

Datasec

Estado de la Ciberseguridad en Uruguay.

EMPRESAS Y PERSONAS

Encuesta 2024-2025

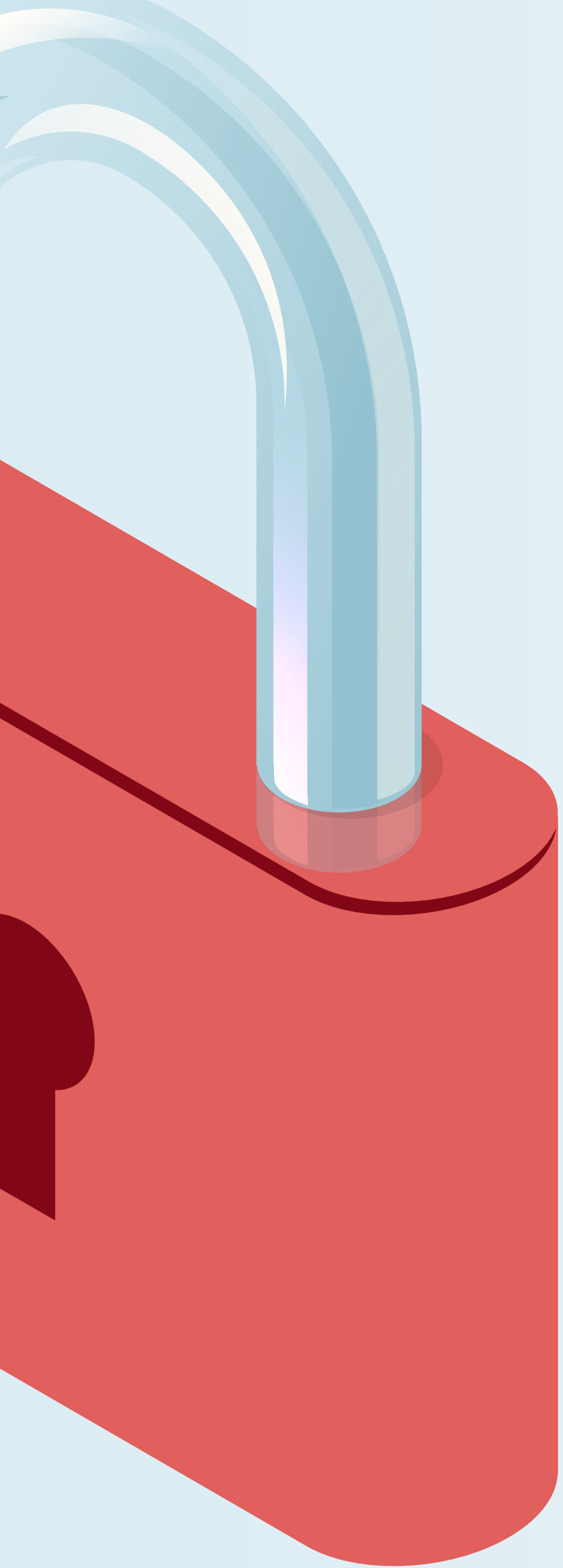
GRUPO
RADAR
INTELIGENCIA DE MERCADO



Introducción

En 2025, la ciberseguridad se ha consolidado como una prioridad global, impactando profundamente a individuos, empresas y gobiernos. El Informe de Riesgos Globales 2025 del Foro Económico Mundial resalta la vulnerabilidad del ciberespacio como una de las principales amenazas a corto plazo, impulsada por factores como las tensiones geopolíticas, la rápida evolución de las tecnologías emergentes y el creciente nivel de sofisticación de la ciberdelincuencia.

En Uruguay, los datos de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Agesic) evidencian la magnitud del problema: en 2024 se detectaron y respondieron más de 14.000 incidentes de ciberseguridad, lo que representa un alarmante incremento del 65% respecto al año anterior. Este crecimiento refleja la urgencia de reforzar las estrategias de prevención y concienciación tanto a nivel empresarial como individual.



Un enfoque integral: Empresas e individuos en la mira

Desde 2016, Datasec ha colaborado con Grupo Radar para desarrollar estudios específicos sobre ciberseguridad en Uruguay. Inicialmente, estos informes se centraron en la población general, abordando la percepción y comportamiento de los usuarios en materia de seguridad digital. En 2019, el enfoque se trasladó hacia las empresas, evaluando su madurez y preparación ante desafíos cibernéticos. Sin embargo, reconociendo la creciente amenaza que enfrentan tanto organizaciones como individuos, la edición 2024 de la Encuesta de Ciberseguridad amplió nuevamente su alcance para incluir a los usuarios individuales. Tácticas como el phishing, la suplantación de identidad y los fraudes financieros generan un impacto significativo en la vida cotidiana de los usuarios.

El estudio actual, basado en una muestra representativa de 600 empresas y miles de usuarios individuales, analiza tanto la preparación de las organizaciones como la percepción y el comportamiento de los internautas uruguayos en materia de ciberseguridad.

Hallazgos clave: Una brecha preocupante

Los resultados de la encuesta exponen una preocupante discrepancia entre la conciencia sobre los riesgos y la adopción de medidas efectivas de protección:

- **El 77% de las empresas** no cuenta con políticas documentadas de ciberseguridad.
- **El 47% de las empresas** no ofrece formación ni programas de concientización en ciberseguridad a sus empleados.
- **El 80% de las medianas y grandes empresas** percibe que sus clientes no consideran la ciberseguridad una prioridad.
- **El 32% de los usuarios** de internet no tiene instalado un antivirus.
- **Menos de la mitad de las personas** que tienen computadora realizan respaldos regulares de sus datos en la nube o dispositivos externos.

- **1 de cada 20 usuarios** de internet perdió dinero debido a fraudes en línea en el último año, lo que, considerando la población de Uruguay de aproximadamente 3.5 millones de personas, equivale a cerca de 175.000 uruguayos afectados. Además, el 2% de los usuarios indicó haber perdido información personal como resultado de estos fraudes, lo que representa aproximadamente 70.000 personas.

Estos datos reflejan un desafío crítico: aunque la transformación digital avanza rápidamente, la seguridad digital sigue sin ser percibida como una prioridad en muchos sectores.

**Más allá de
la tecnología:**

**Un cambio cultural
necesario**

La ciberseguridad no puede abordarse únicamente desde una perspectiva técnica; es imprescindible promover un cambio cultural que fomente la educación en seguridad digital y la adopción de prácticas seguras tanto a nivel personal como organizacional. La concienciación y la capacitación son claves para construir un entorno digital más seguro y resiliente en el Uruguay del presente y del futuro.

Confiamos en que este análisis sirva como una herramienta valiosa para impulsar el cambio y guiar a empresas e individuos hacia una protección efectiva frente a los crecientes desafíos del mundo digital.

Ing. Reynaldo C. de la Fuente
Socio Director - Datasec
www.datasec-soft.com

Datasec

Encuesta

Empresas

Datasec



Ficha técnica

	UNIVERSO	MUESTRA
TOTAL	184.000	600
Micros y pequeñas	175.382	351
Medianas y grandes	8.618	249
Industria	25.906	100
Comercio	61.761	250
Servicios	96.333	250
Montevideo + ZM	102.302	300
Interior	81.697	300

Se aplicó una encuesta telefónica a una muestra aleatoria de 600 empresas, representativa del universo de todas las empresas uruguayas.

Se definieron cuotas según tres criterios:

Zona geográfica: Montevideo + zona metropolitana/Interior.

Tamaño de empresa: micro/pequeñas y medianas/grandes.

Sector de actividad: Industria, Comercio y Servicios. Se excluyó el sector primario del estudio, por tratarse de un universo demasiado reducido.

Se sobre-muestrearon los segmentos con universos más reducidos: industria, y empresas medianas y grandes. A efectos del procesamiento de los resultados generales se le dio a cada segmento su peso real en el universo de empresas.

El margen de error máximo para la muestra general es de ± 4.0 , para un nivel de confianza del 95%.

Las sumas pueden no dar 100% por errores de redondeos.

El relevamiento de campo se realizó en el transcurso de noviembre y diciembre 2024.

Referencia de bases

Empresas que tienen página web, venden por internet y/o para quienes el mail es un instrumento importante en su empresa.

Base 1

Si la empresa tiene un responsable de la Ciberseguridad.

Base 2

Empresas medianas y grandes, que tienen página web, venden por internet y/o para quienes el mail es un instrumento importante en su empresa.

Base 3

Empresas medianas y grandes.

