2023 - Estudio sobre el estado de la seguridad de la información y privacidad de datos en Centroamérica y CARICOM

12 de mayo de 2023

CONTENIDO

RESUMEN EJECUTIVO

El “Estudio sobre el Estado de la Seguridad de la Información y Privacidad de Datos” fue llevado a cabo del 1 de marzo al 28 de abril de 2023 y contó con 163 participantes en Centroamérica, CARICOM y República Dominicana. El estudio tiene como objetivo dar a conocer la madurez de las iniciativas en la seguridad de la información en la región.

Si bien es cierto, el estudio muestra una evolución importante en la adopción de tecnologías para la protección de la información y redes, el mismo refleja que los esfuerzos de las organizaciones para mantener un nivel de seguridad maduro distan del grado de complejidad, sofisticación y frecuencia de las amenazas y riesgos tecnológicos que encaran las organizaciones hoy día. Esta afirmación se sostiene debido a que:

- Limitada existencia de un Comité de Seguridad de la Información, Ciberseguridad o Riesgo Tecnológico entre los participantes. Solo un 42% confirmaron su existencia. Su ausencia limitaría grandemente a los Altos Ejecutivos, reguladores y partes interesadas, conocer los riesgos y amenazas tecnológicas a las que está expuesta la organización, comprender el nivel de efectividad de los controles y la toma efectiva de decisiones para la protección de los recursos tecnológicos.

RESUMEN EJECUTIVO

- El 88% de los participantes afirmó utilizar estrategias obsoletas y poco vanguardistas para concienciar a los usuarios finales en seguridad de la información. Esto es preocupante, ya que, los usuarios finales son el eslabón más débil en la cadena de seguridad de información.

- El 62% de los participantes indicó no disponer de mapa de riesgo actualizado que muestre el impacto y la probabilidad de los riesgos tecnológicos que pueden afectar la operación de la organización.

- El uso de herramientas tecnológicas de vanguardia que incluya inteligencia artificial o "*machine learning*" para fortalecer las estrategias de seguridad de información es bajo. Solo un 22% indicó utilizar este tipo de tecnologías.

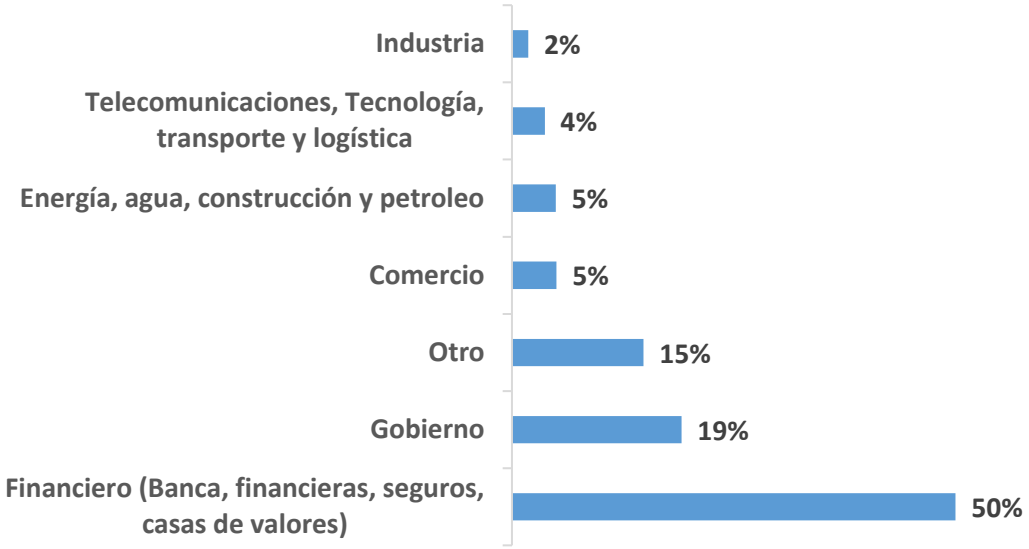
El estudio refleja algunas iniciativas positivas de seguridad de la información entre los participantes. No obstante, no son suficientes.

Respetuosamente invitamos a los participantes a que hagan su *"benchmark"* a fin identificar las áreas que necesitan atención en su organización.

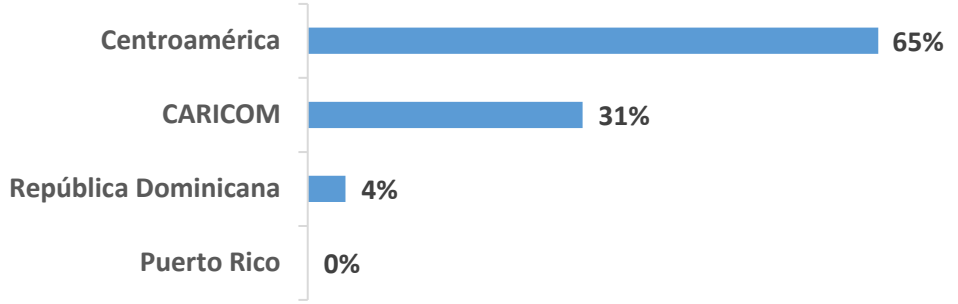
DISTRIBUCIÓN DE PARTICIPANTES

DISTRIBUCIÓN DE PARTICIPANTES

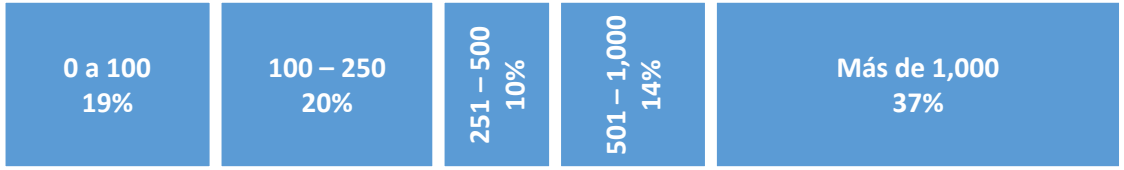
Sector económico



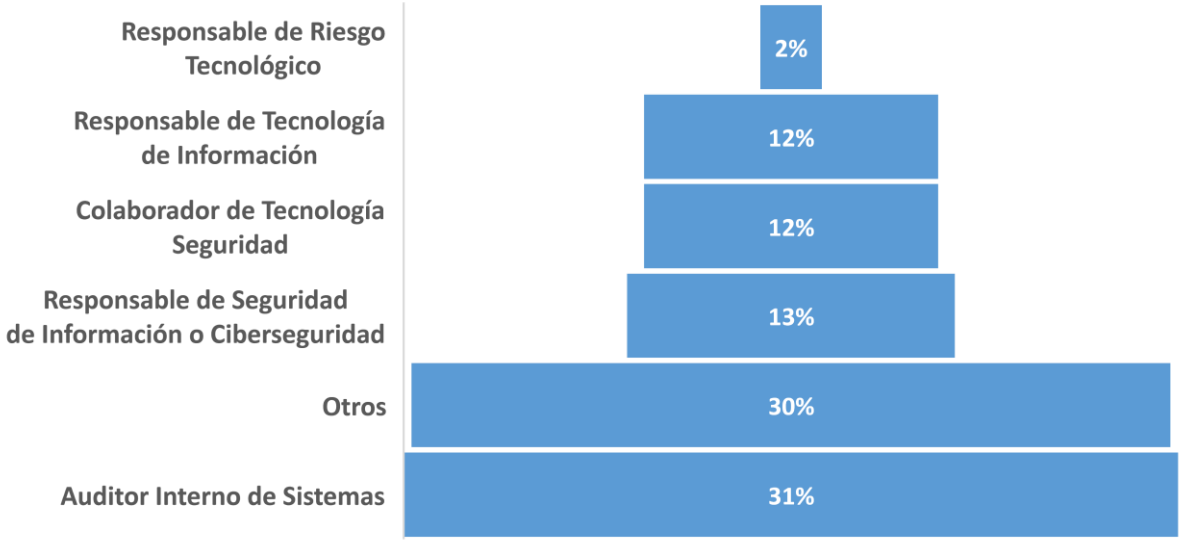
Región



Cantidad de colaboradores



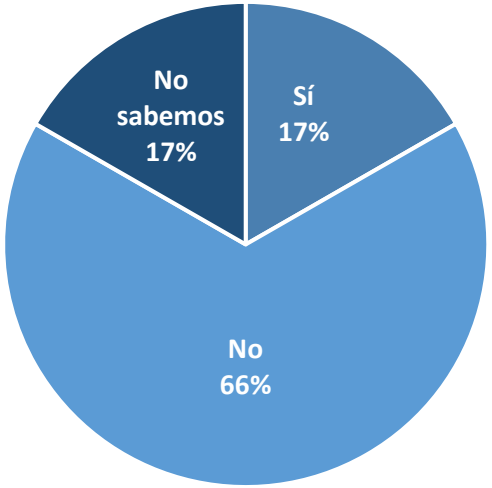
Rol dentro de la Organización




GESTIÓN DE
SEGURIDAD Y
GOBERNAZA

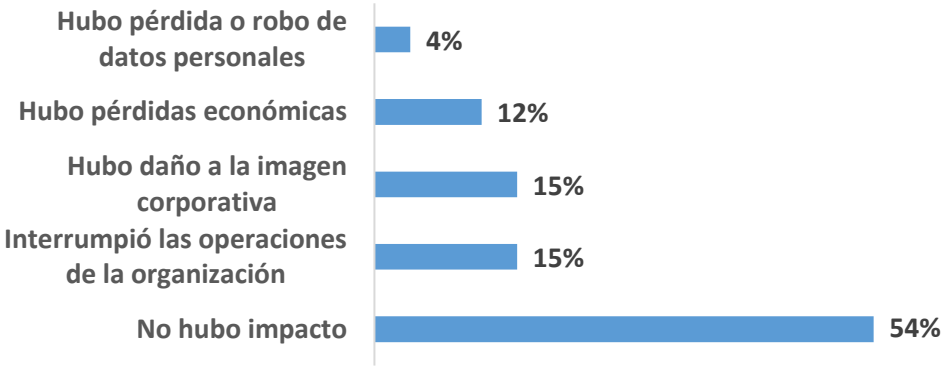
GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN E INCIDENTES

¿Ha sufrido su Organización un incidente de seguridad en los últimos 12 meses?

