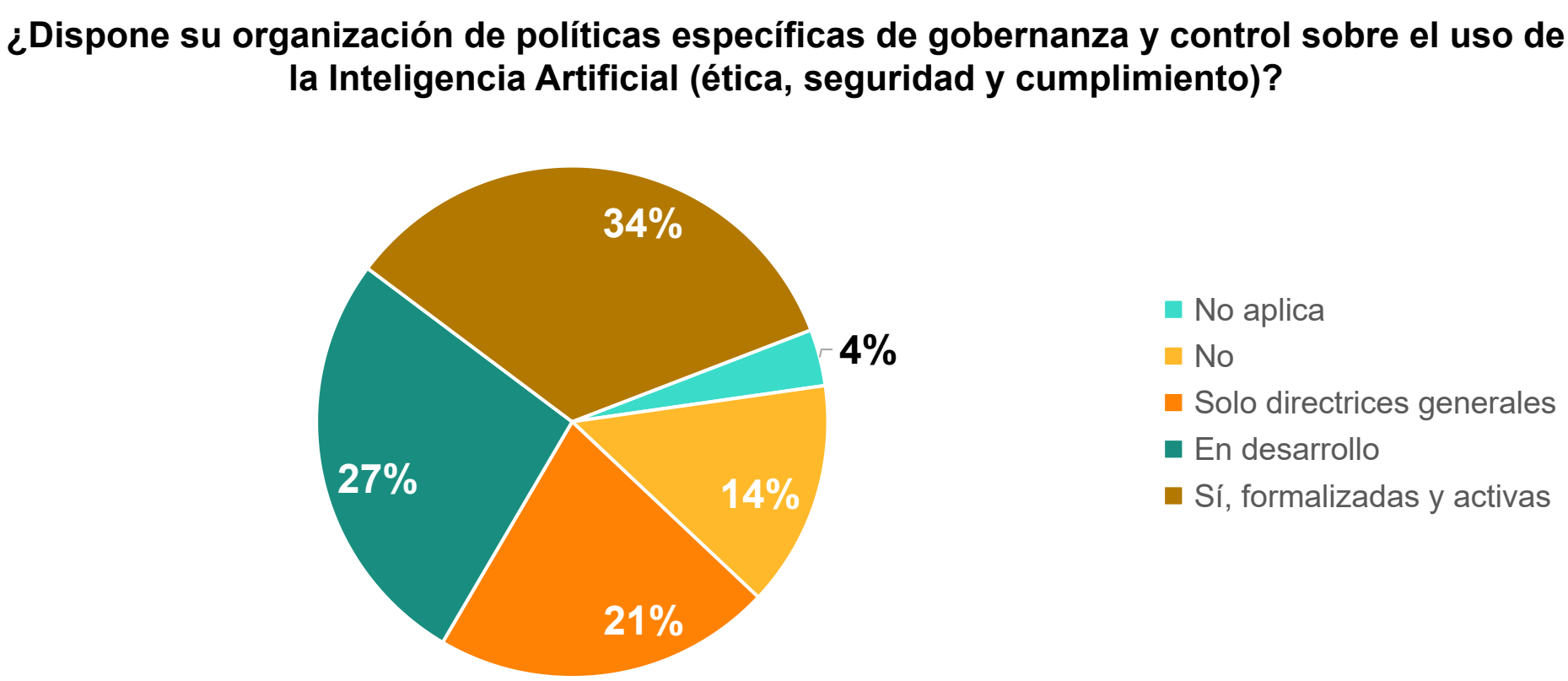
Políticas de gobernanza y control sobre IA

¿Dispone su organización de políticas específicas de gobernanza y control sobre el uso de la Inteligencia Artificial (ética, seguridad y cumplimiento)?