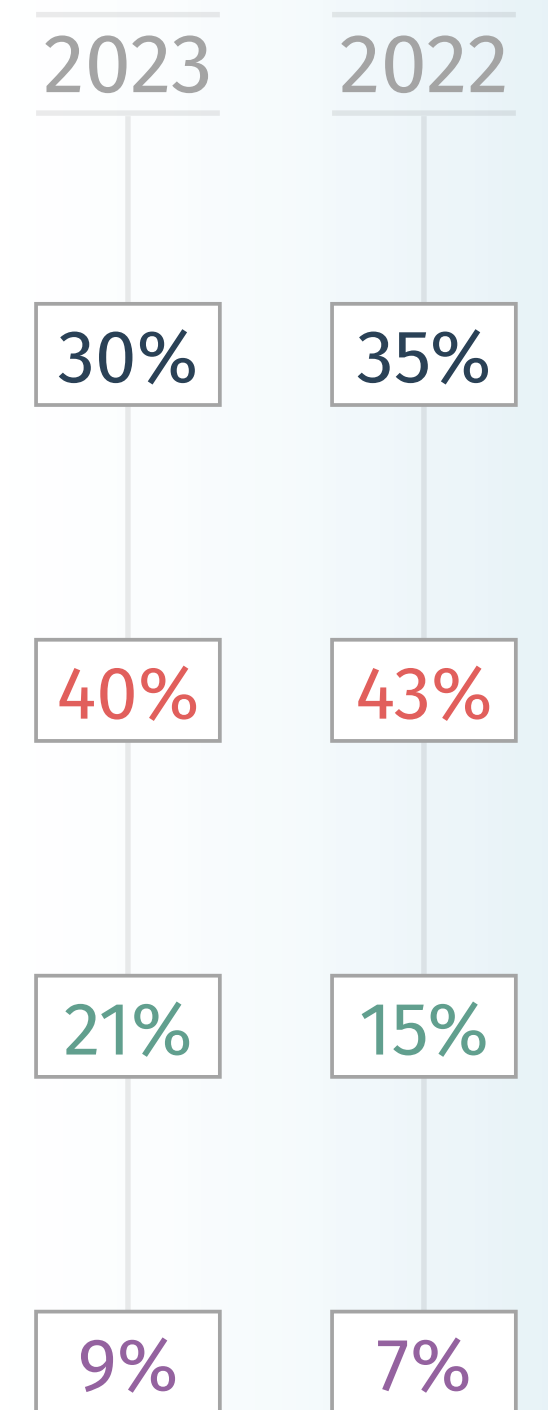
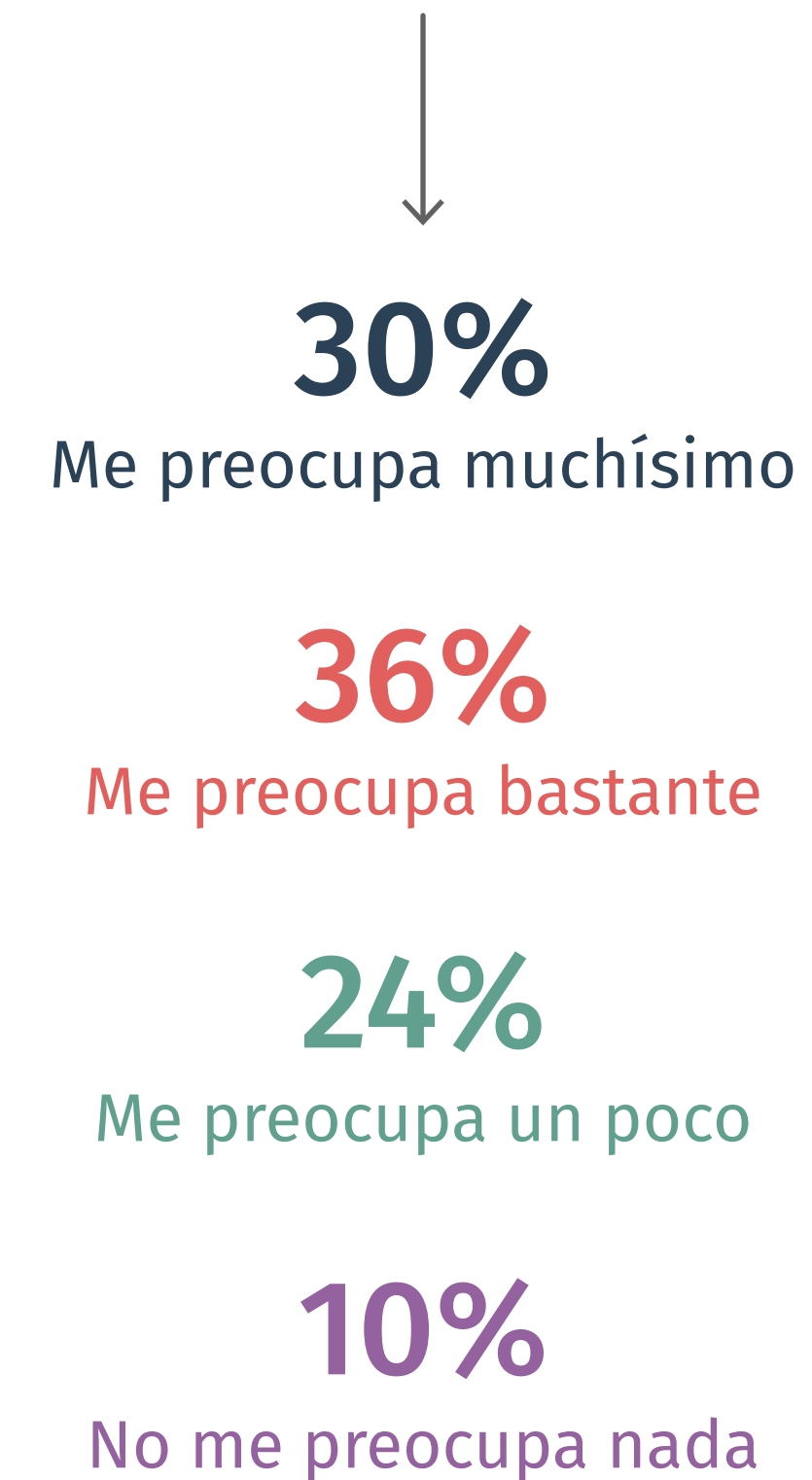
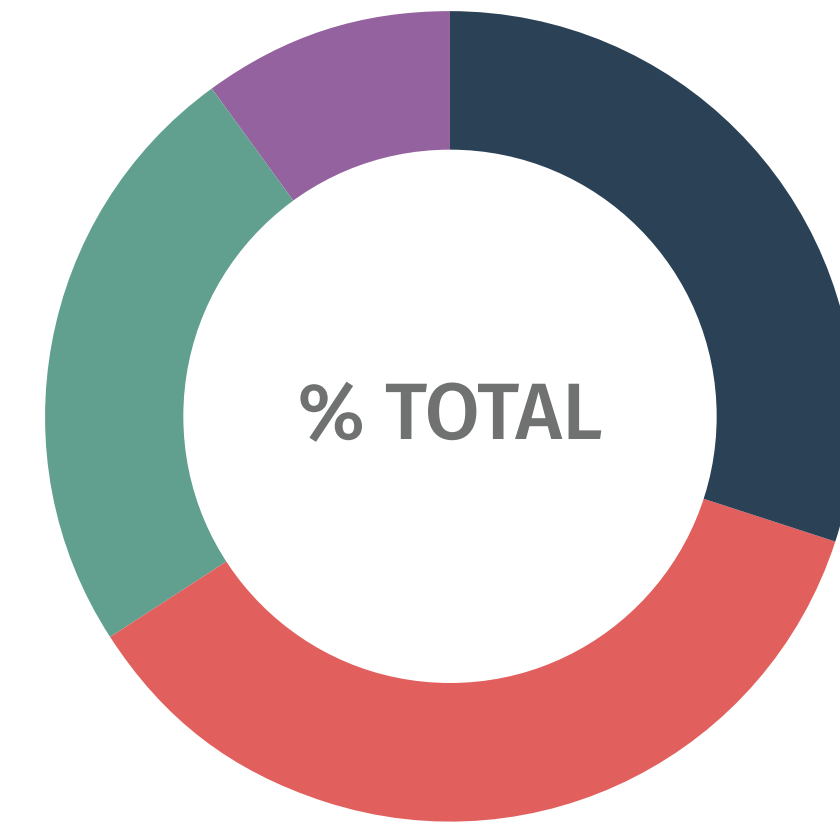
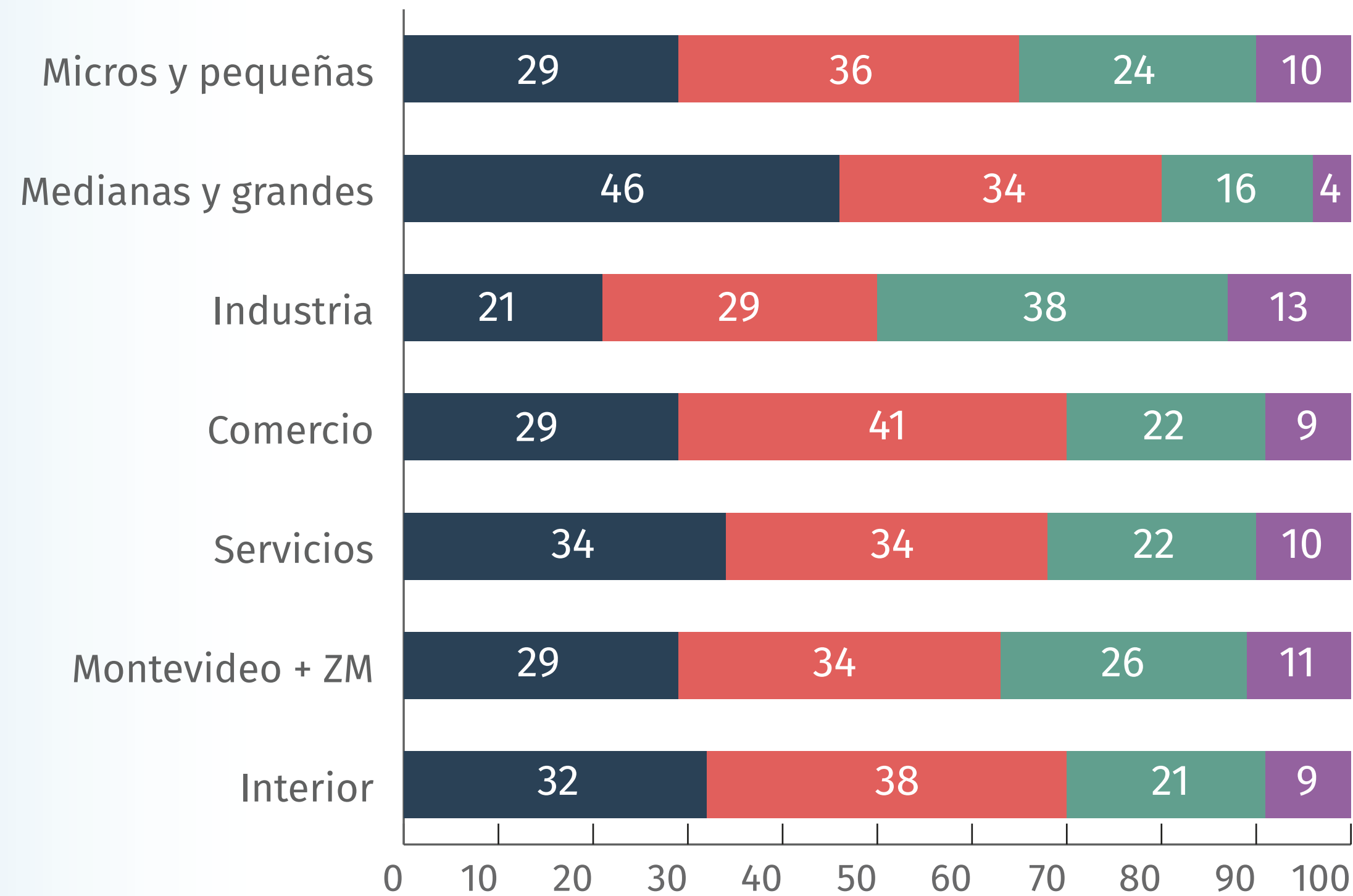
Base 4

¿Cuánto le preocupa a su empresa los incidentes en seguridad de información?

Ejemplo: virus, hackeos, correos fraudulentos, robos o secuestros de información.

Base 1

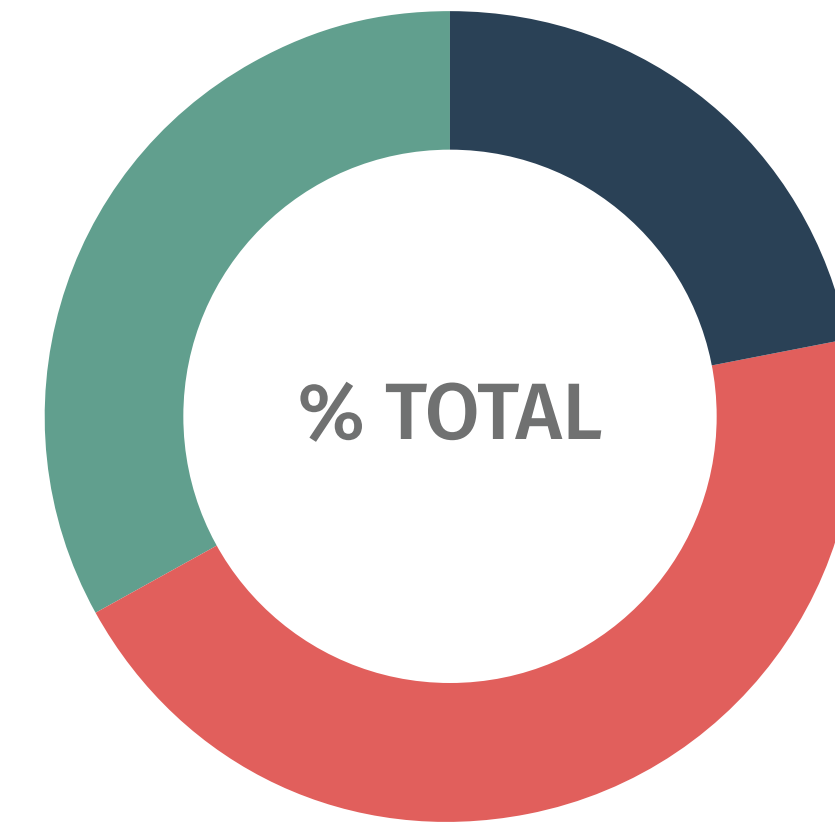
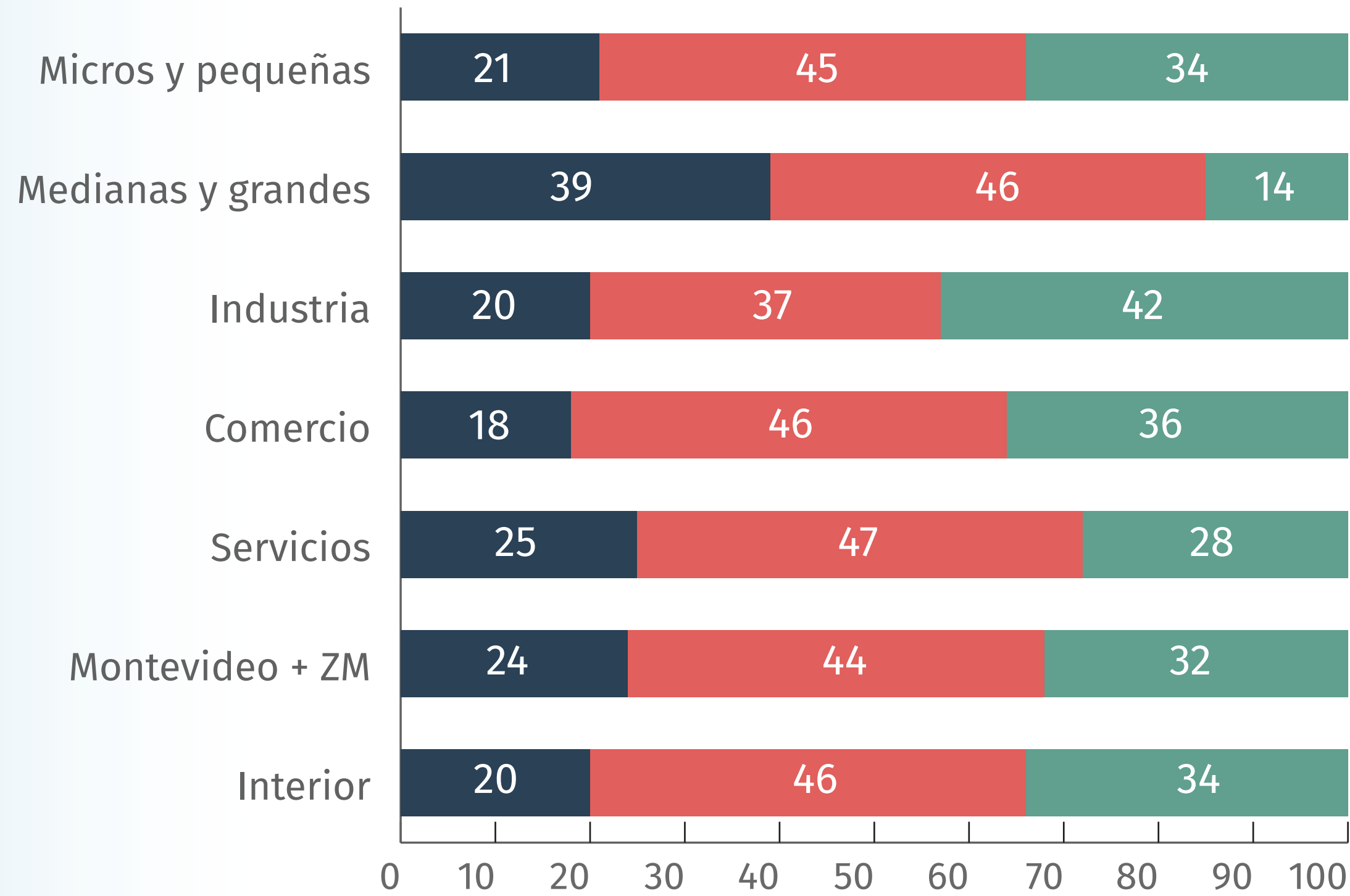
- Me preocupa muchísimo
- Me preocupa bastante
- Me preocupa un poco
- No me preocupa nada



¿Considera que su empresa ha tomado suficientes medidas para no ser víctima de incidentes de Ciberseguridad?