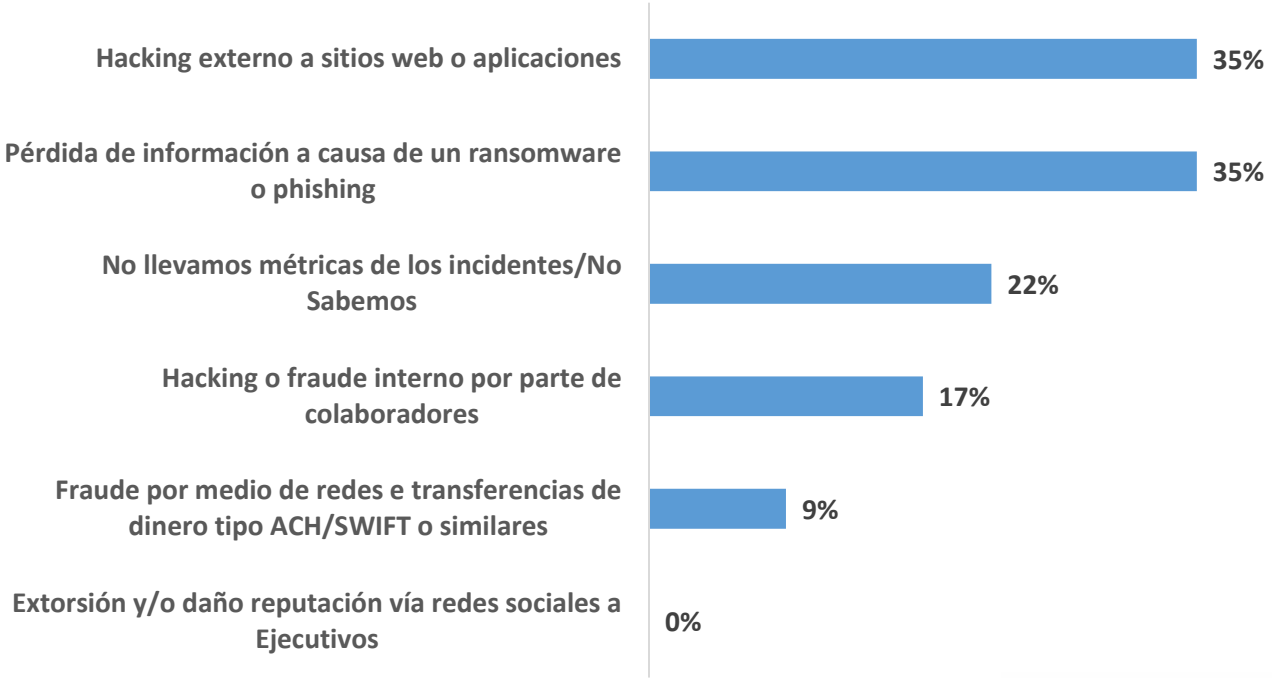


- Preocupa que un 17% indique que no sabe si hay sufrido un incidente de seguridad.
- De los participantes que sufrieron un incidente, un 31% sufrió daño a la imagen o interrupción de las operaciones.

¿Cuál su fue impacto?

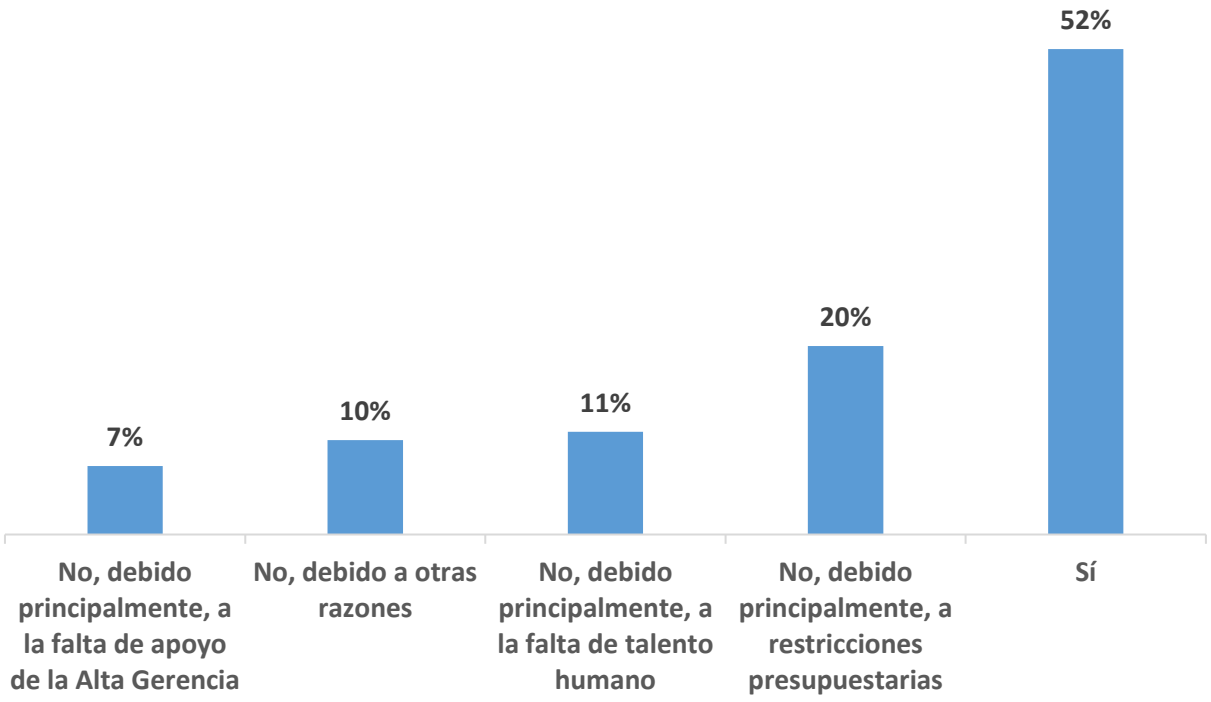


¿Qué tipo de incidentes ha experimentado su Organización en los últimos 12 meses?

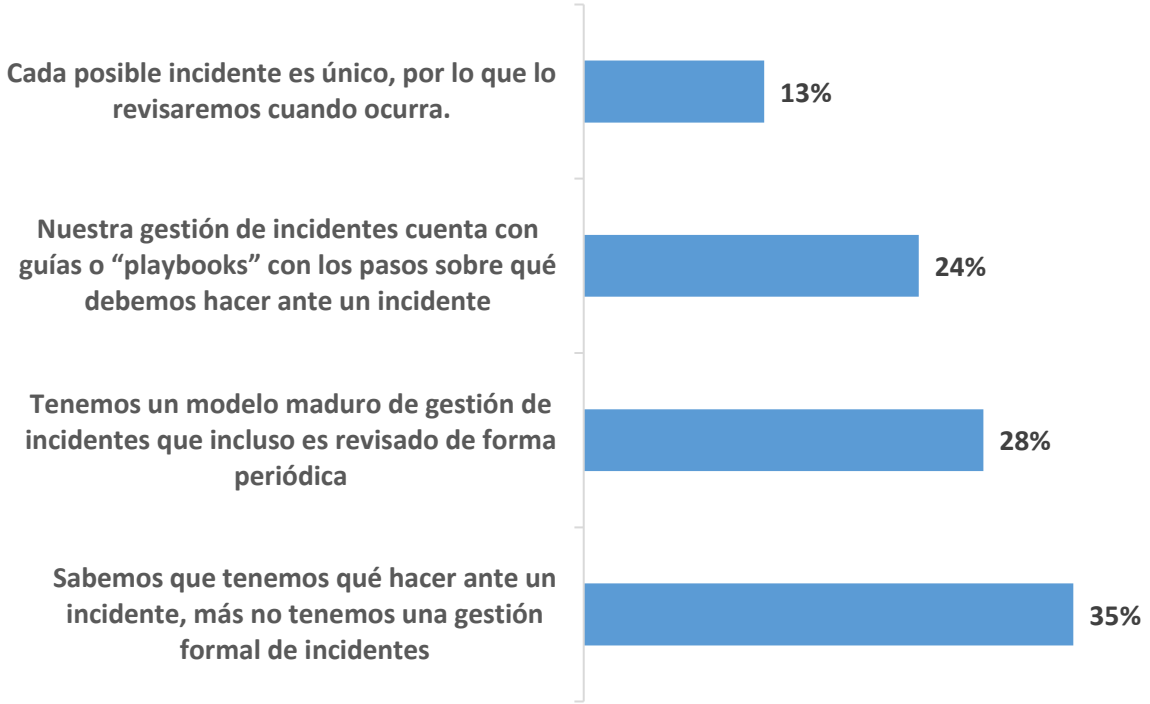


GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN E INCIDENTES

¿Considera que la función de seguridad de la información está cubriendo las necesidades de su Organización?



¿Cuál de los siguientes enunciados describiría, de la mejor forma, la estrategia de gestión de incidentes de seguridad de su Organización?