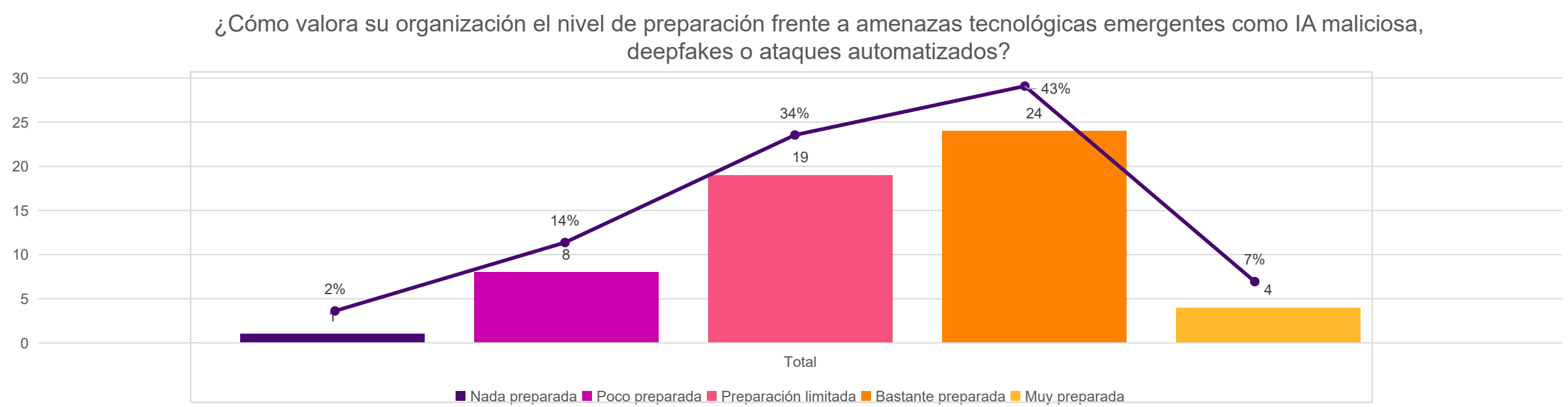
Políticas de gobernanza y control sobre IA

¿Dispone su organización de políticas específicas de gobernanza y control sobre el uso de la Inteligencia Artificial (ética, seguridad y cumplimiento)?



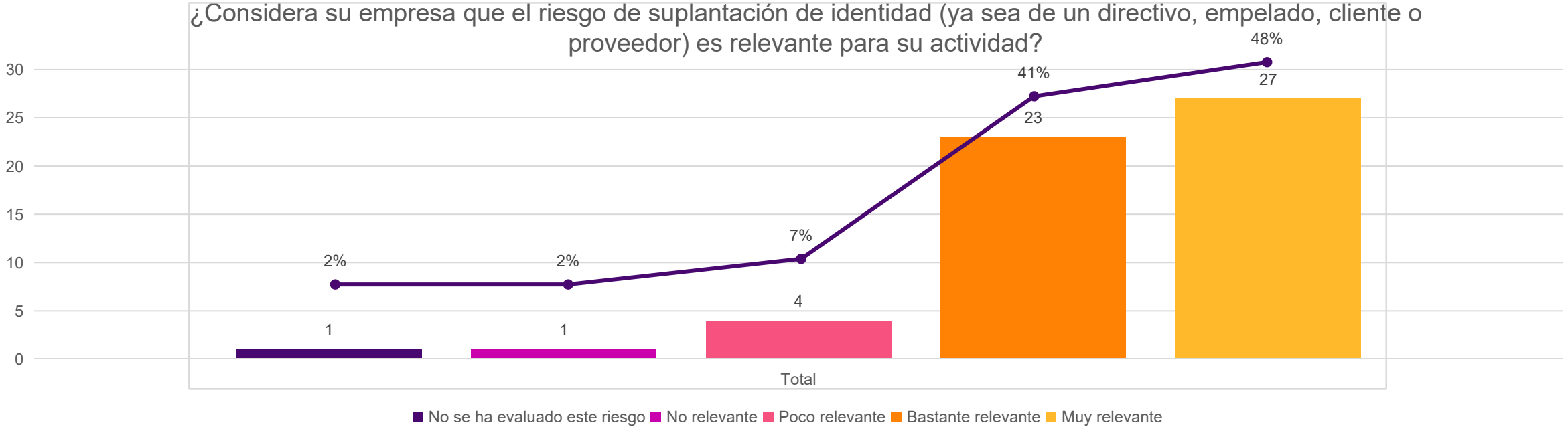
Nivel de preparación frente a amenazas tecnológicas emergentes.