Base 1

● Sí, completamente
 ● Sí, parcialmente
 ● No
 ● No sabe



↓

22%

Sí, completamente

45%

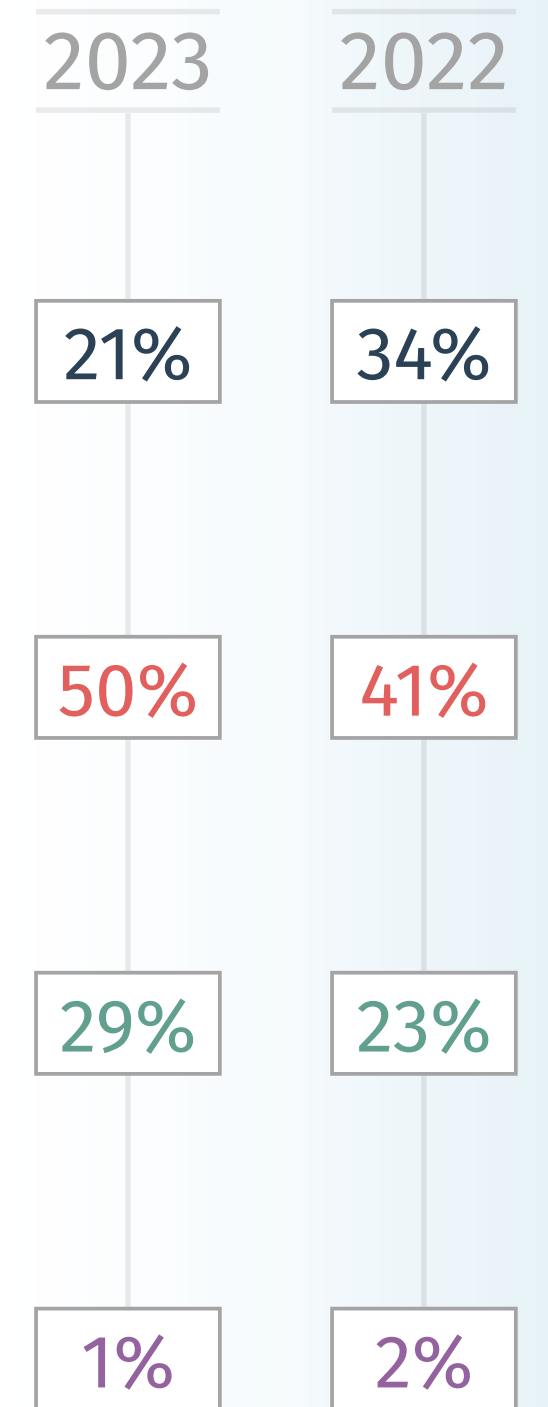
Sí, parcialmente

33%

No

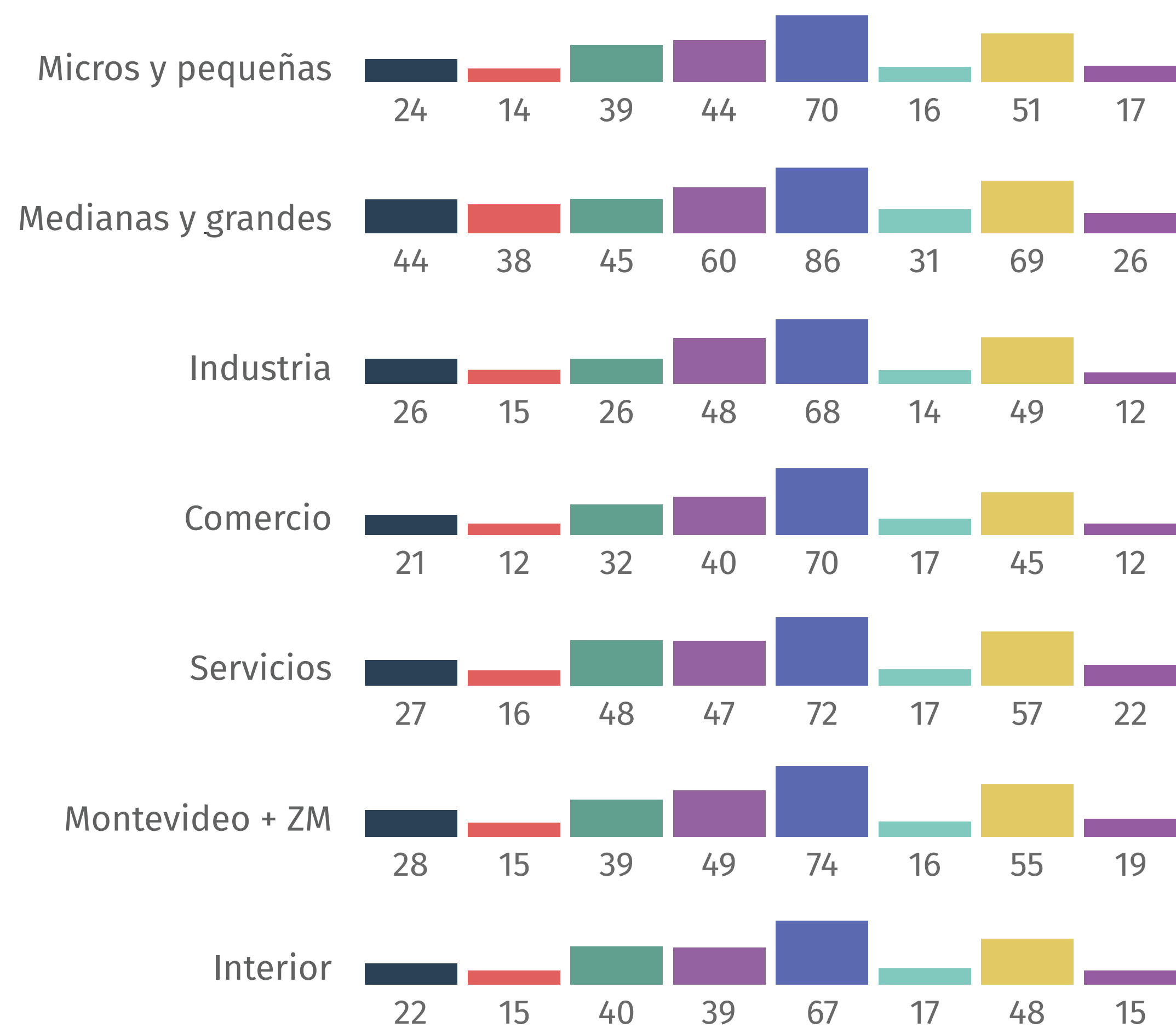
0%

No sabe



¿Qué controles de Ciberseguridad ha implementado?

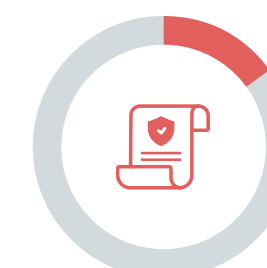
Base 1



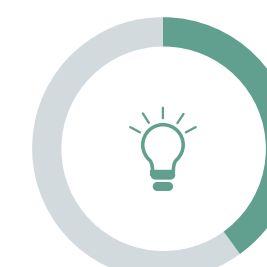
Designaron un responsable de Ciberseguridad
25%



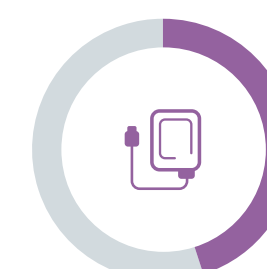
Cuentan con políticas de Ciberseguridad
15%



Concientizan a sus colaboradores
40%



Respaldan información en un sitio externo
45%



Cuentan con Antivirus
71%



Encriptan sus equipos portables
16%



Filtración de correos basura y fraudulentos
52%



2º Factor de autenticación para el trabajo remoto, toquen o app
17%

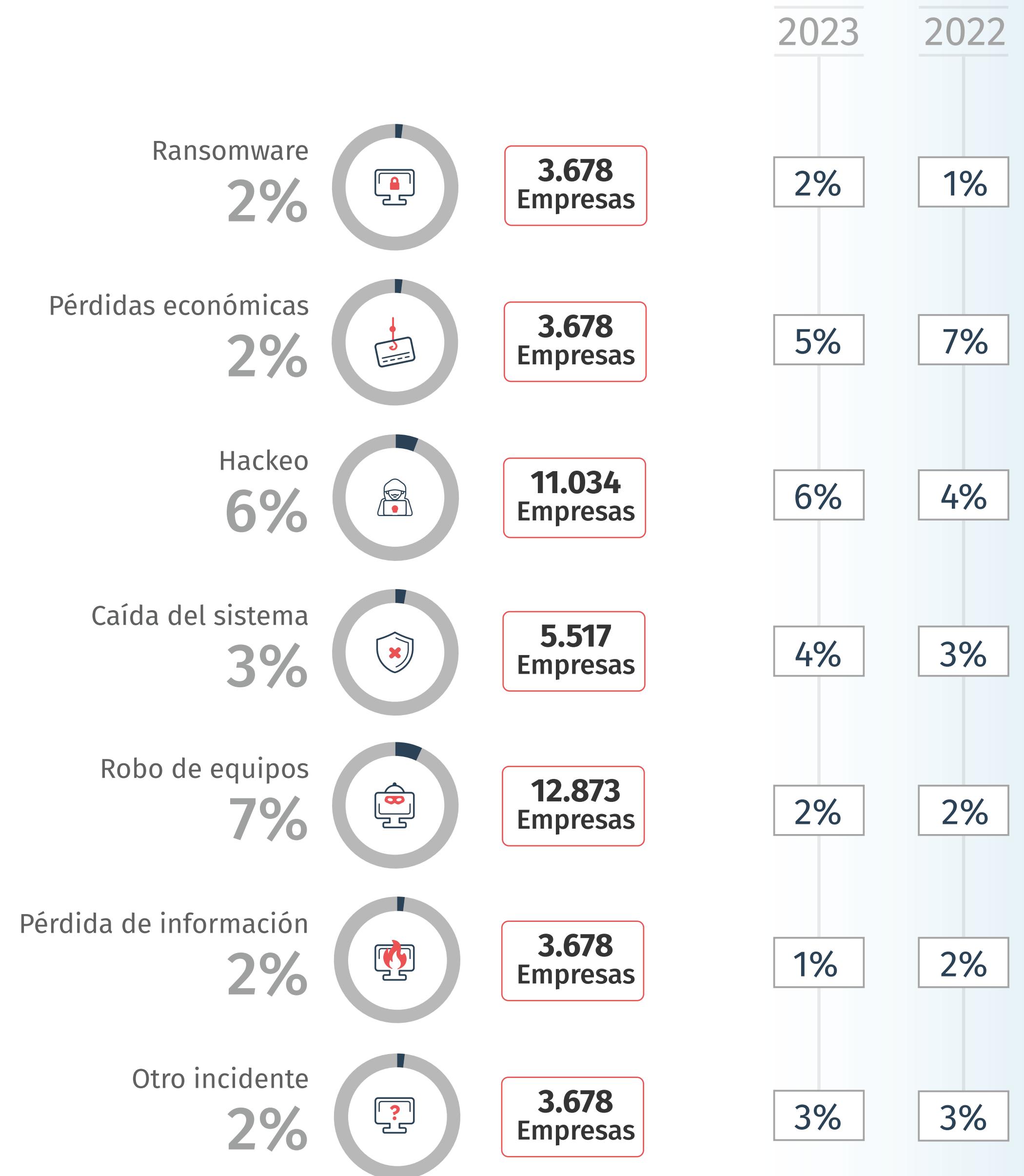
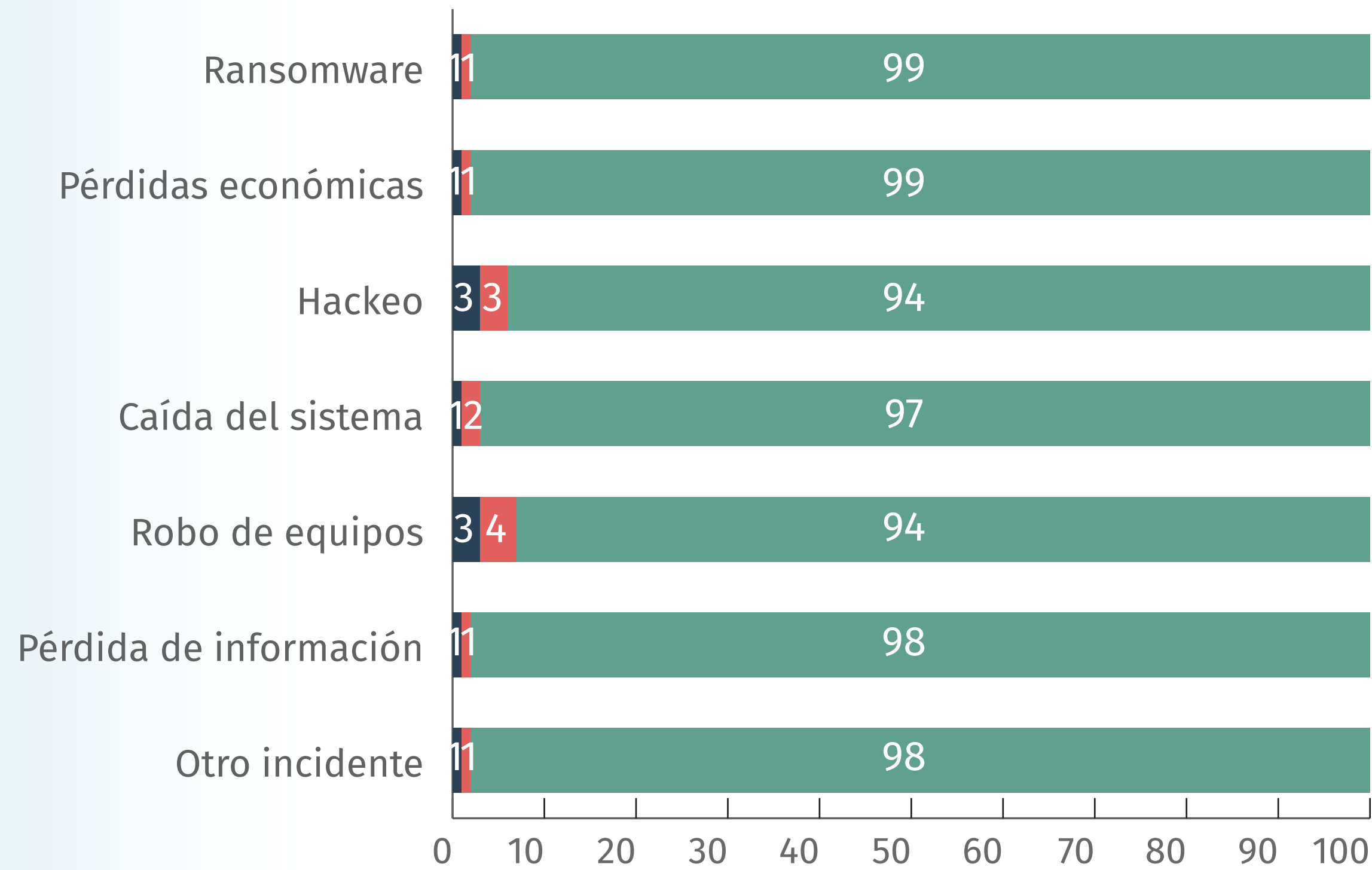


	2023	2022
Designaron un responsable de Ciberseguridad	25%	28%
Cuentan con políticas de Ciberseguridad	17%	19%
Concientizan a sus colaboradores	44%	47%
Respaldan información en un sitio externo	55%	53%
Cuentan con Antivirus	83%	81%
Encriptan sus equipos portables	26%	30%
Filtración de correos basura y fraudulentos	62%	59%
2º Factor de autenticación para el trabajo remoto, toquen o app	14%	32%

¿Su empresa ha sufrido alguno de estos incidentes en el último año?