En una sociedad interconectada digitalmente y donde los hackeos ocurren diariamente, preocupa:

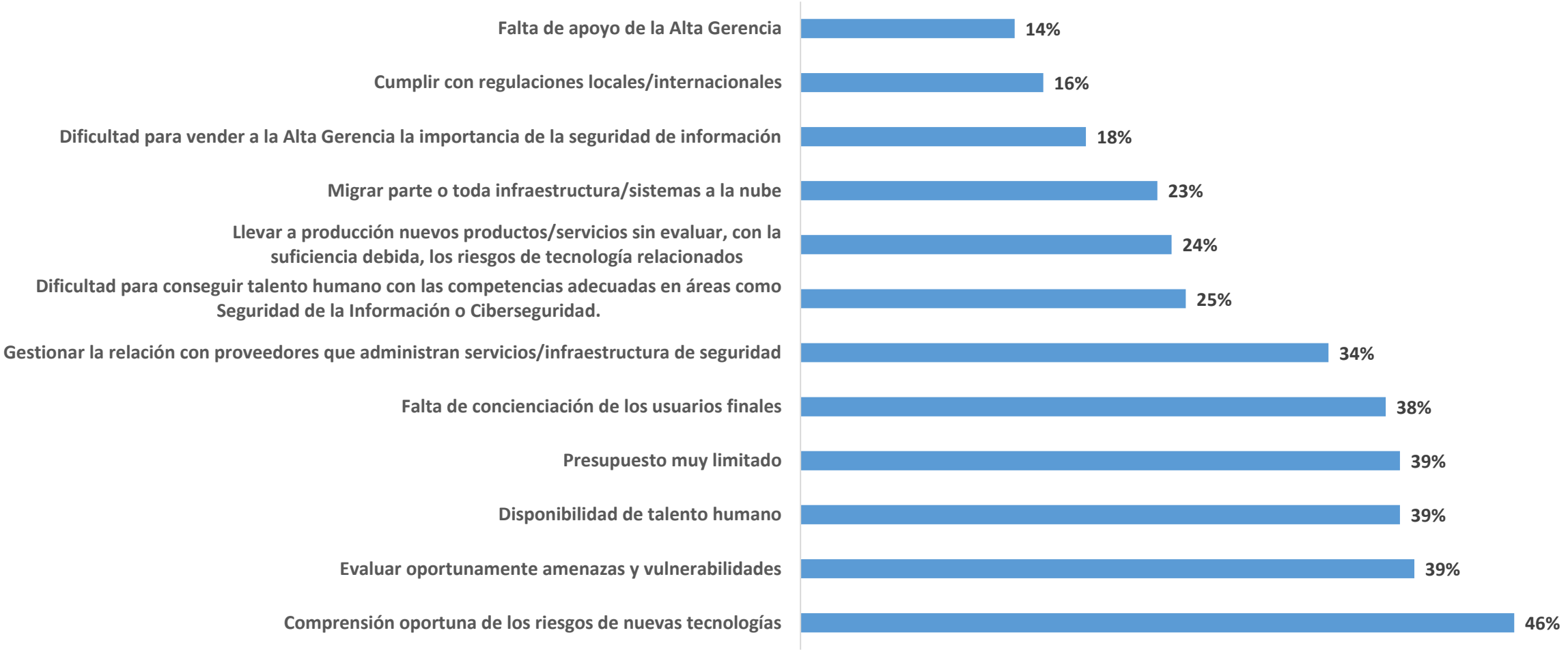
- Que el 48% considere que la seguridad de información no cubre las necesidades de la organización
- Que solo el 28% tenga un modelo de gestión de incidentes de seguridad

GOBERNANZA

En el 2023, ¿cuáles considera usted serán las principales prioridades, en cuanto a seguridad de información, en su Organización?

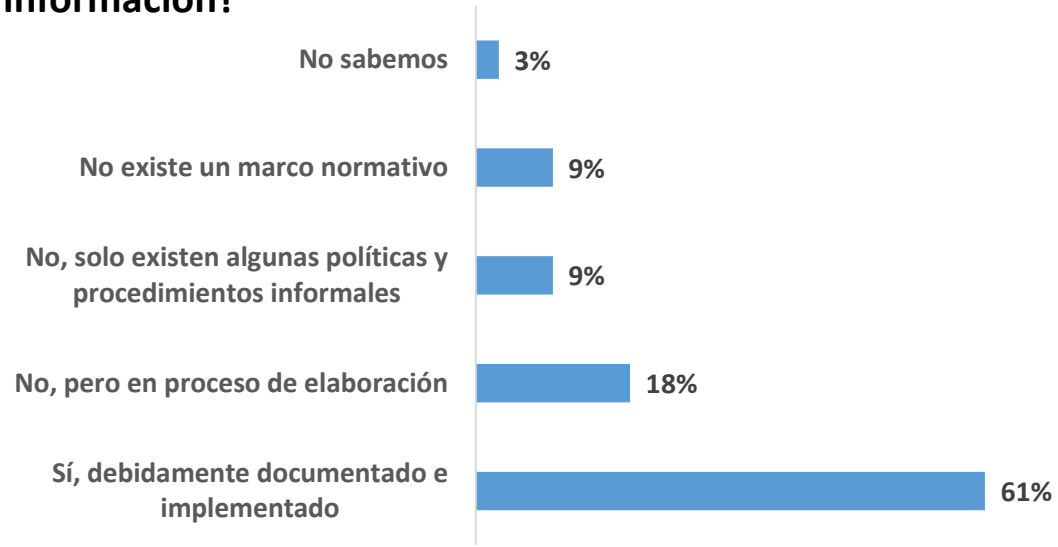
GOBERNANZA

En el 2023, ¿cuáles considera usted serán los principales desafíos para mejorar la seguridad de la información en la organización?

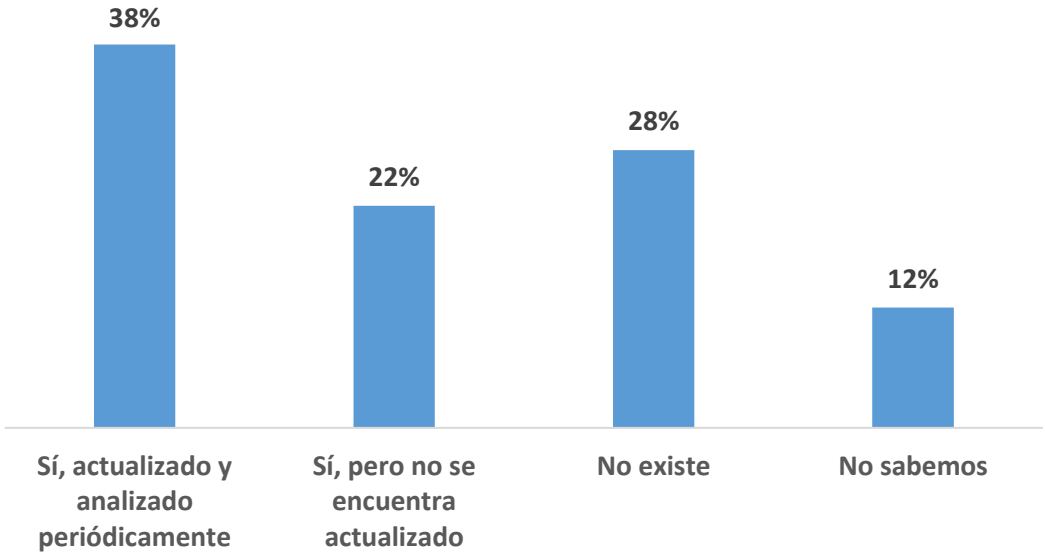


GOBERNANZA

¿Existe en su Organización un marco normativo (políticas, procesos y procedimientos), para administrar la seguridad de la información a fin de mitigar los riesgos derivados del uso de tecnología de información?



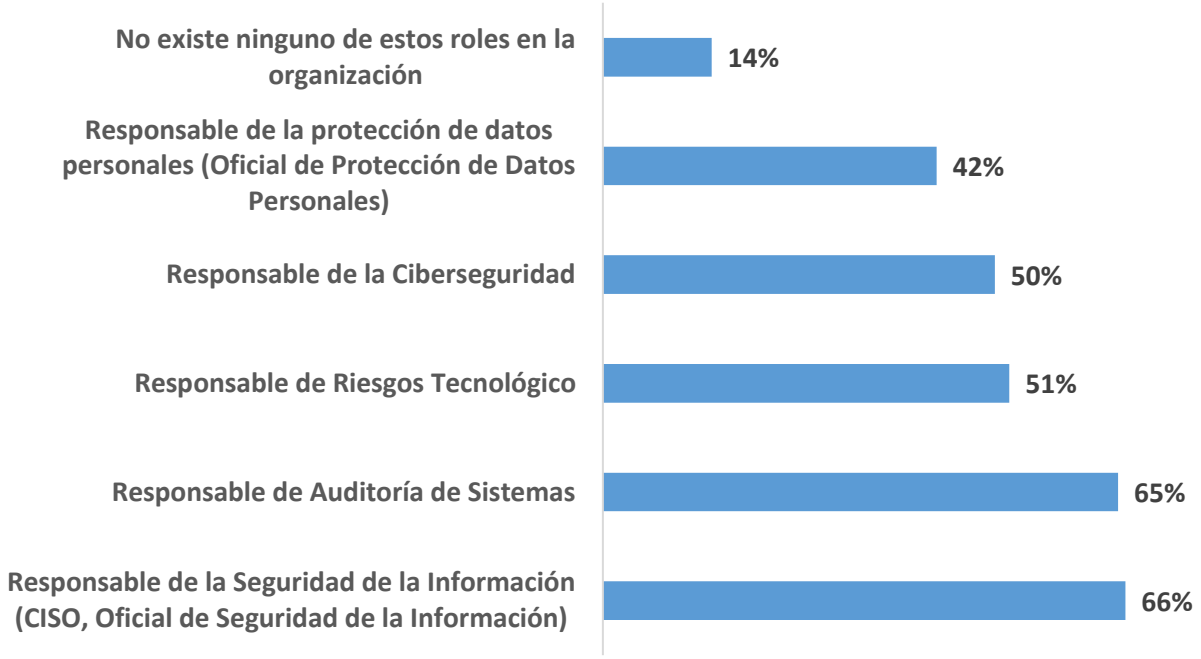
¿Existe un mapa de riesgo que muestre el impacto y la probabilidad de los riesgos tecnológicos que pueden afectar la operación de la organización?