¿Cómo valora su organización el nivel de preparación frente a amenazas tecnológicas emergentes como IA maliciosa, deepfakes o ataques automatizados?



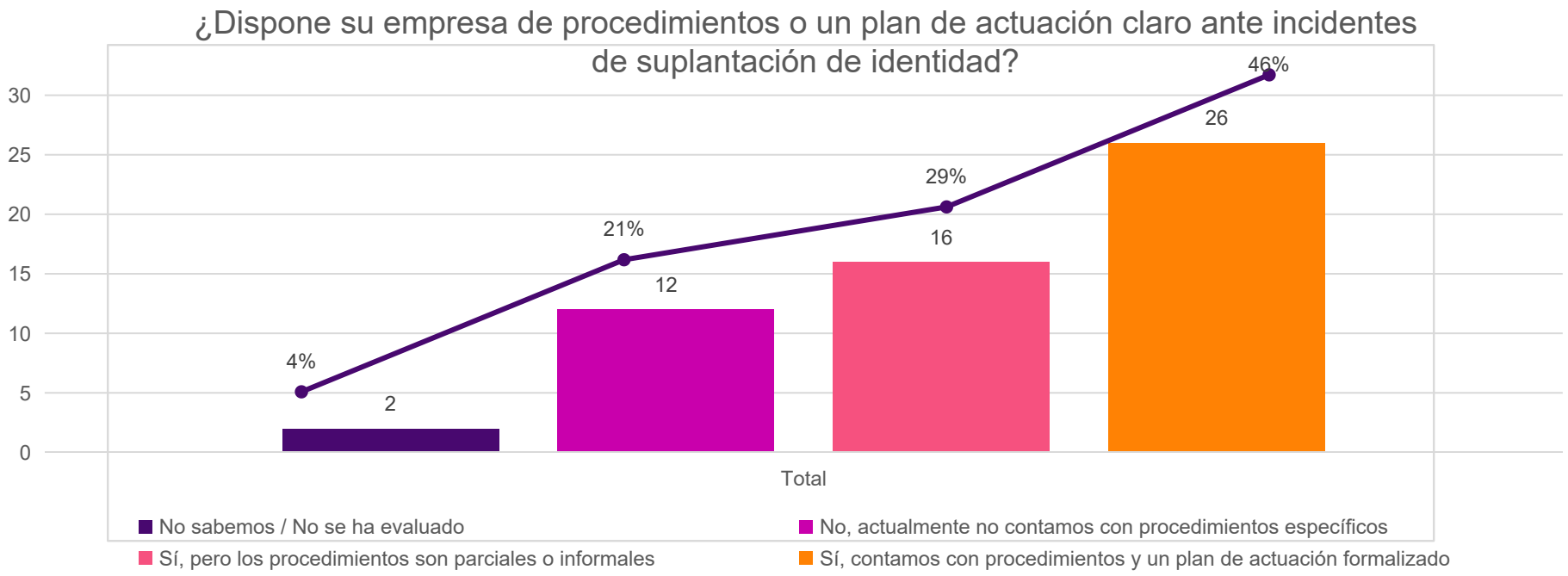
Relevancia del riesgo de suplantación de identidad.

¿Considera su empresa que el riesgo de suplantación de identidad (ya sea de un directivo, empelado, cliente o proveedor) es relevante para su actividad?