Base 1

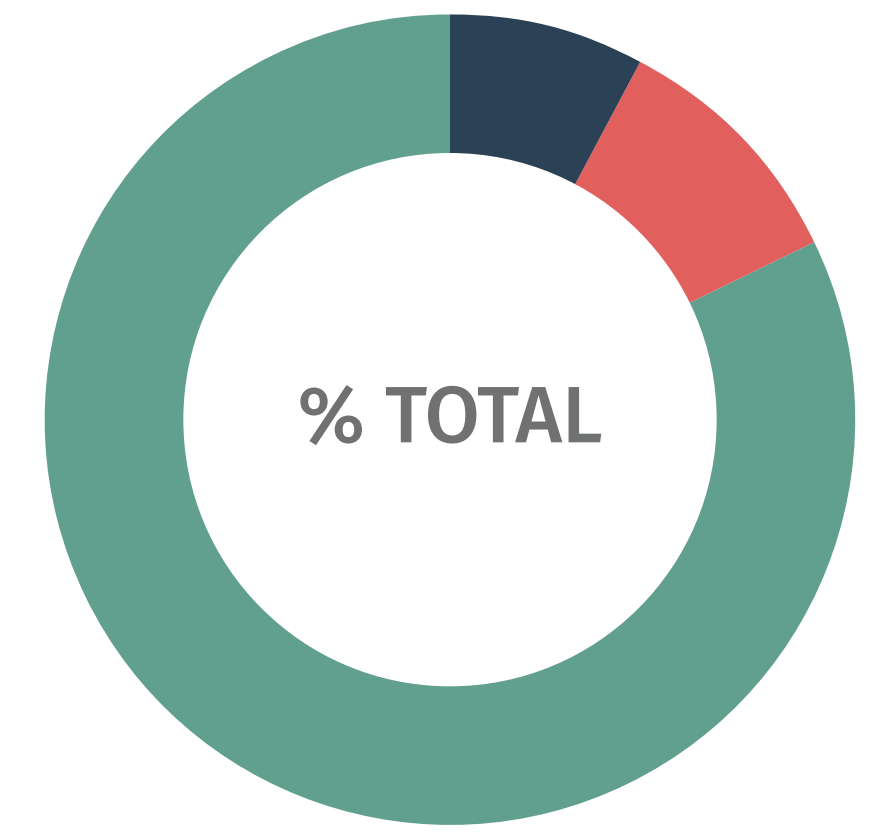
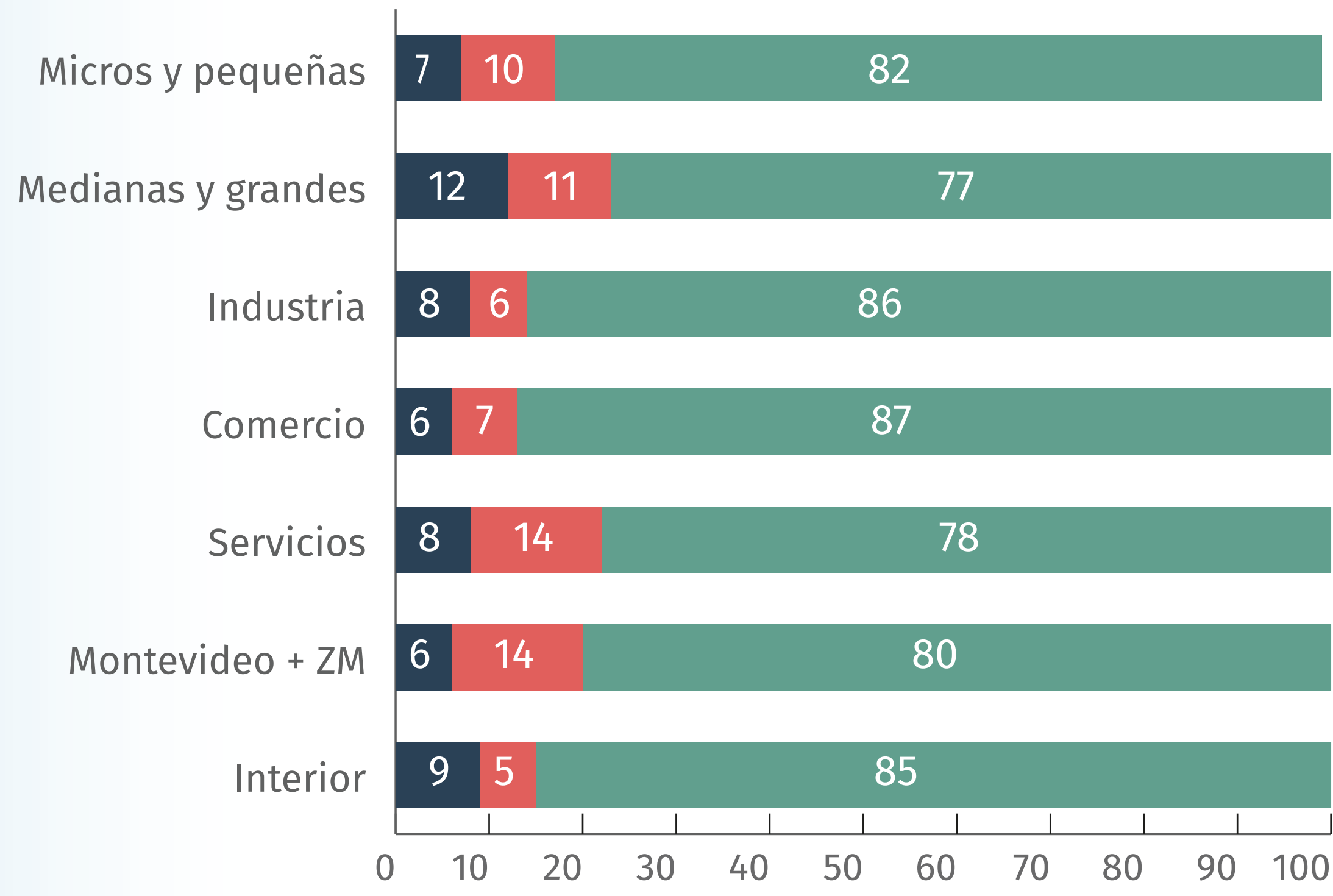
● Sí, y causó daños
 ● Sí, pero no causó daños
 ● No



¿Conoce alguna empresa que haya tenido algún incidente grave de Ciberseguridad el último año pero que no haya sido publicado en la prensa?