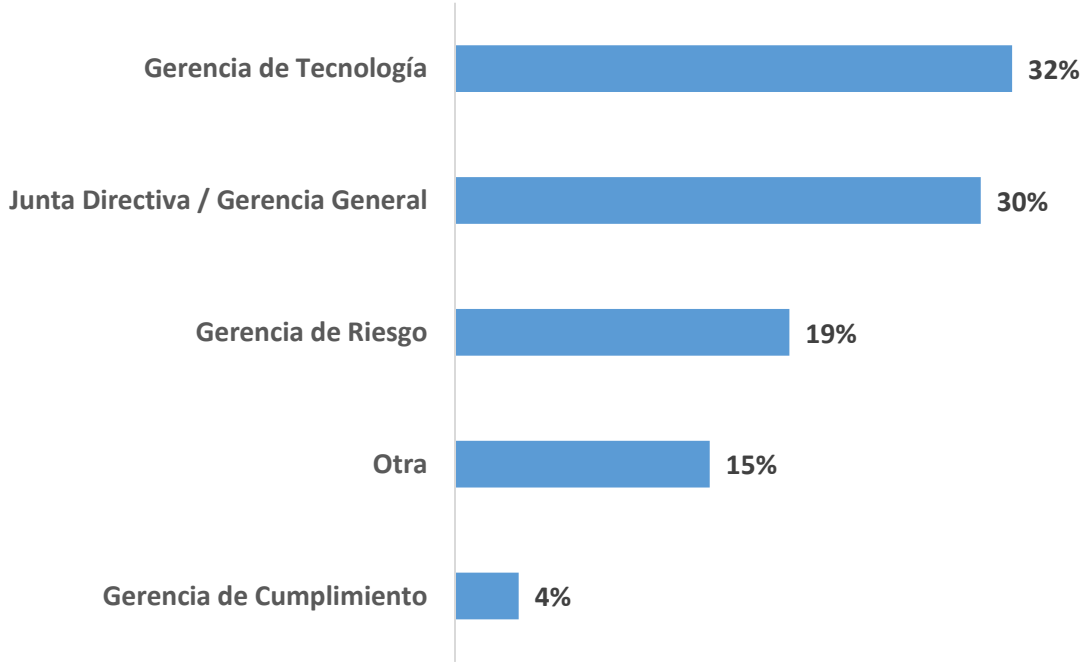
Que solo el 39% de los participantes afirme no tener un marco documentado para la gestión de seguridad merece la atención de las organizaciones. Lo anterior se complica ya que, solo el 38% indicó disponer de un mapa de riesgos tecnológicos actualizado.

GOBERNANZA

¿Cuenta la organización con talento humano para alguna de las siguientes funciones?



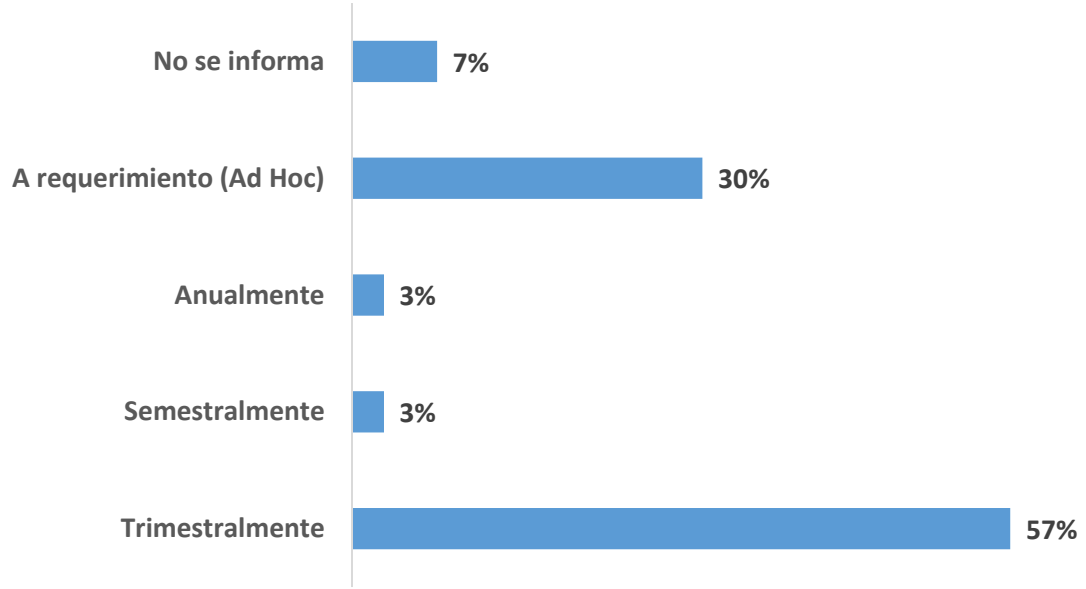
¿A quién reporta el Oficial de Seguridad de la Información?



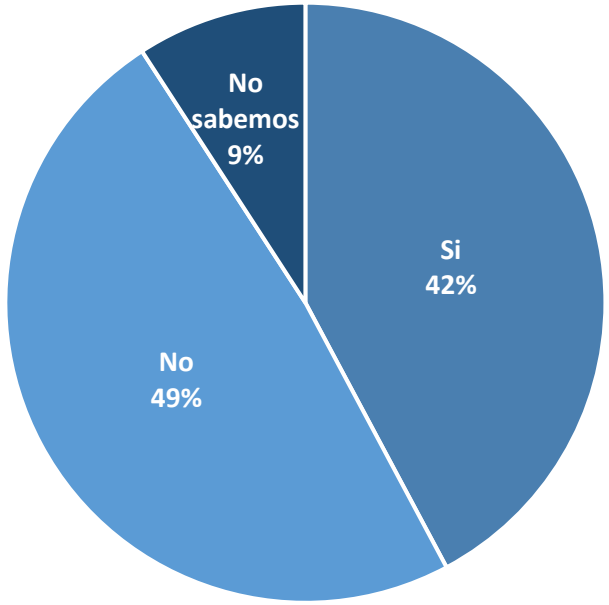
La ausencia de áreas de control en un 14% de los encuestados es preocupante con el creciente número de amenazas al que están expuestas las organizaciones.

GOBERNANZA

¿Con qué frecuencia se informa a los niveles superiores (por ejemplo, Gerente General, Comités, Vicepresidentes, Junta Directiva, Ministros de Estado) sobre el nivel de seguridad de información de la organización?



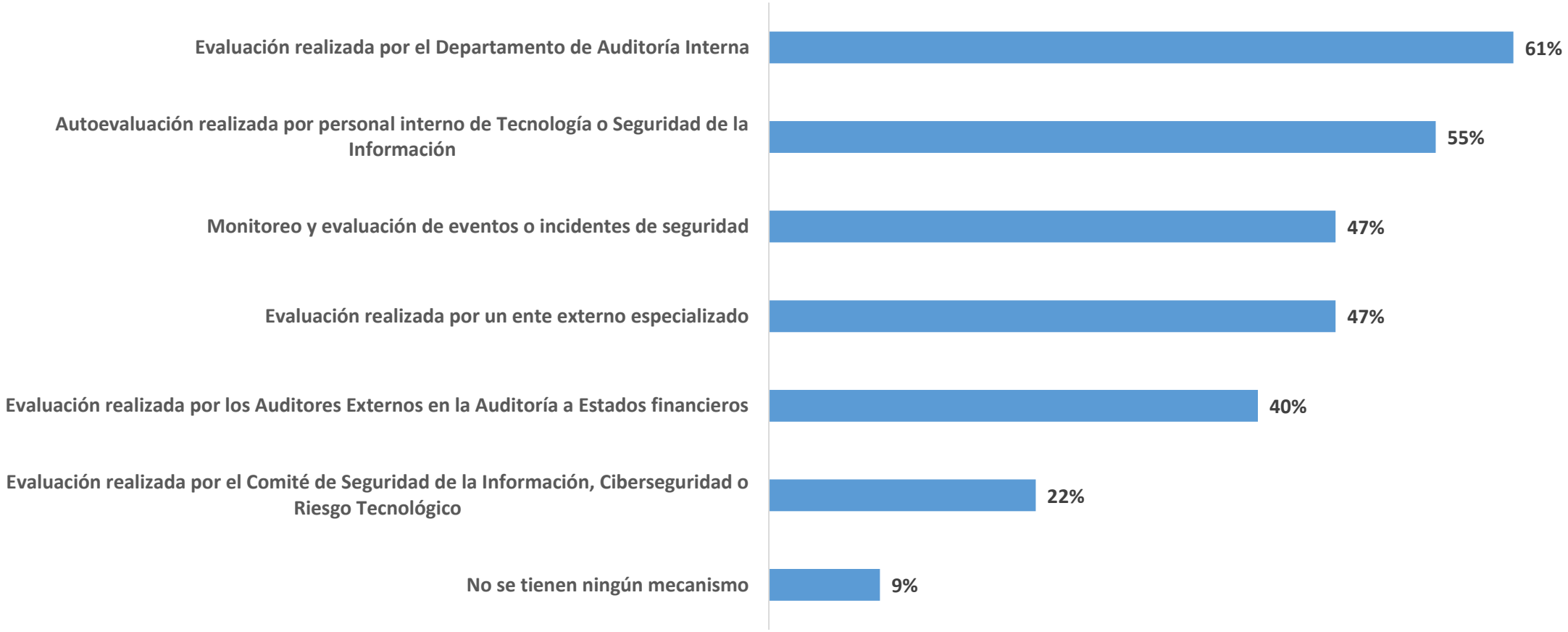
¿Cuenta su organización con un Comité de Seguridad de la Información, Ciberseguridad o Riesgo Tecnológico?



El estudio evidencia que las Juntas Directivas y/o “C-Levels” no son documentados recurrentemente sobre el estado de la seguridad de la información en la organización. Un 13% no reciben información o con un poco frecuencia.