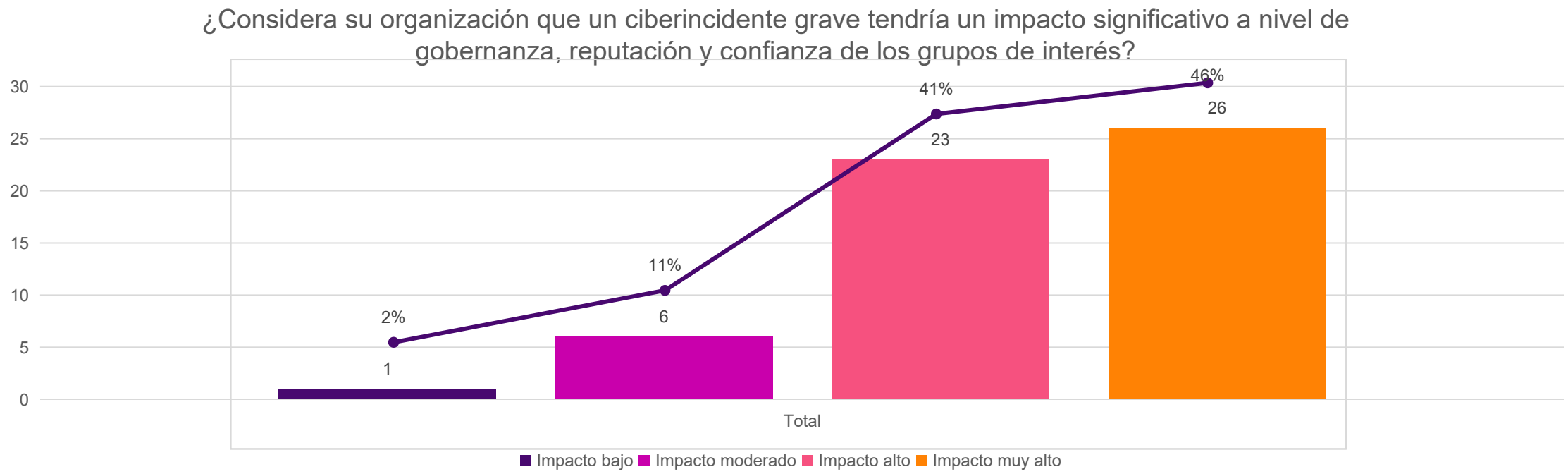
Procedimientos de respuesta ante incidentes.

¿Dispone su empresa de procedimientos o un plan de actuación claro ante incidentes de suplantación de identidad?



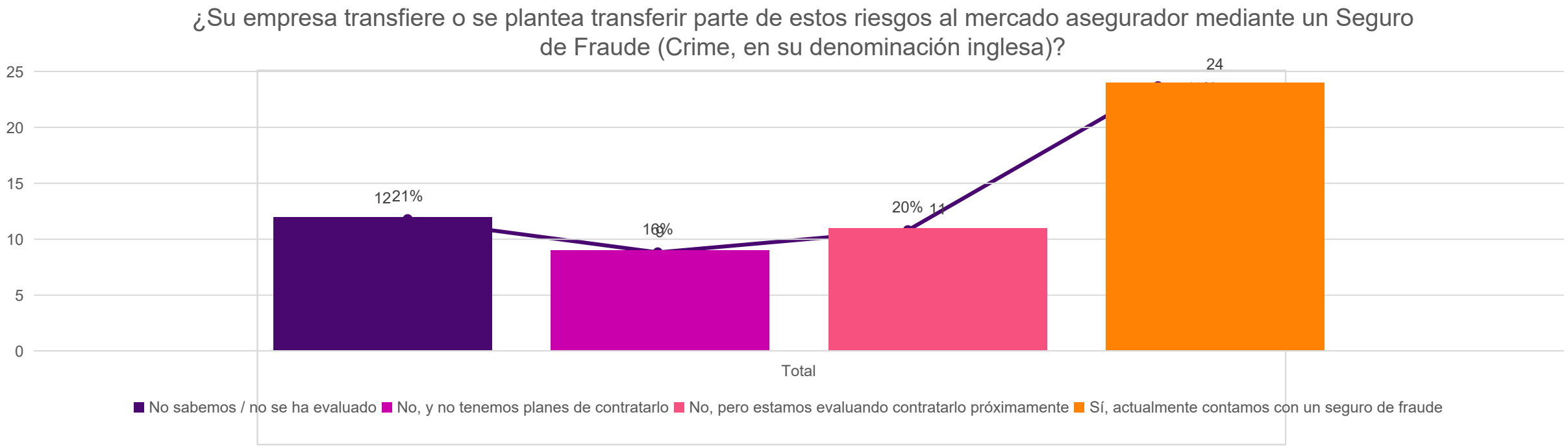
Impacto de un ciberincidente grave.