Base 1

● Sí, más de una ● Sí, una ● Ninguna

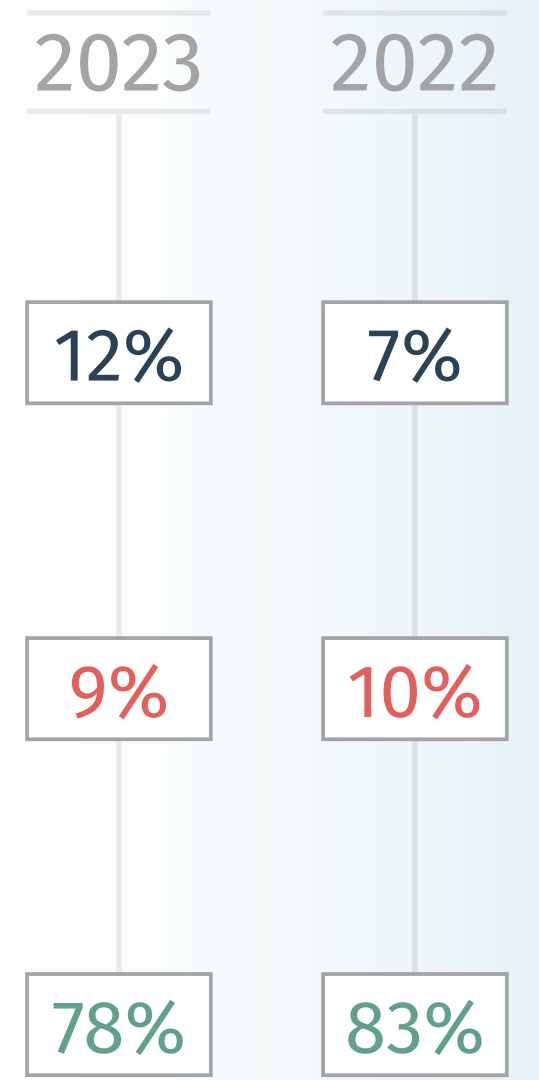


↓

8%
Sí, más de una

10%
Sí, una

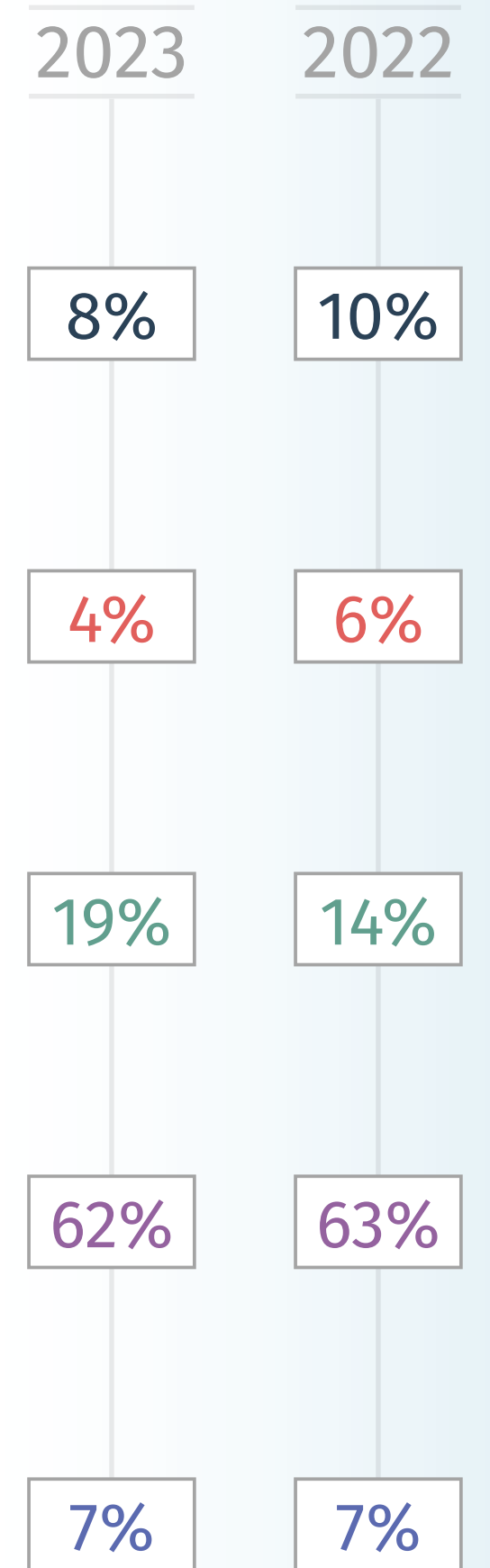
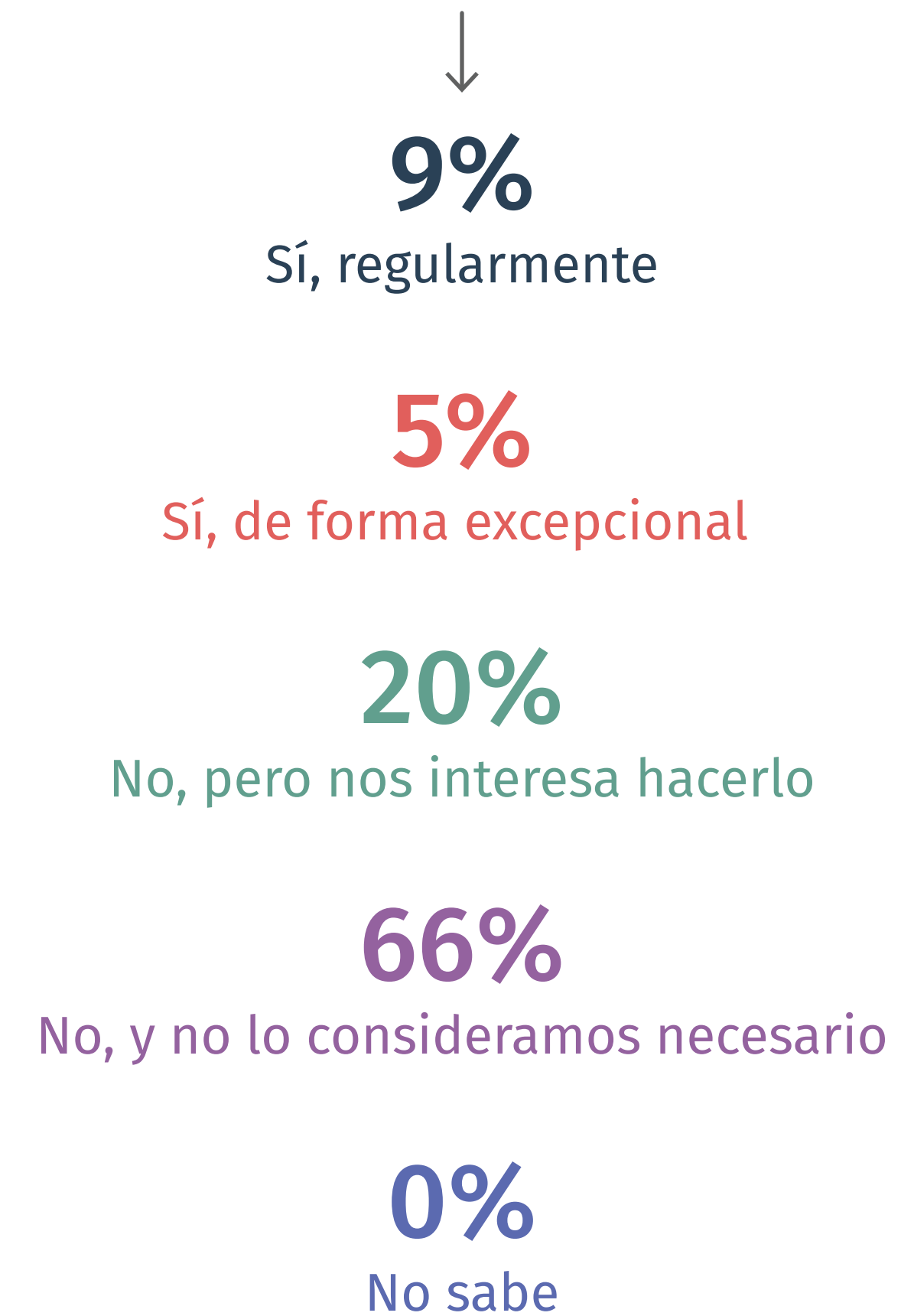
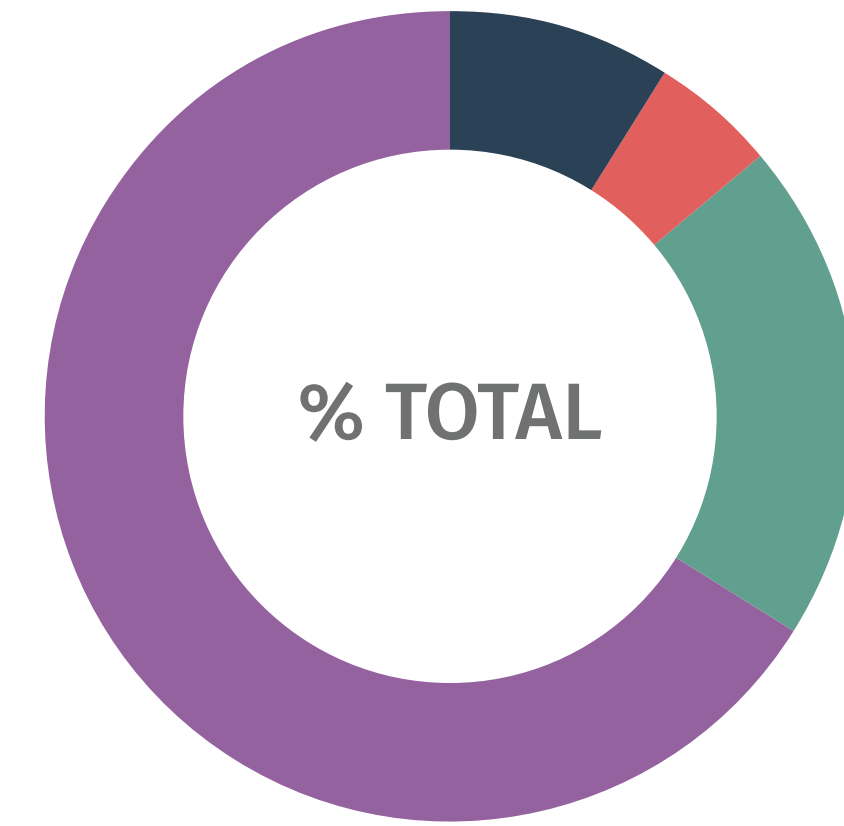
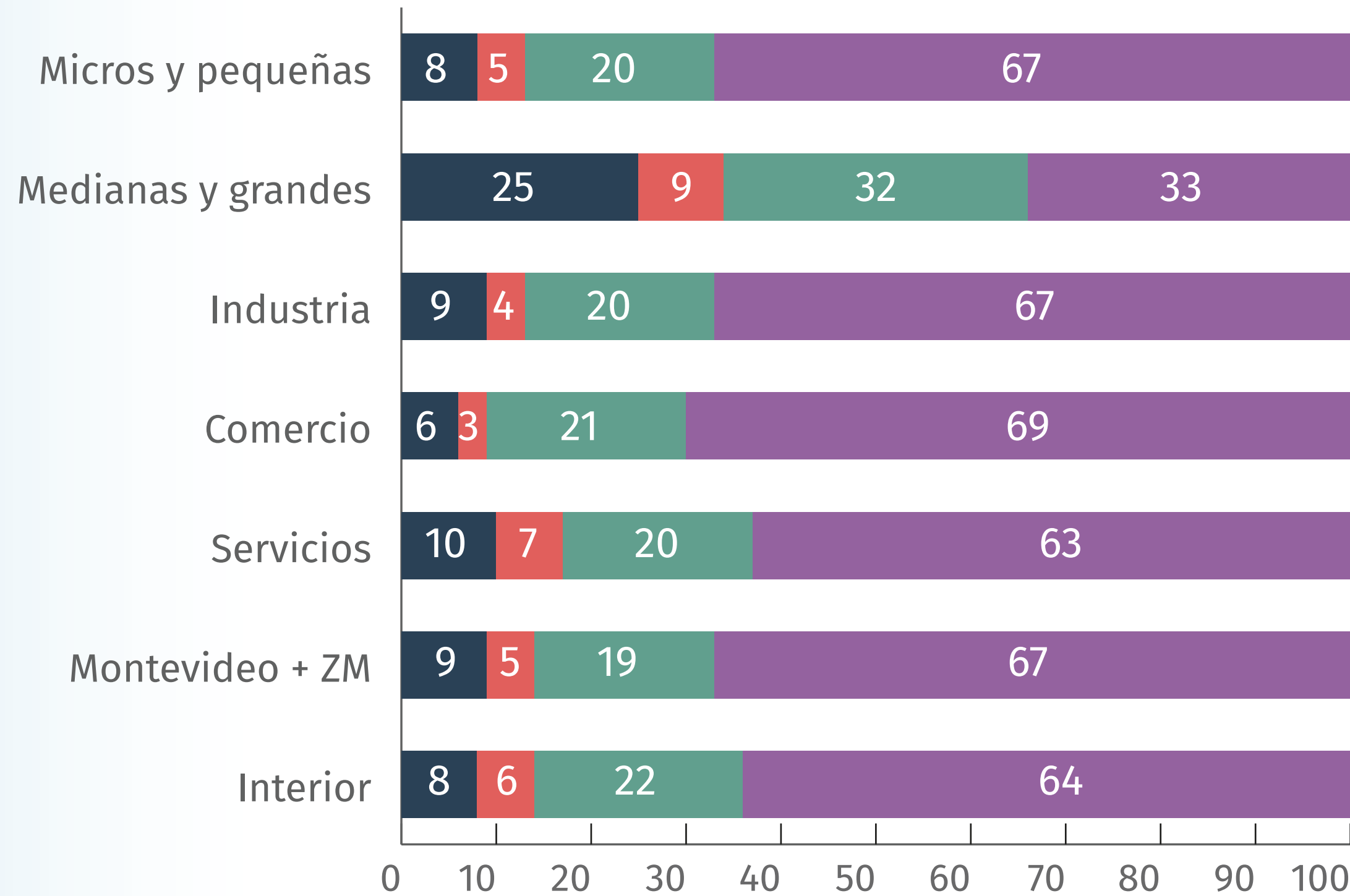
82%
Ninguna



¿Se ha realizado algún tipo de evaluación del estado de su Ciberseguridad?

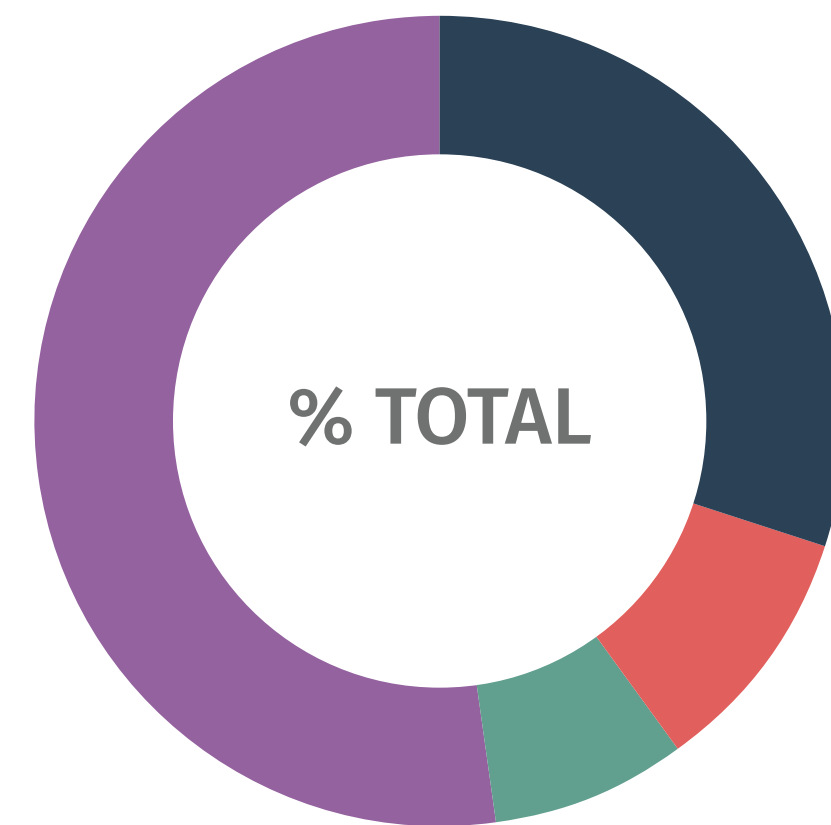
Base 1

- Sí, regularmente
- Sí, de forma excepcional
- No, pero nos interesa hacerlo
- No, y no lo consideramos necesario
- No sabe



¿La empresa ha sido sometida a un hacking ético o escaneo de vulnerabilidad para evaluar su seguridad?

En sitios web, mails y aplicaciones expuestas a Internet, que contestaron “Sí, regularmente” en la respuesta anterior.



- Sí, regularmente
- Sí, de forma excepcional
- No, pero nos interesa hacerlo
- No, y no lo consideramos necesario