GOBERNANZA

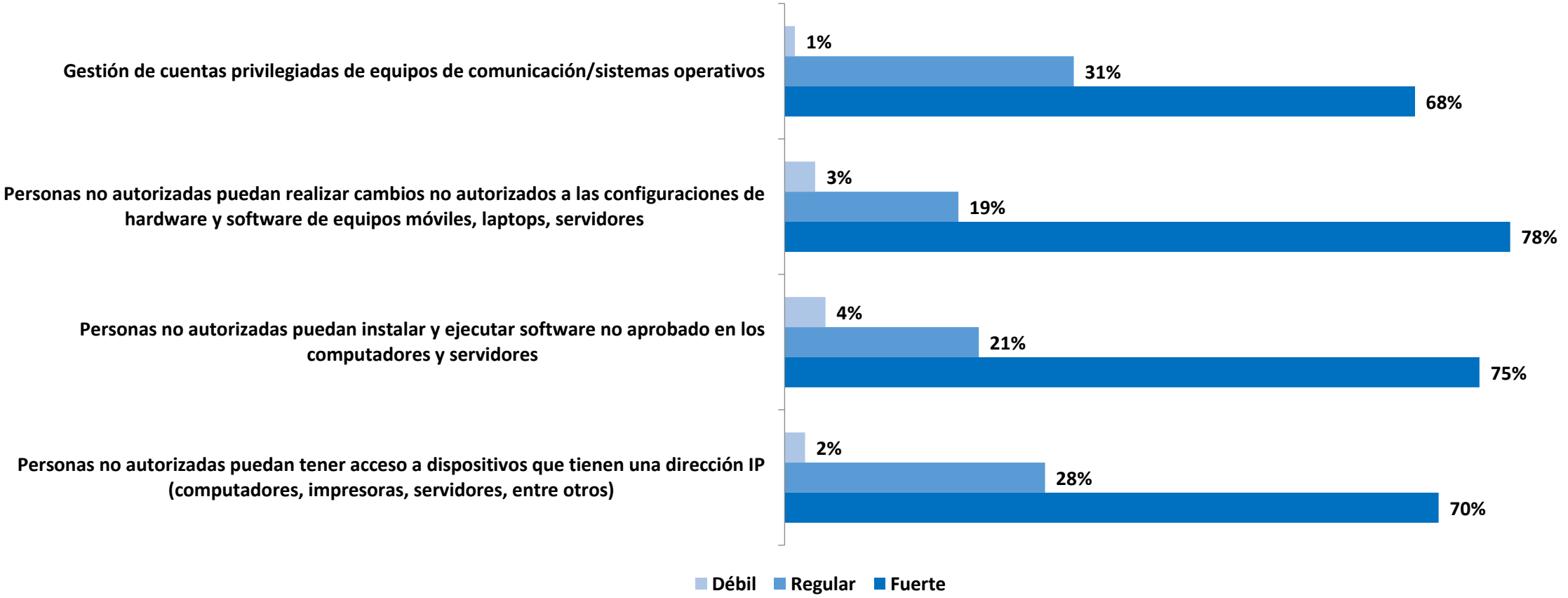
¿Cuáles mecanismos utilizan en la organización para evaluar la efectividad de la estrategia de seguridad de información?




OPERACIONES Y
TECNOLOGIAS DE
SEGURIDAD

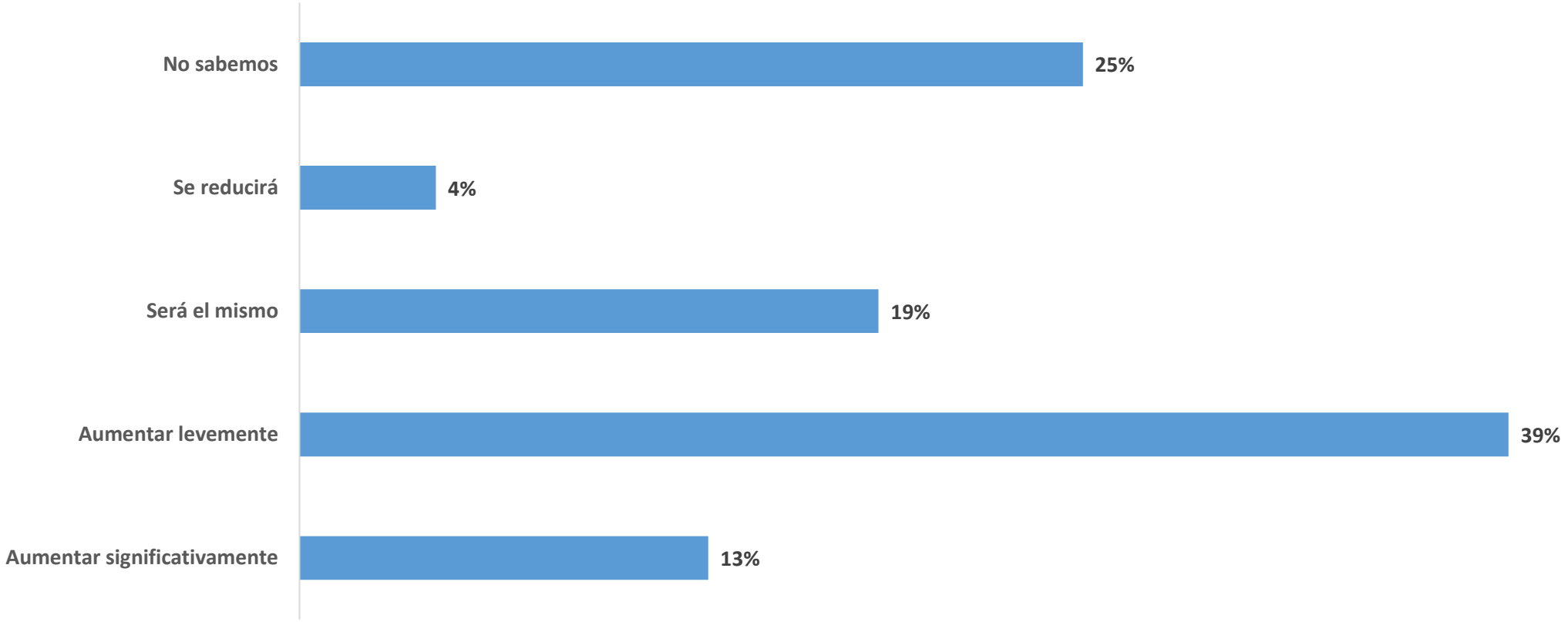
OPERACIONES Y TECNOLOGÍAS DE SEGURIDAD

Considera usted que los controles implantados en su organización, para mitigar los riesgos abajo descrito, ¿son?:



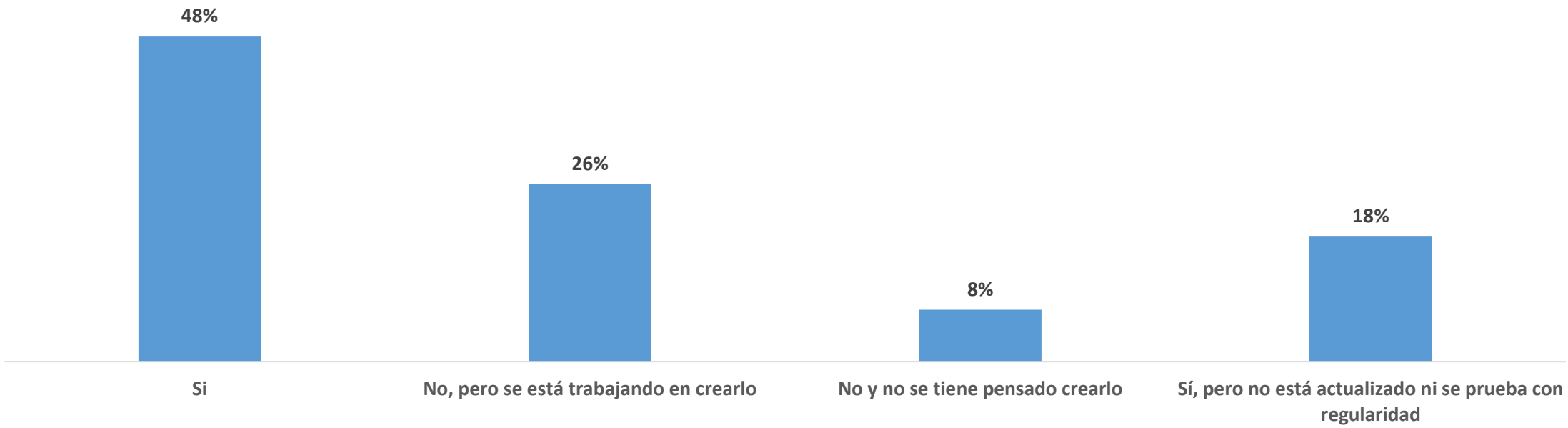
OPERACIONES Y TECNOLOGÍAS DE SEGURIDAD

¿Considera que el presupuesto asignado a seguridad de información para el 2023 y comparado con el del 2022 va a…?