¿Considera su organización que un ciberincidente grave tendría un impacto significativo a nivel de gobernanza, reputación y confianza de los grupos de interés?



Transferencia de riesgo al mercado asegurador.

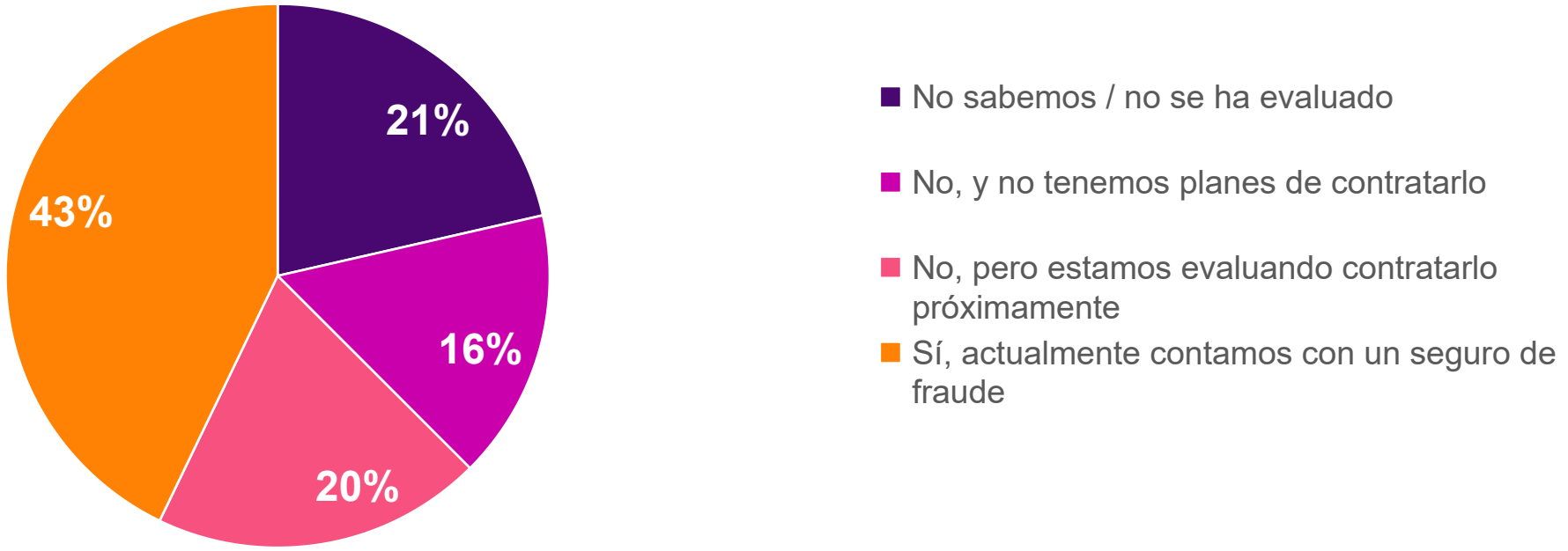
¿Su empresa transfiere o se plantea transferir parte de estos riesgos al mercado asegurador mediante un Seguro de Fraude (Crime, en su denominación inglesa)?