30%
Sí, regularmente

10%
Sí, de forma excepcional

8%
No, pero nos interesa hacerlo

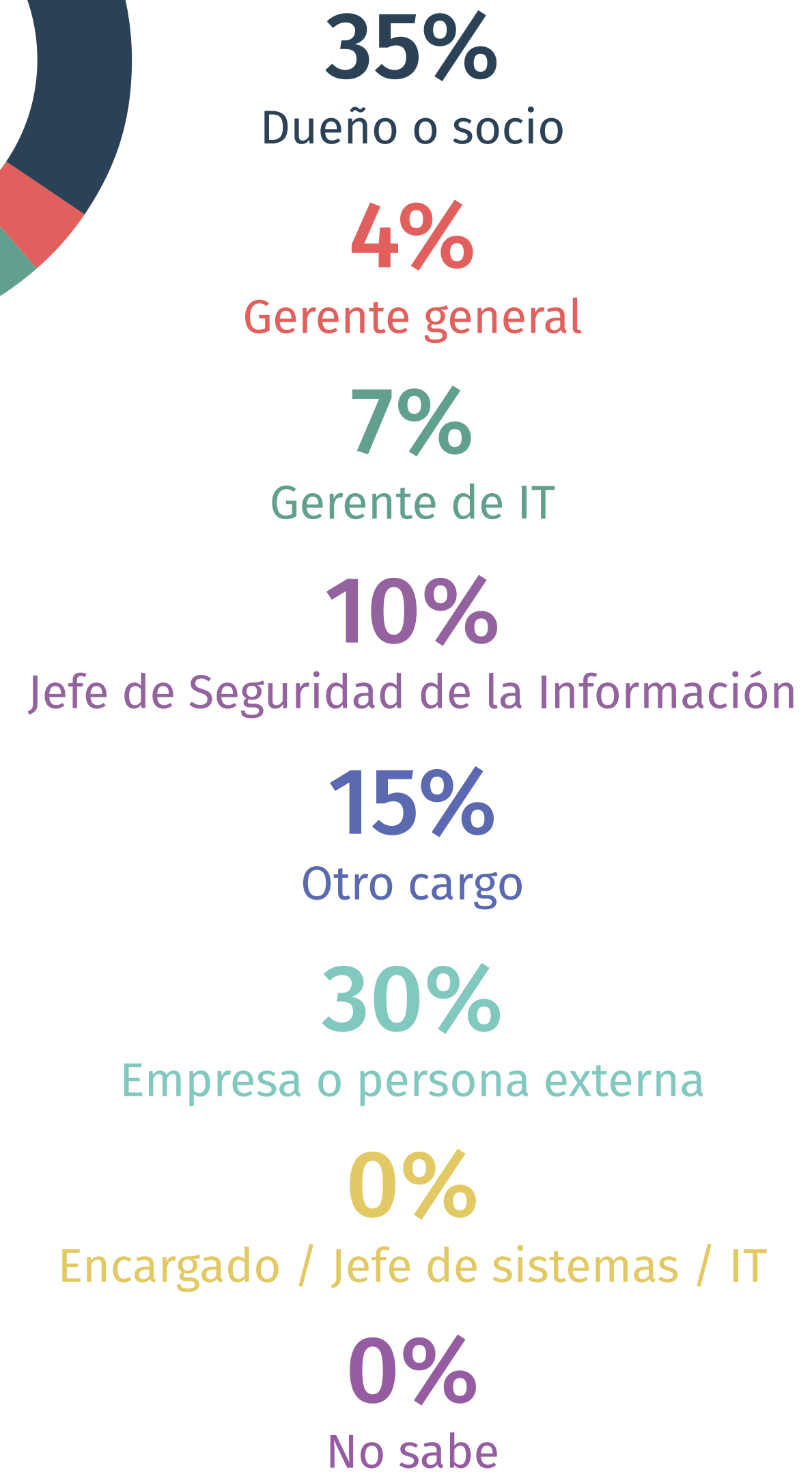
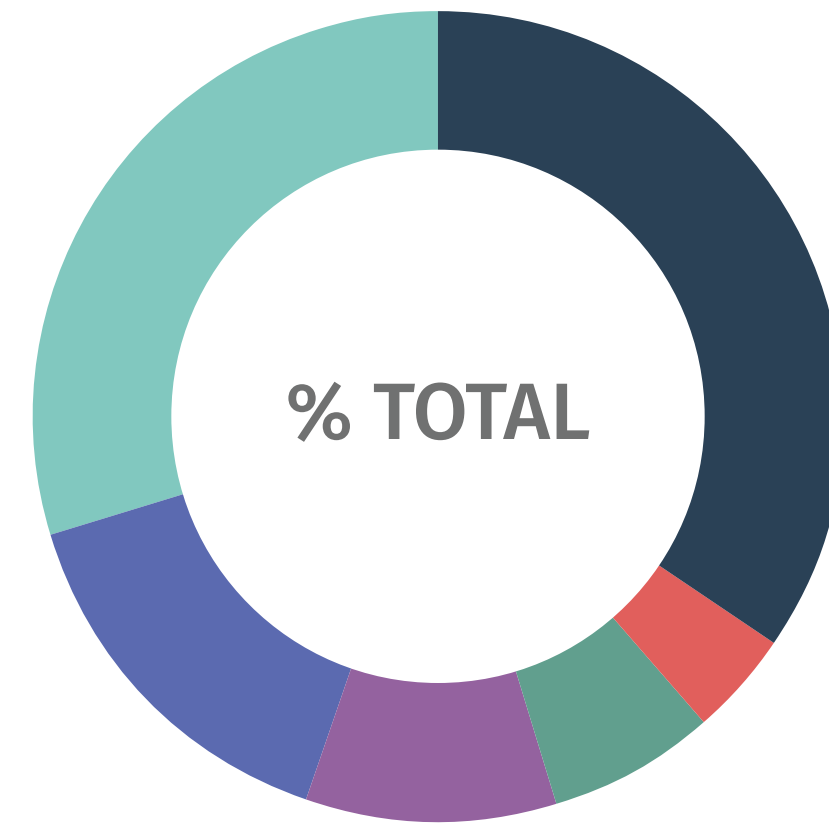
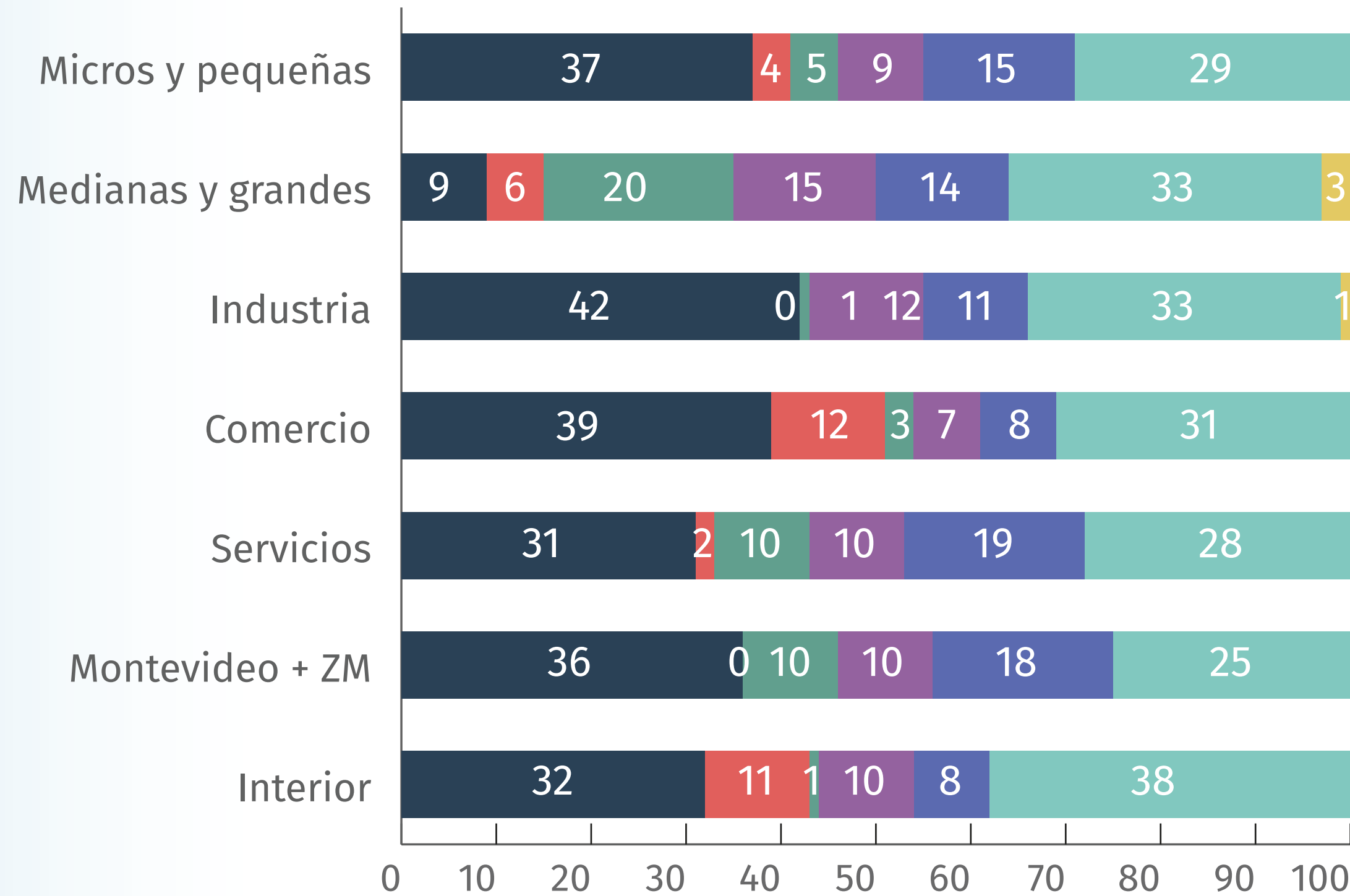
52%
No, y no lo consideramos necesario



¿Quién es el/la responsable de la Ciberseguridad?

Base 2

- Dueño o socio
- Gerente general
- Gerente de IT
- Jefe de Seguridad de la Información
- Otro cargo
- Empresa o persona externa
- Encargado/Jefe de sistemas/IT
- No sabe

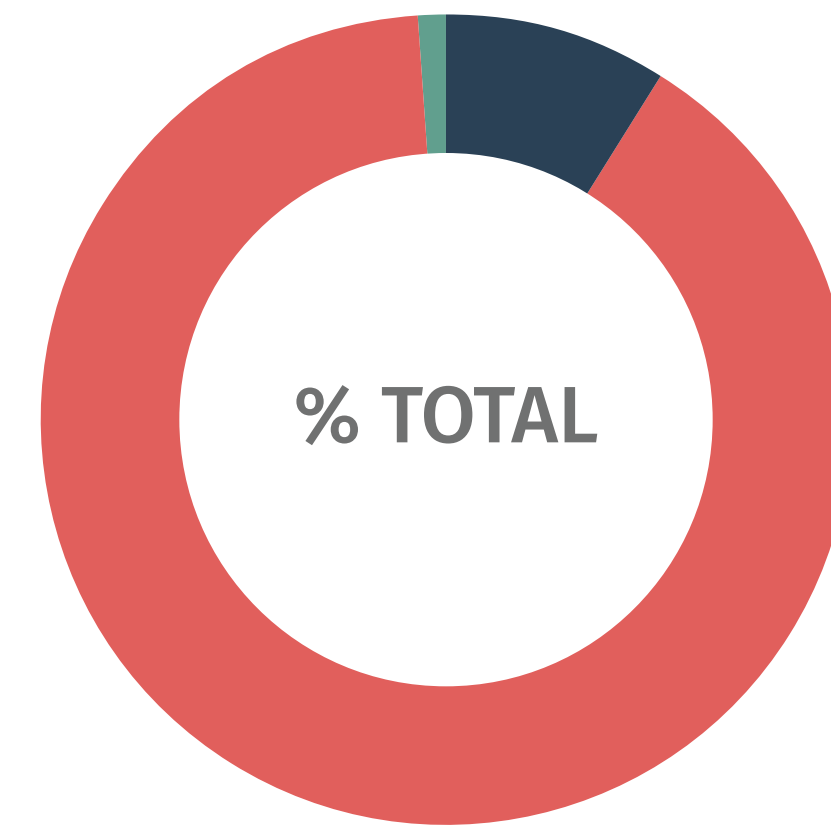
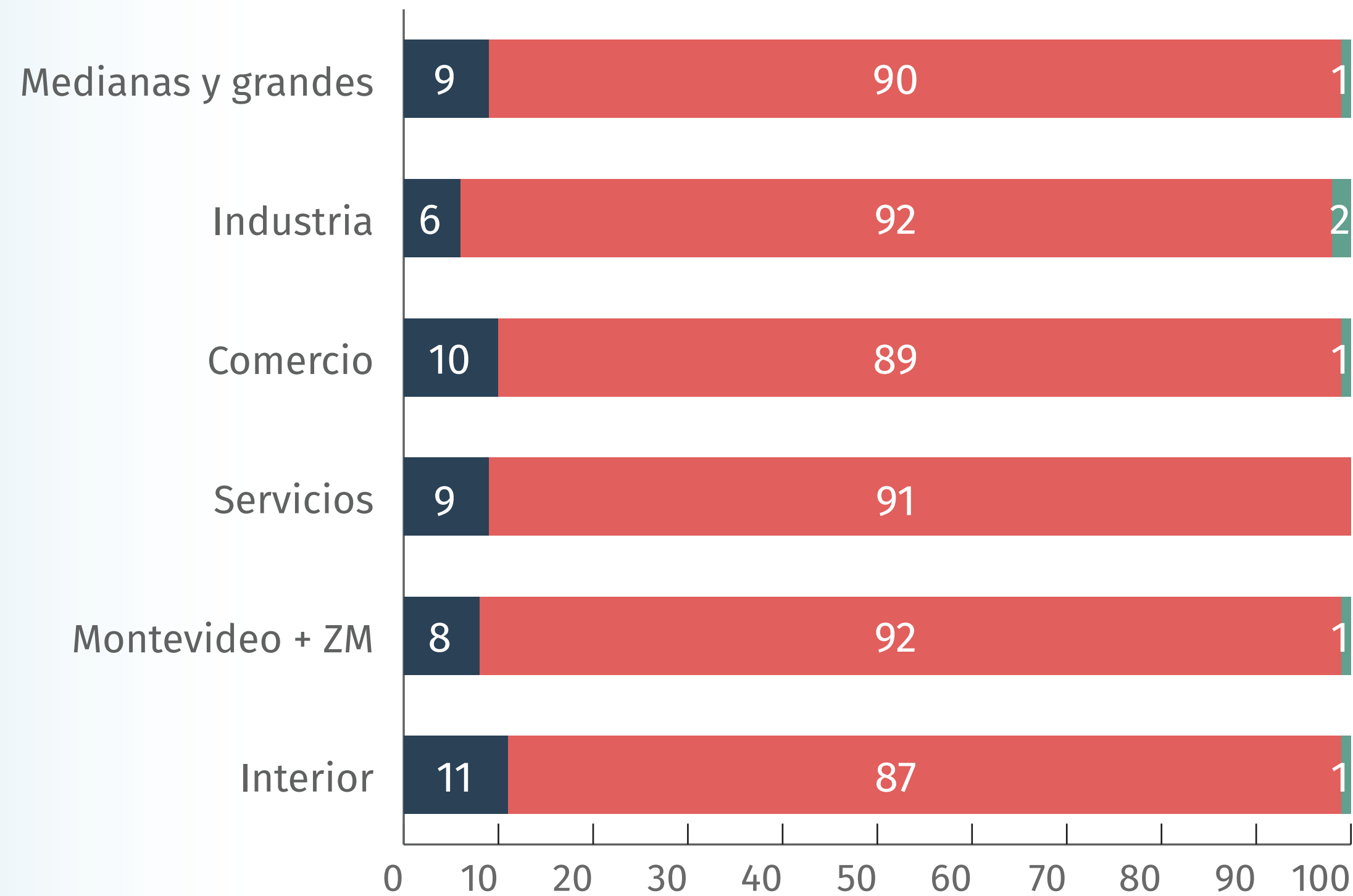


	2023	2022
Dueño o socio	47%	32%
Gerente general	3%	6%
Gerente de IT	9%	4%
Jefe de Seguridad de la Información	4%	9%
Otro cargo	13%	19%
Empresa o persona externa	25%	28%
Encargado / Jefe de sistemas / IT	0%	2%
No sabe	0%	2%

¿La empresa ha contratado un seguro para cubrirse ante incidentes de Ciberseguridad?