OPERACIONES Y TECNOLOGÍAS DE SEGURIDAD

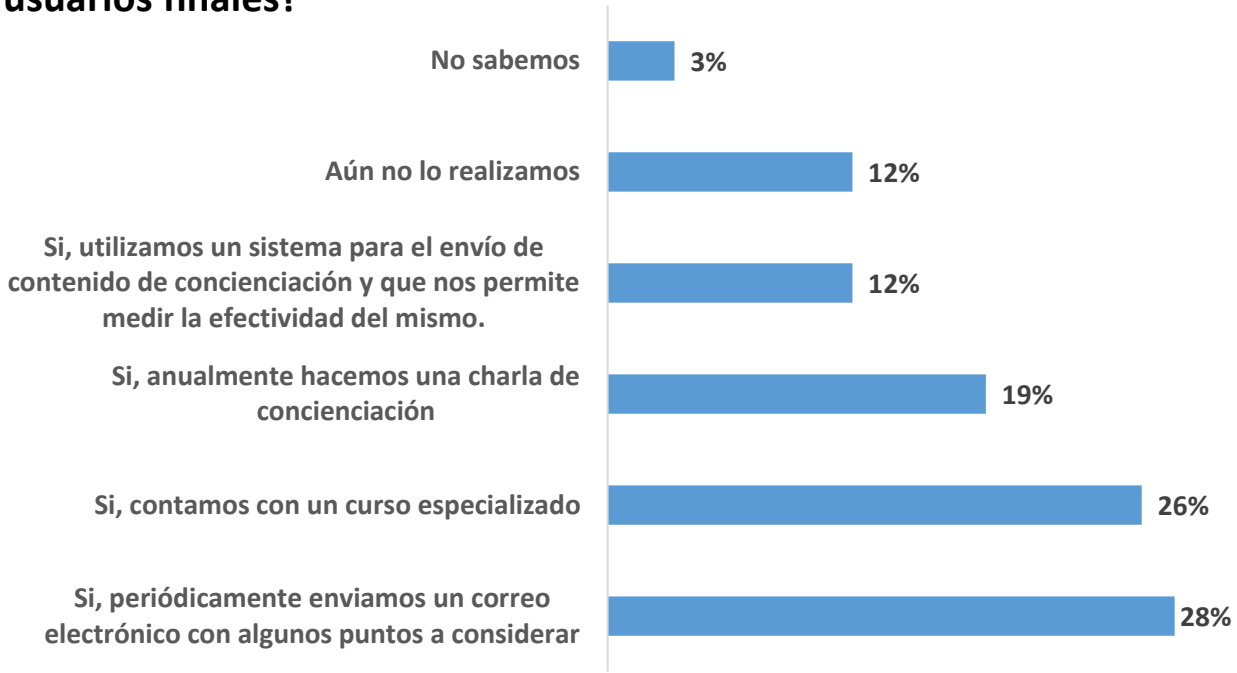
¿Dispone la organización de un plan de recuperación ante desastres, debidamente documentado y probado con regularidad?



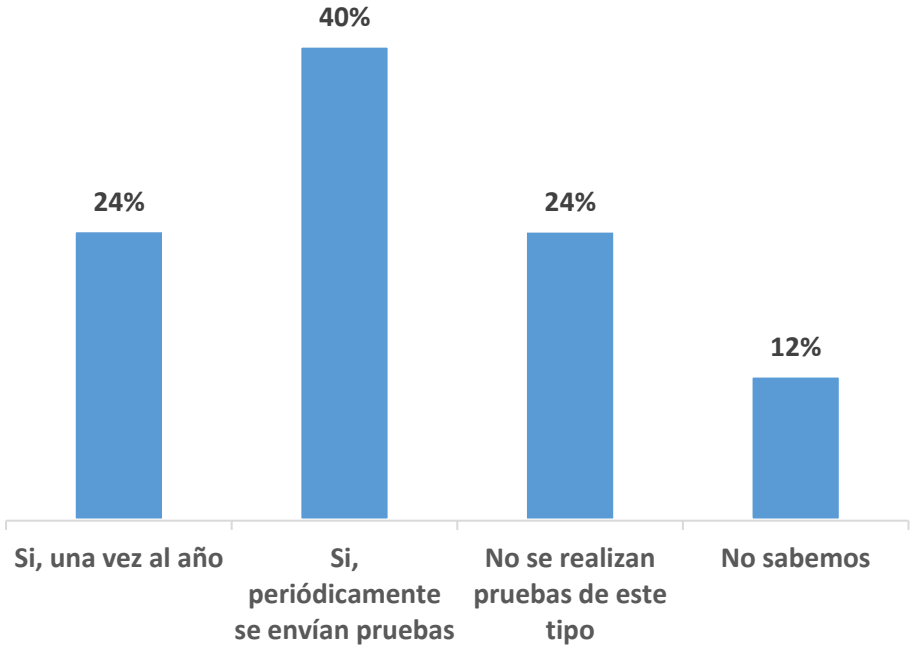
A pesar de que un 48% comenta tener un plan de recuperación ante desastres, es inquietante que el restante 52% de los encuestados no dispongan de un plan o que el mismo no se encuentre actualizado.

OPERACIONES Y TECNOLOGÍAS DE SEGURIDAD

¿Dispone la organización de alguna estrategia para reforzar la concienciación en seguridad de la información de los usuarios finales?



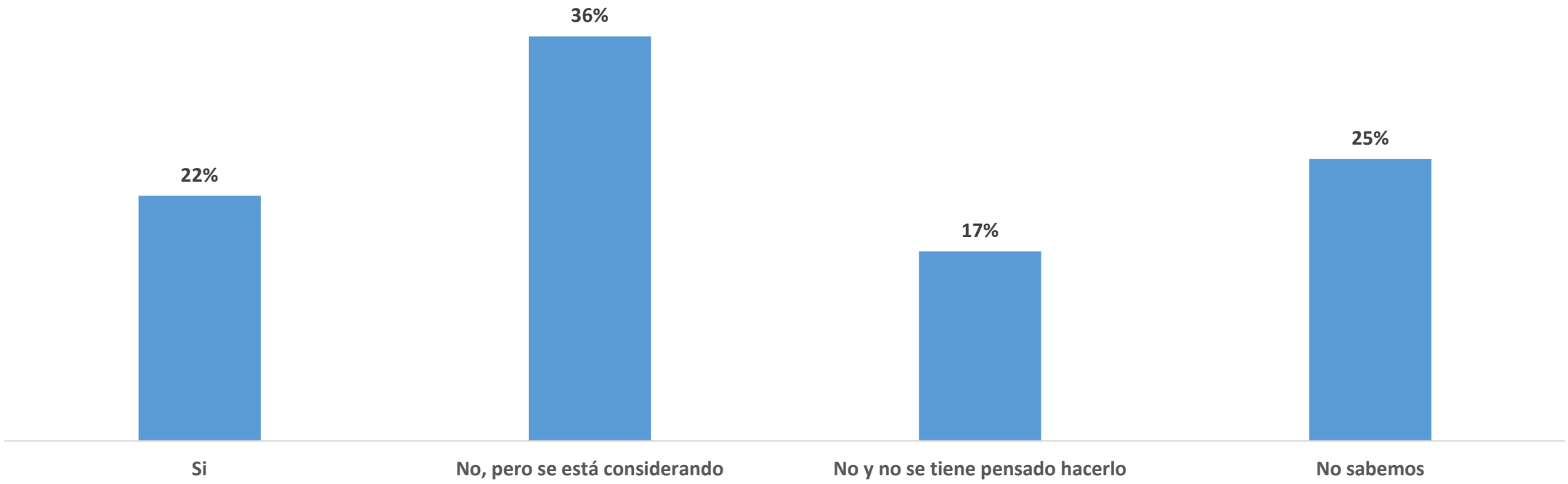
¿Su organización realiza pruebas o simulaciones de phishing o ransomware regularmente?



Es evidente que la concienciación de los usuarios es una pieza fundamental en la estrategia de seguridad de la información, no obstante, el 73% utiliza mecanismos poco medibles o que no permiten reforzar, eficazmente, la concienciación de los usuarios.

OPERACIONES Y TECNOLOGÍAS DE SEGURIDAD

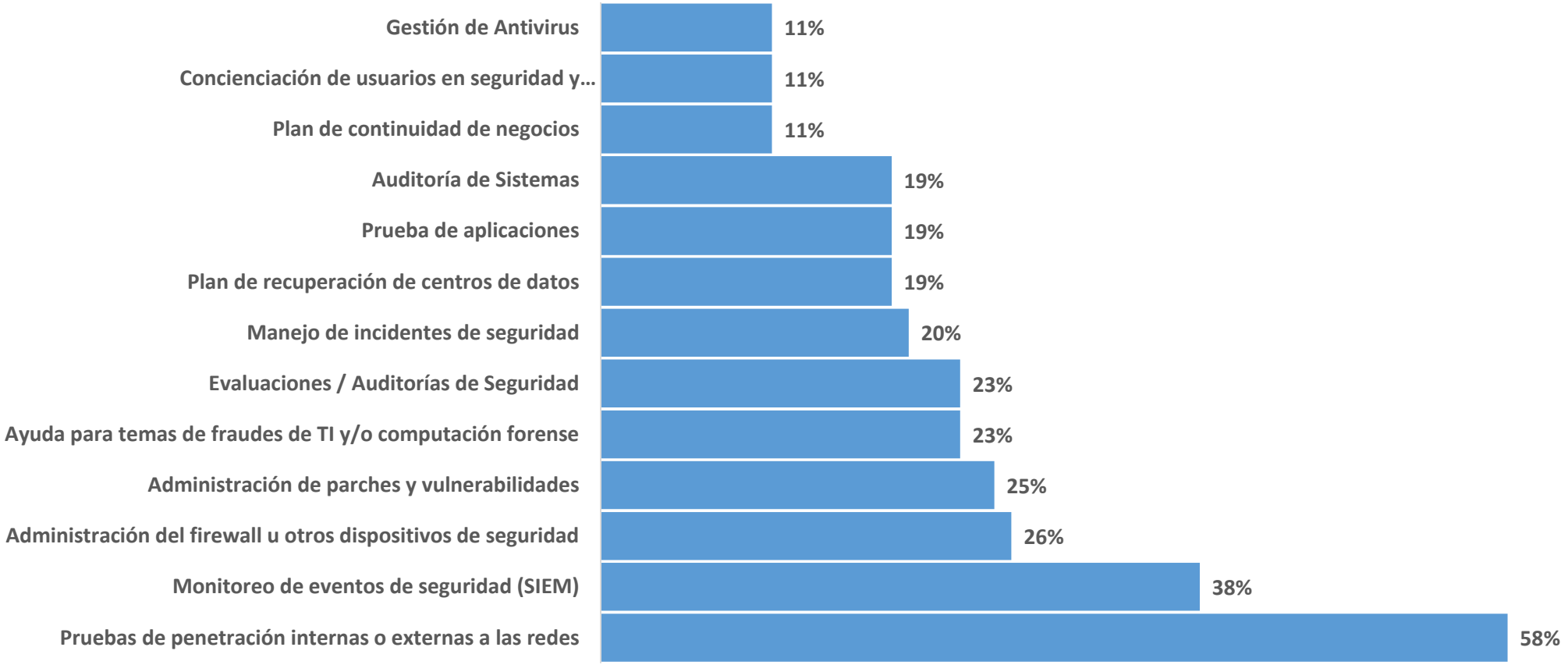
¿La estrategia de seguridad de información y ciberseguridad en la organización incluye software que incorporen técnicas de inteligencia artificial o "machine learning"?