Transferencia de riesgo al mercado asegurador.

¿Su empresa transfiere o se plantea transferir parte de estos riesgos al mercado asegurador mediante un Seguro de Fraude (Crime, en su denominación inglesa)?

¿Su empresa transfiere o se plantea transferir parte de estos riesgos al mercado asegurador mediante un Seguro de Fraude (Crime, en su denominación inglesa)?



Comentarios 1/2

Opcionalmente, ¿desea compartir alguna declaración relacionada con la temática de este estudio? (Puede escribirla a continuación. Esta podrá ser utilizada por Corresponsables en la publicación de las conclusiones del estudio)	Nombre y apellido/s:	Organización	Cargo
Es importante saber combinar las coberturas de las pólizas de Crime, Cyber y D&O	Manuel Font Del Águila	ACCIONA	Gerente de Siniestros
La gestión de ciberseguridad y fraude debe integrarse en el modelo de gobernanza corporativa: prevención, detección, respuesta y transferencia de riesgo. La combinación de controles técnicos, procesos de validación y preparación ante incidentes es clave para proteger la confianza de clientes, terceros y empleados	Anabella Torres	Aranzadi LA LEY	Security Manager South
Estamos en proceso de avanzar en IA en este 2026	sergio moreno	feu vert	area de formación y comuniación interna
Todos sabemos que la IA permite reducir tiempo y esfuerzo a tareas que anteriormente lo requerían. Para los ciberdelincuentes esto supone generar fraudes más rápidos y personalizados, lo que aumenta significativamente el retorno de sus inversiones y, por lo tanto, mayor cantidad de empresas entran entre sus objetivos. Es por ello por lo que la ciberseguridad debe consolidarse como un pilar estratégico para garantizar las operaciones de las compañías y sólo aquellas que entiendan y sepan realizarlo correctamente podrán ser competitivas y sostener su crecimiento en el futuro.	Vicente Camús	Globalvia	Cybersecurity Manager
Hay algo fundamental que debemos tener claro: de nada valen todas las herramientas y avances tecnológicos sin el compromiso personal de cada una de las personas que forman parte de una organización. La tecnología es solo el habilitador; la verdadera seguridad y excelencia dependen de la responsabilidad individual y el compromiso de cada persona del equipo en el uso diario de estas herramientas. Los sistemas son tan fuertes como lo sea el compromiso con las buenas prácticas.	Javier Calvo	GRUPO neoCK	Operations Excellence Manager
Las personas que no poseen conocimientos básicos sobre el uso de la inteligencia artificial y el tratamiento que esta hace de los datos, tanto a nivel personal como profesional, se encuentran en una posición de vulnerabilidad. Incluso cuando se utiliza la propia IA como herramienta de aprendizaje, la velocidad de evolución tecnológica y el volumen de información gestionada superan con frecuencia la capacidad humana de asimilación.	Zargo Alejandro Claudios Santos	Record go Alquiler Vacacional, SLU	Systems Manager
El impacto de la IA sobre la ciberseguridad de los sistemas y la información está en continuo cambio, ligado al rápido desarrollo de la IA y sus aplicaciones. En mi opinión, va más allá del impacto analizado hasta ahora (confidencialidad, disponibilidad e integridad). La IA puede tener un impacto directo sobre los procesos internos. Es capaz de alterar datos para manipular los resultados, saltarse controles para modificar procesos de trabajo o engañar a los usuarios suplantando a los interlocutores. Es necesario establecer modelos claros para analizar y controlar estos riesgos en un entorno tan dinámico y cambiante.	Laura Prats	Relyens	Cyber Risk Manager
La integración de la ciberseguridad y la prevención del fraude en los marcos de gobernanza es clave en un entorno donde la IA y las tecnologías emergentes avanzan rápidamente. Las organizaciones deben reforzar una gobernanza tecnológica responsable, alineada con criterios ESG, para garantizar confianza, resiliencia y transparencia.	Antonio Rodríguez	TALAT	Responsable IT