Base 3

● Sí ● No ● No sabe

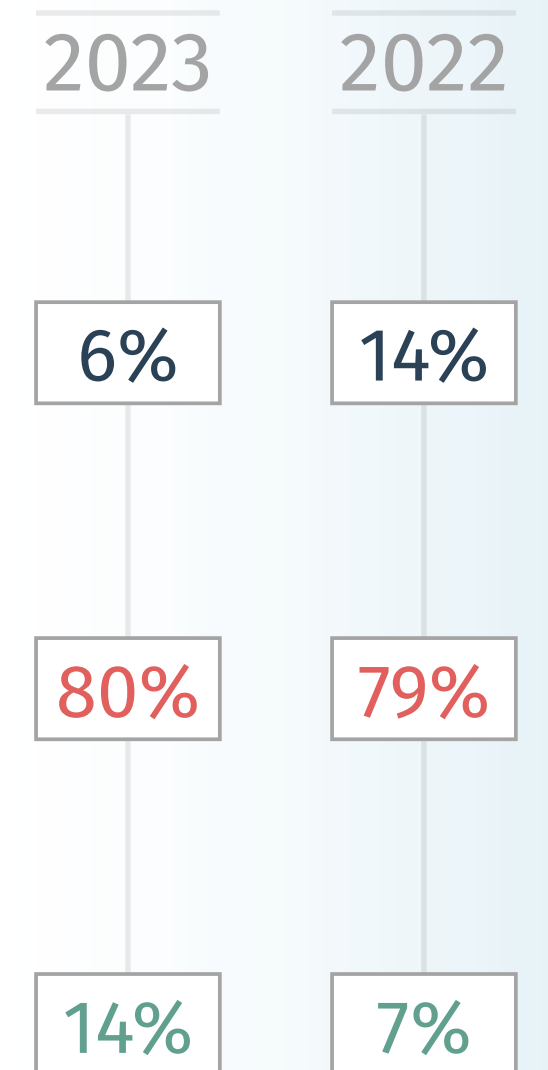


↓

9%
Sí

90%
No

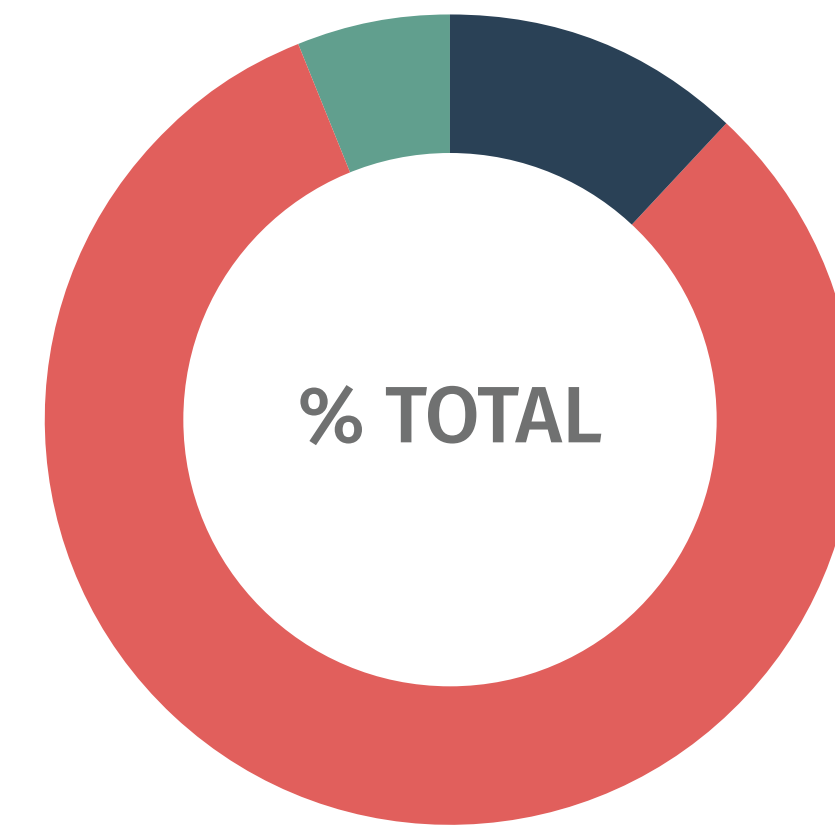
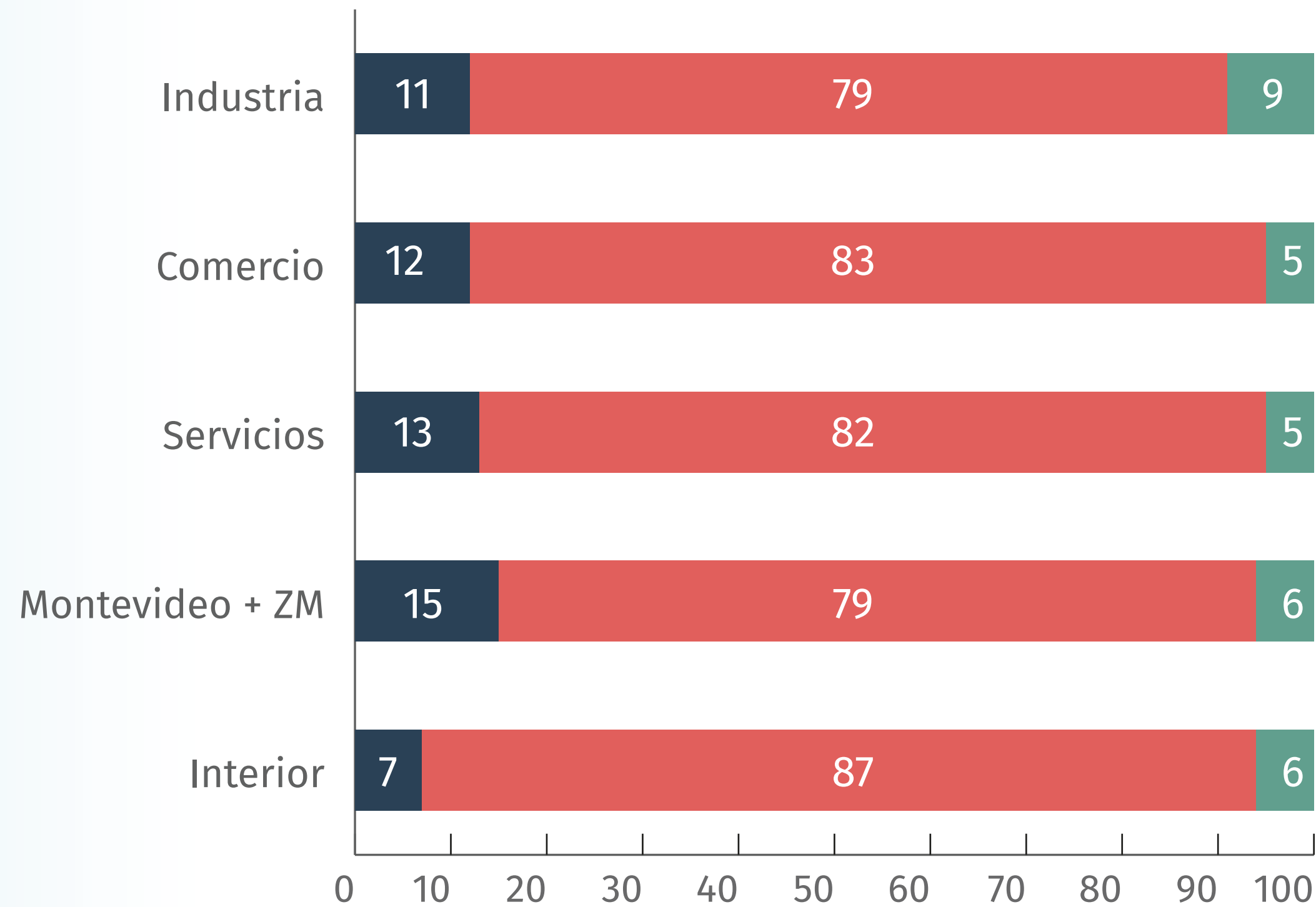
1%
No sabe



¿Los clientes de la empresa exigen niveles de Ciberseguridad importantes?