Es un hecho que, cada vez se dispone de un mayor número de información tanto para la identificación de incidentes de seguridad, asi como para la toma de decisiones. El uso de nuevas tecnologías que nos ayuden a manejar ese volumen se vuelve crítico.

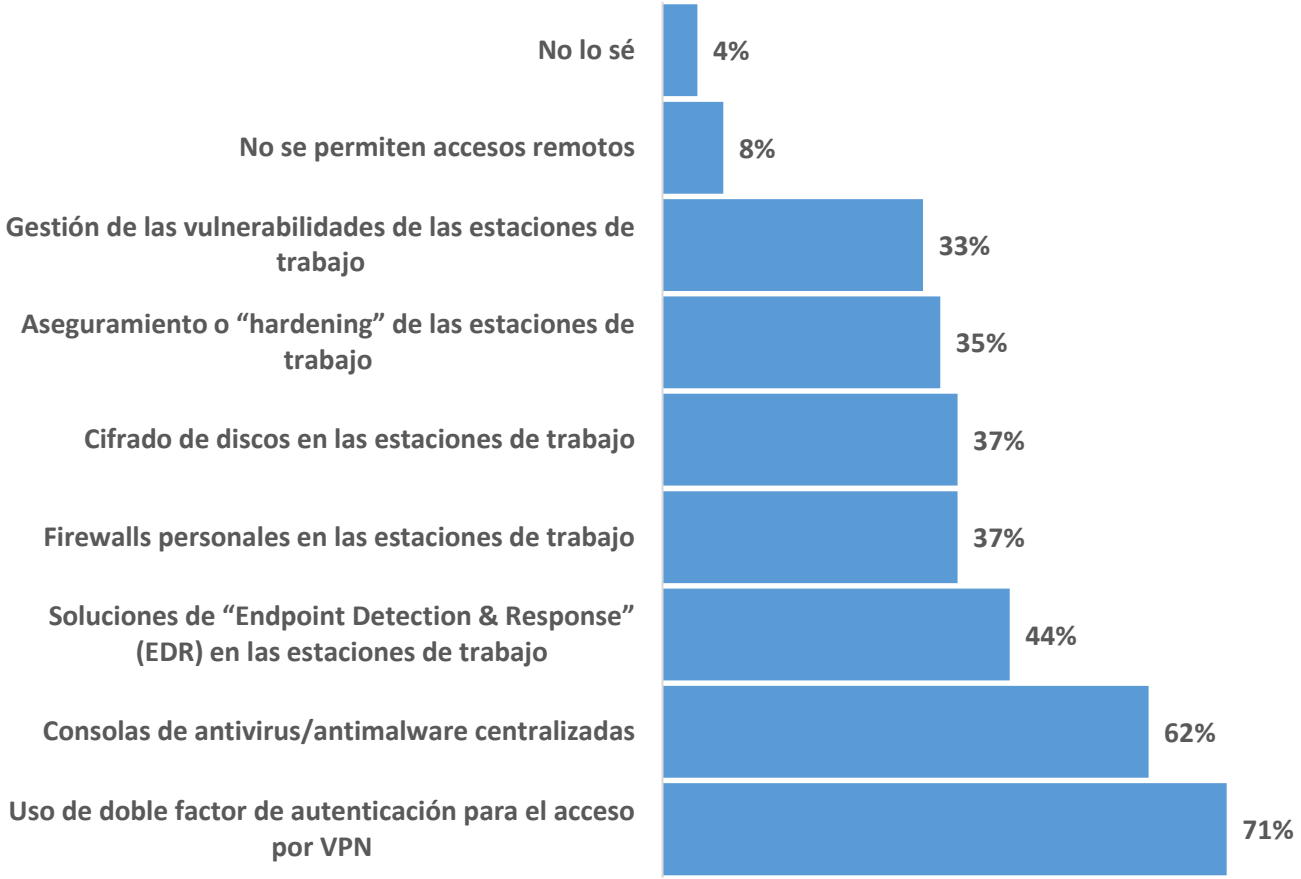
OPERACIONES Y TECNOLOGÍAS DE SEGURIDAD

¿Cuál de las siguientes actividades relacionadas con seguridad de información han sido o están siendo consideradas para tercerizar (“outsourcing”)?

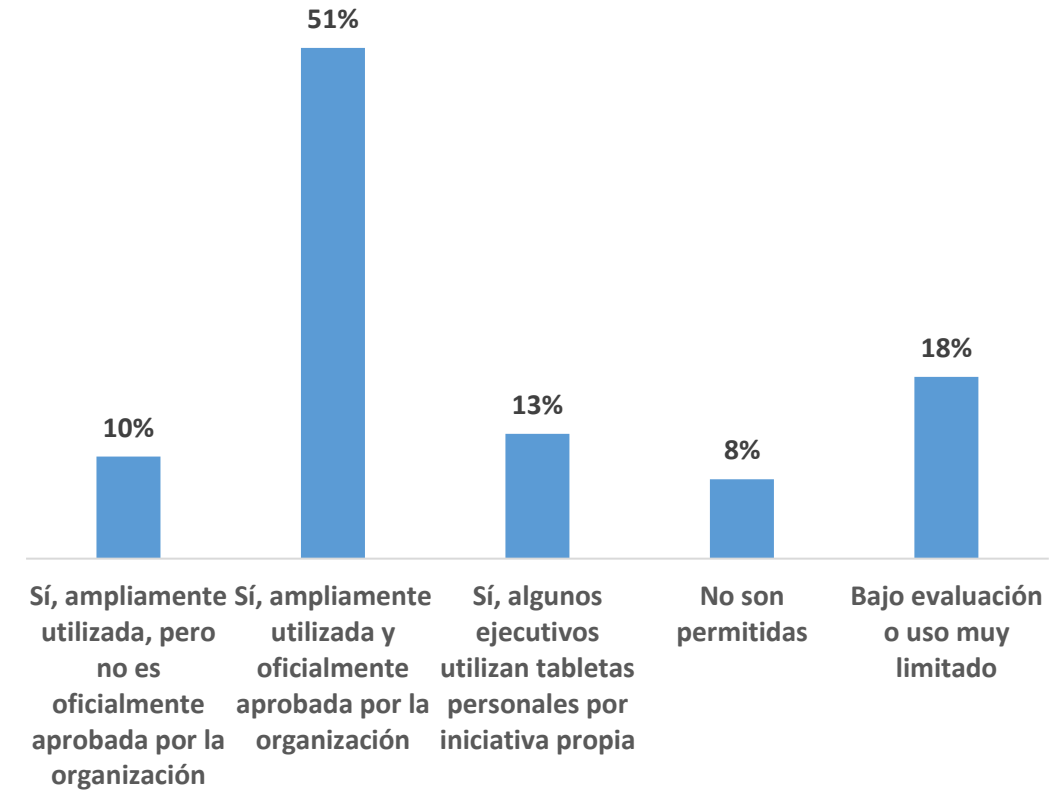


OPERACIONES Y TECNOLOGÍAS DE SEGURIDAD

¿En vista que el trabajo remoto se ha convertido en parte de muchas organizaciones, qué controles de seguridad ha implementado su organización para reducir los riegos relacionados a esta tecnología?

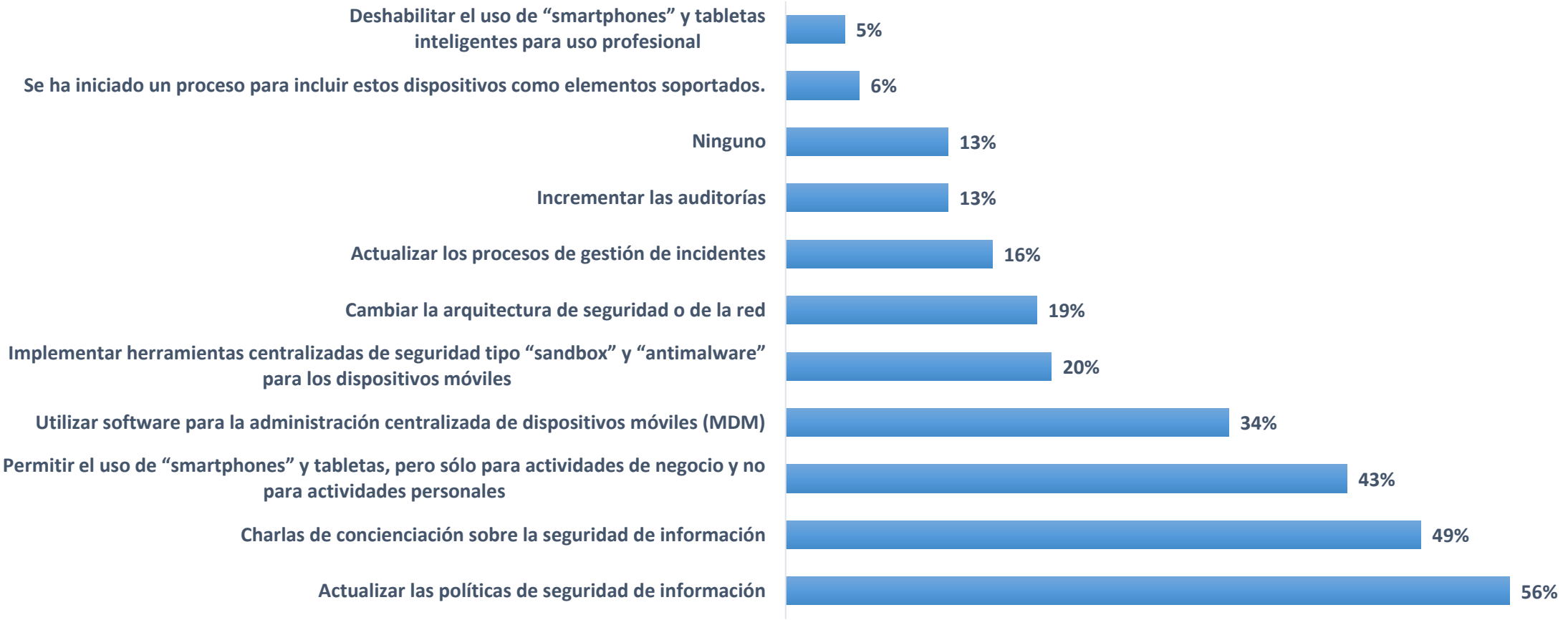


¿Actualmente en su organización se permite el uso de dispositivos móviles como teléfonos inteligentes ("smartphones") o tabletas ("tablets"), para actividades de negocio?