Comentarios 2/2

Opcionalmente, ¿desea compartir alguna declaración relacionada con la temática de este estudio? (Puede escribirla a continuación. Esta podrá ser utilizada por Corresponsables en la publicación de las conclusiones del estudio)	Nombre y apellido/s:	Organización	Cargo
Este escenario global se refleja también a nivel nacional. Solo en 2025, la Agencia Española de Protección de Datos (AEPD) recibió más de 19.000 reclamaciones, una cifra que pone de manifiesto la creciente presión regulatoria y operativa a la que se enfrentan las organizaciones para garantizar la privacidad de la información en contextos cada vez más digitales y complejos. A esta complejidad se suma la adopción acelerada (y sin la consiguiente respuesta a contingencias) de nuevas tecnologías. En España, el 86% de las organizaciones reconoce no contar con un plan de respuesta ante posibles fallos o errores en el uso de la IA, y solo el 20% destina presupuesto específico a la protección de la privacidad asociada a esta tecnología, según un estudio de Zoho con Arion Research. Cuatro claves que marcarán la privacidad de los datos en el entorno laboral en 2026 Zoho prevé una integración cada vez más profunda de las prestaciones de seguridad en torno a cuatro grandes ejes, que redefinirán cómo las empresas protegen la privacidad de los datos en el entorno laboral. 1. De soluciones aisladas a un modelo integrado de seguridad Este año, las organizaciones dejarán progresivamente atrás los enfoques basados en herramientas independientes, para avanzar hacia modelos integrados de seguridad del entorno laboral, que aborden de forma conjunta la identidad, la autenticación, la protección de los datos y el control de accesos. Este cambio permitirá reducir los riesgos derivados de soluciones en silos y de la aplicación inconsistente de políticas. 2. La gestión de identidades, eje central de la privacidad en la empresa En entornos de trabajo híbridos, donde los empleados acceden a aplicaciones y datos desde múltiples dispositivos, la identidad digital se consolida como la fuente única de referencia para la autenticación y la autorización. De cara a 2026, las empresas tenderán a apoyarse en credenciales únicas, autenticación multifactorial y métodos resistentes al phishing, como las passkeys, junto con políticas adaptativas y automatizaciones. 3. El navegador como nueva frontera de la privacidad de los datos Con las operaciones diarias cada vez más concentradas en aplicaciones SaaS, los navegadores empresariales se convertirán en una pieza clave para la protección de la privacidad, al ser el entorno desde el que los empleados interactúan con la mayor parte de la información corporativa. Frente a los navegadores de consumo, los navegadores empresariales permiten aplicar políticas de acceso, control de datos y monitorización de sesiones. 4. Simplicidad operativa como requisito para proteger la privacidad En paralelo, los equipos de seguridad priorizarán plataformas integradas frente a soluciones fragmentadas, con el objetivo de mejorar la visibilidad, reducir la fricción para los usuarios y acelerar la respuesta ante incidentes. En 2026, la protección de la privacidad en el entorno laboral evolucionará hacia ecosistemas únicos y optimizados, capaces de ofrecer una experiencia de usuario coherente sin renunciar a un nivel elevado de seguridad.	Sridhar Iyengar	Zoho	Director General de Zoho en Europa
Hay algo fundamental que debemos tener claro: de nada valen todas las herramientas y avances tecnológicos sin el compromiso personal de cada una de las personas que forman parte de una organización. La tecnología es solo el habilitador; la verdadera seguridad y excelencia dependen de la responsabilidad individual y el compromiso de cada persona del equipo en el uso diario de estas herramientas. Los sistemas son tan fuertes como lo sea el compromiso con las buenas prácticas.	Javier Calvo	GRUPO neoCK	CEO

Gracias