DISPOSITIVOS MÓVILES

¿Cuáles de los siguientes controles ha implementado su organización para mitigar los riesgos relacionados con el uso de dispositivos móviles por parte de los colaboradores (ejemplo, teléfonos inteligentes y tabletas)?

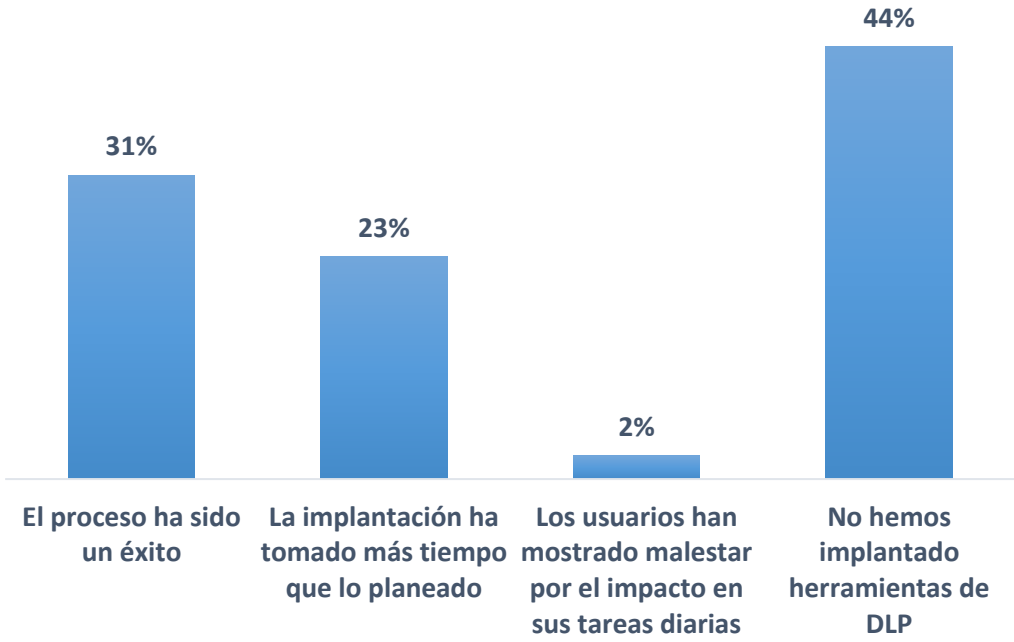


PRIVACIDAD DE DATOS

PRIVACIDAD DE DATOS

¿Qué acciones ha implementado su organización para mantener la adecuada gestión de los datos personales de clientes, colaboradores y proveedores?

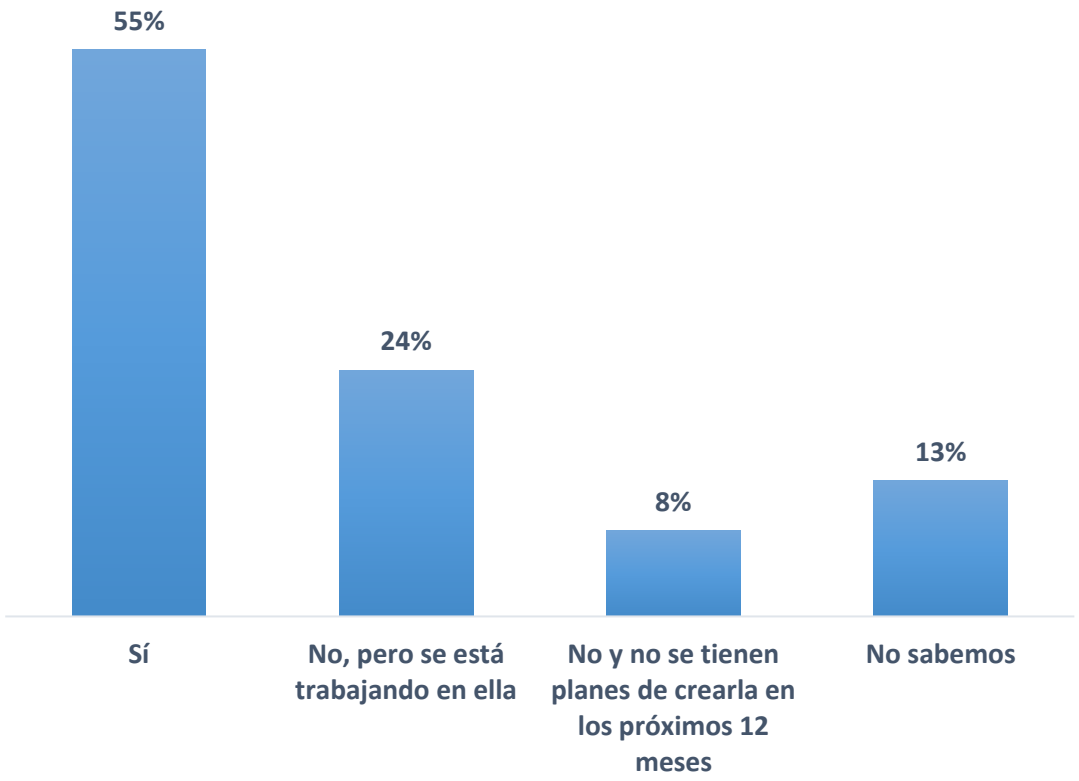
¿Con relación a la implementación de herramientas de Data Loss Prevention (DLP) o similares en su organización, cómo describiría usted dicho proceso?



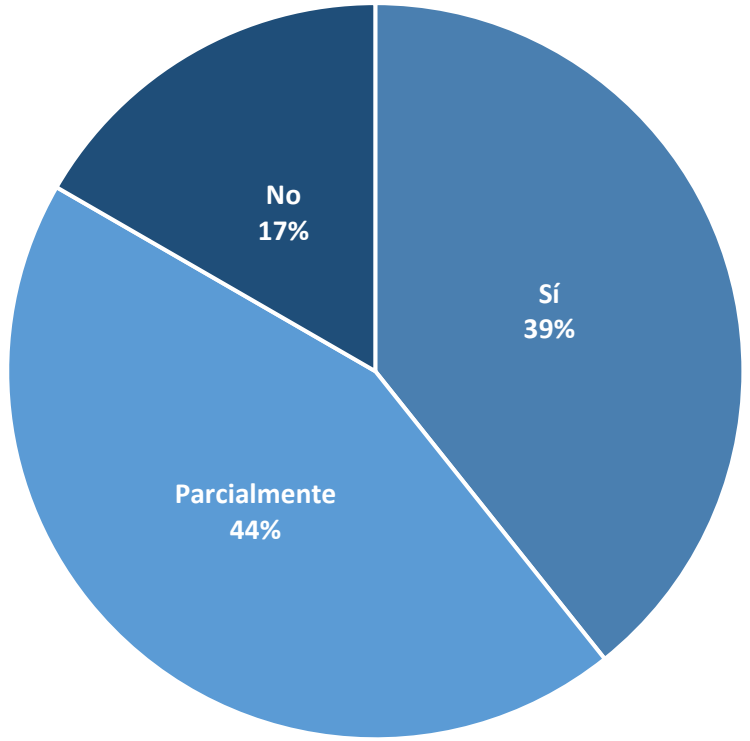
A pesar de que los datos personales son un activo de información relevante sólo un 31% cuenta con herramientas para monitorear la manipulación o robo de datos, incluyendo datos personales. Esta situación es más relevante ya que el 20% de los participantes indica no tener mecanismos o herramientas para la protección de dichos datos personales.

PRIVACIDAD DE DATOS

¿Existe alguna estrategia formal a nivel directivo, para establecer controles y procedimientos para proteger los datos personal de sus clientes?



¿Existe algún proceso para la clasificación de datos (público, confidencial, etc.) que permita definir los mecanismos de control para proteger los datos personales de los clientes?



CONTACTOS

Panamá y CARICOM

Antonio Ayala I.
aayala@riscco.com

Roberto Delgado
rdelgado@riscco.com

Rubén Fernández
rfernámdez@riscco.com

Guatemala, EL Salvador, Honduras, Nicaragua, Costa Rica

Maria Cristina Marroquín
mmarroquin@riscco.com

Asesor Externo

Dr. Modaldo Tuñón (Universidad Tecnológica de Panamá)
modaldotunon@gmail.com

riscco.com

Es una compañía regional independiente y dedicada de manera exclusiva ayudar a organizaciones a enfrentar sus desafíos en GRC (*Governance, Risk & Compliance*) y ESG (*Environmental, Social & Governance*); compuesta por profesionales con el conocimiento y credibilidad necesaria para traducir aspectos muy técnicos a un lenguaje simple y con sentido de negocio. Con catorce (14) años de haber iniciado operaciones, RISCCO cuenta en su cartera de clientes con compañías privadas e Instituciones del Estado en la región líderes en su ramo.