Base 4

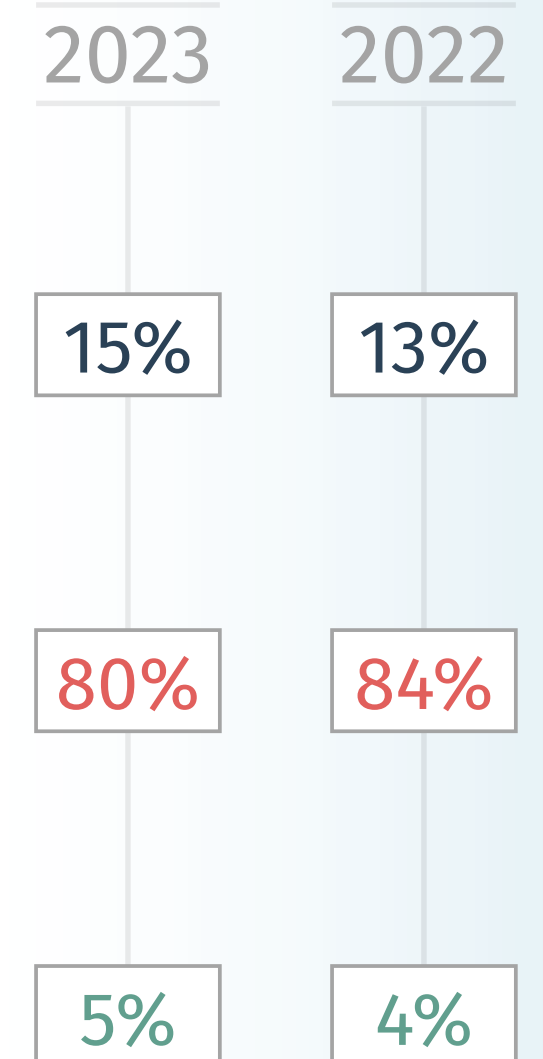
● Sí ● No ● No sabe



12%
Sí

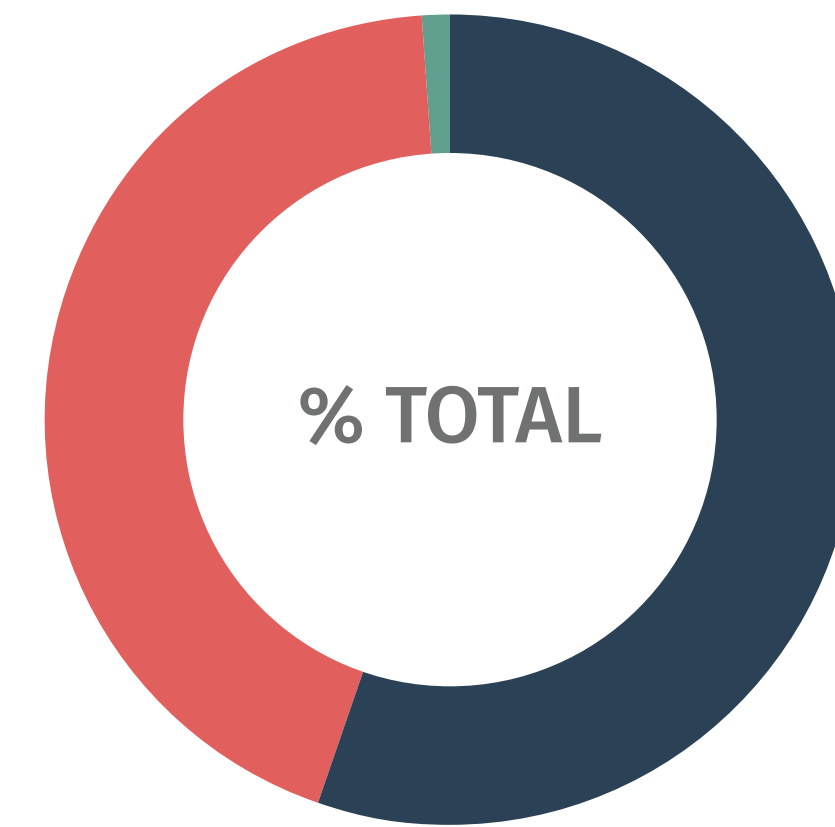
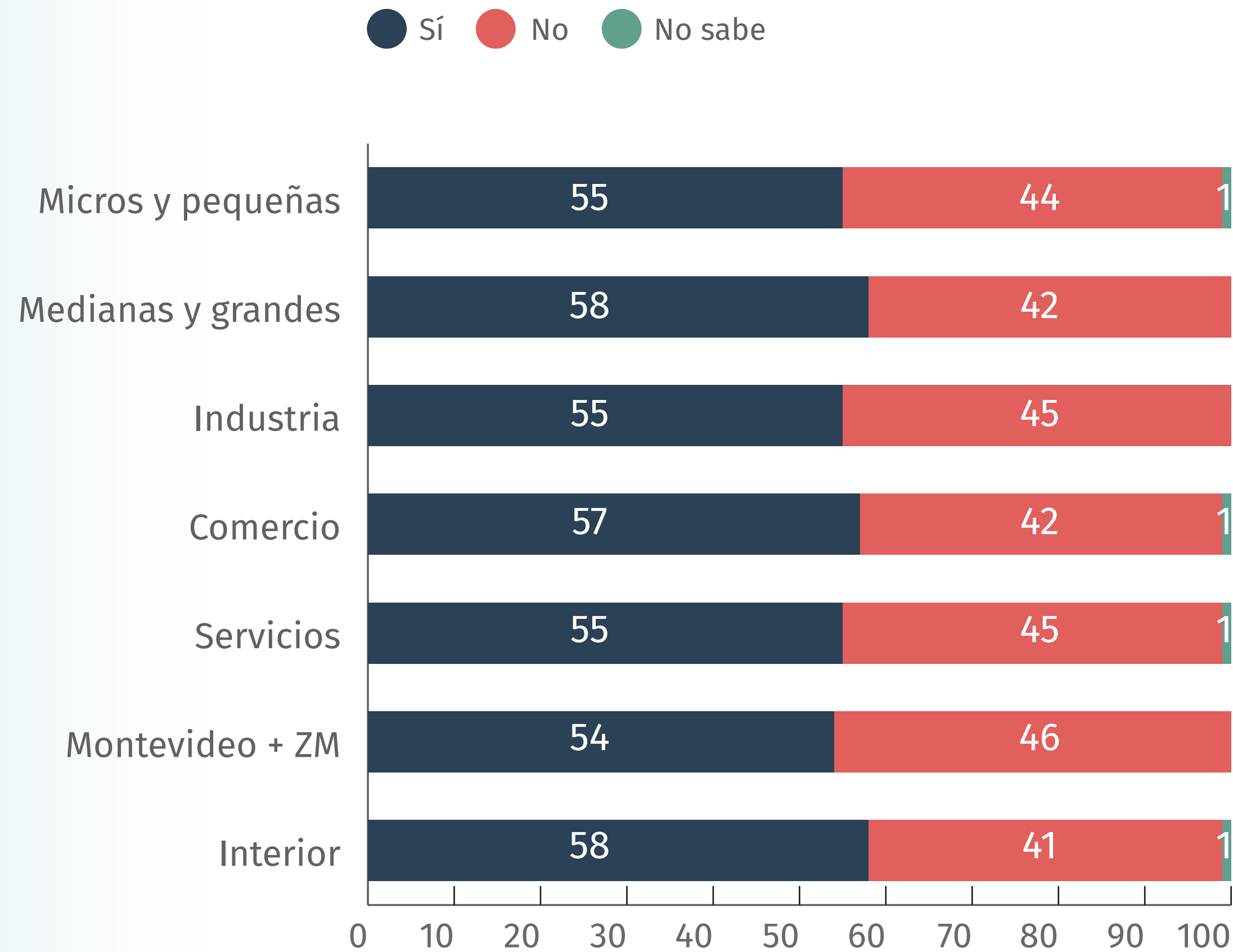
82%
No

6%
No sabe



¿La empresa guarda datos personales de sus clientes?

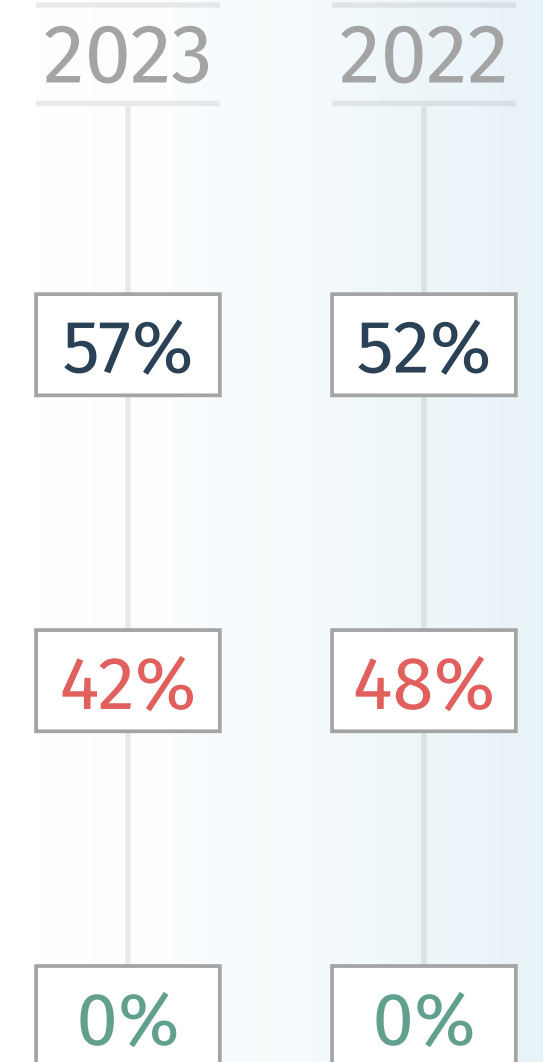
Base 1



56%
Sí

44%
No

1%
No sabe



Encuesta

Personas

Datasec



Ficha técnica

Grupo RADAR realiza desde 2001 un estudio anual, llamado **El Perfil del Internauta Uruguayo**, que con los años se transformó el estudio de referencia sobre los usos de internet en el Uruguay, que se utiliza tanto en la Academia como a nivel de Gobierno, y empresas vinculadas a la actividad digital (agencias de publicidad, agencias de medios, anunciantes, etc.).

La metodología de este estudio ha ido cambiando con el transcurso de los años y a medida que los usos de internet se iban complejizando.

En las últimas ediciones, el estudio consistió en los siguientes módulos:

1 - Una encuesta telefónica a una muestra aleatoria de 800 números de celular, encuestándose solo mayores de 12 años. Se definen cuotas de acuerdo a la distribución real de la población según tres variables: edad (4 tramos), género, y 6 estratos de localidades de acuerdo a su población (Montevideo y área Metropolitana, localidades de + de 20.000 habitantes, de 10.000 a 20.000, de 5.000 a 10.000, de 2.000 a 5000, y menos de 2.000. El margen de error máximo es de ± 3.1 , para un nivel de confianza del 95%.

El objetivo de este módulo es determinar la penetración de internet y clasificar los usuarios en altos, medios y bajos, a fin de calcular los ponderadores que se usarán para corregir el sesgo que tiene la encuesta online (módulo 2) hacia usuarios más altos que la media de la población.

2 - Una encuesta online autoadministrada de 2000 casos a personas mayores de 12 años, reclutadas mediante avisos contratados en Facebook e Instagram. Esta encuesta se aplica para todos los temas vinculados a los diferentes usos de internet.

Se definieron previamente cuotas por rango de edad, género y estratos de localidades según su población, de acuerdo al universo de usuarios de internet que surge de la encuesta telefónica.

Además, y a efectos de corregir el sesgo natural de esta muestra se ponderaron sus resultados según la variable Altos / Medios / Bajos usuarios de internet que se investigó en ambas encuestas.

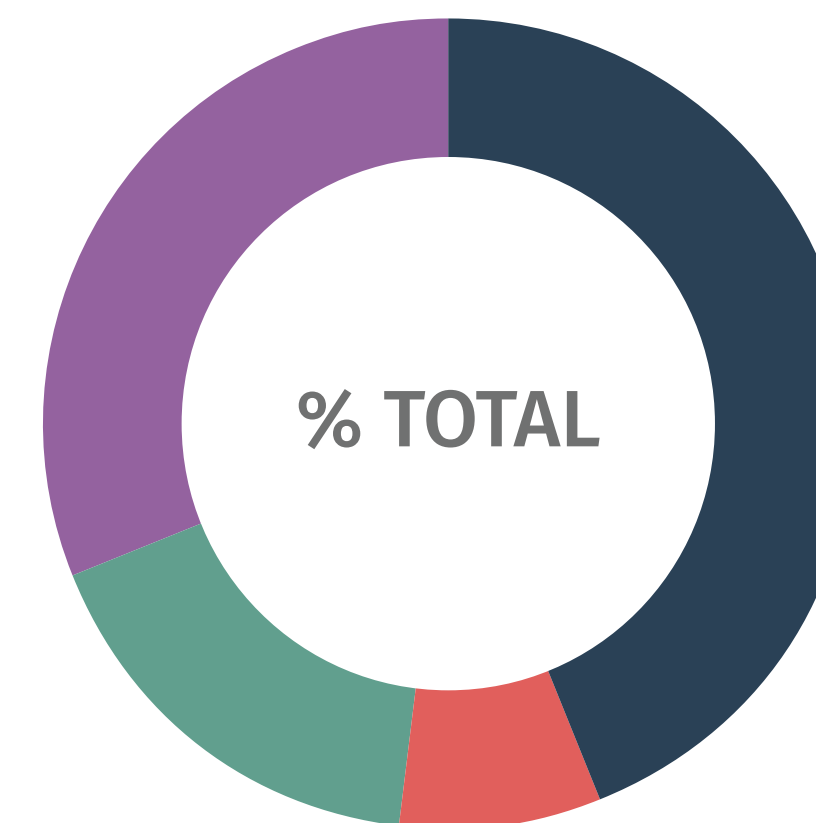
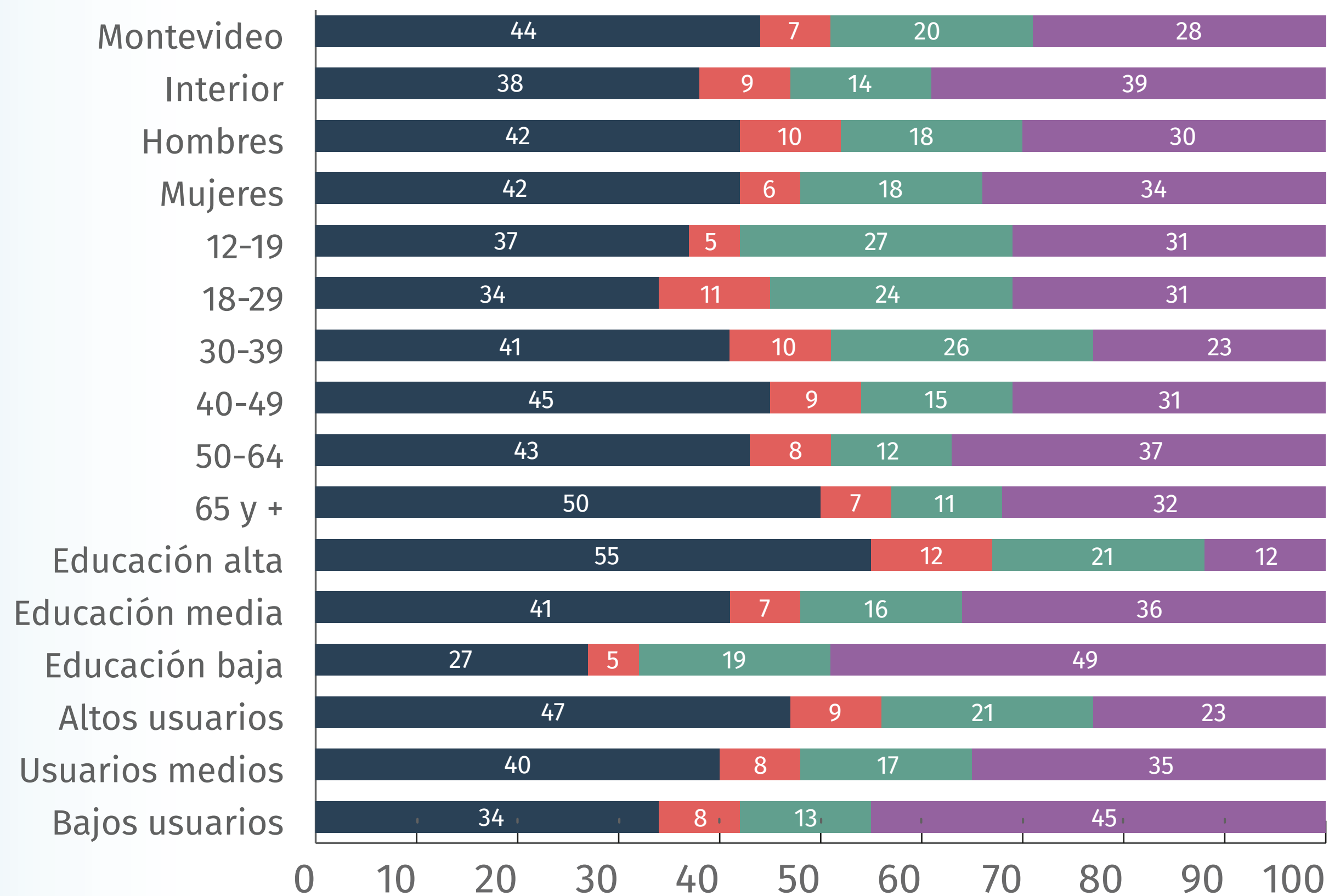
3 - Una encuesta online autoadministrada a una muestra de 1000 personas mayores de 18 años que hubieran realizado alguna compra online en los últimos 7 días. La composición de esta muestra se determinó a partir de los resultados de la encuesta a usuarios de internet en general mayores de 18 años, a fin de que sea representativa del universo de personas que compran por internet. Este módulo es irrelevante a efectos del análisis realizado para DATASEC.

Las sumas pueden no dar 100% por errores de redondeos.

¿Tenés instalado un antivirus en tu computadora?

BASE: 2000 usuarios de internet

● Sí, gratuito
 ● Sí, pago
 ● No tengo antivirus
 ● No tengo computadora



44%
Sí, gratuito

8%
Sí, pago

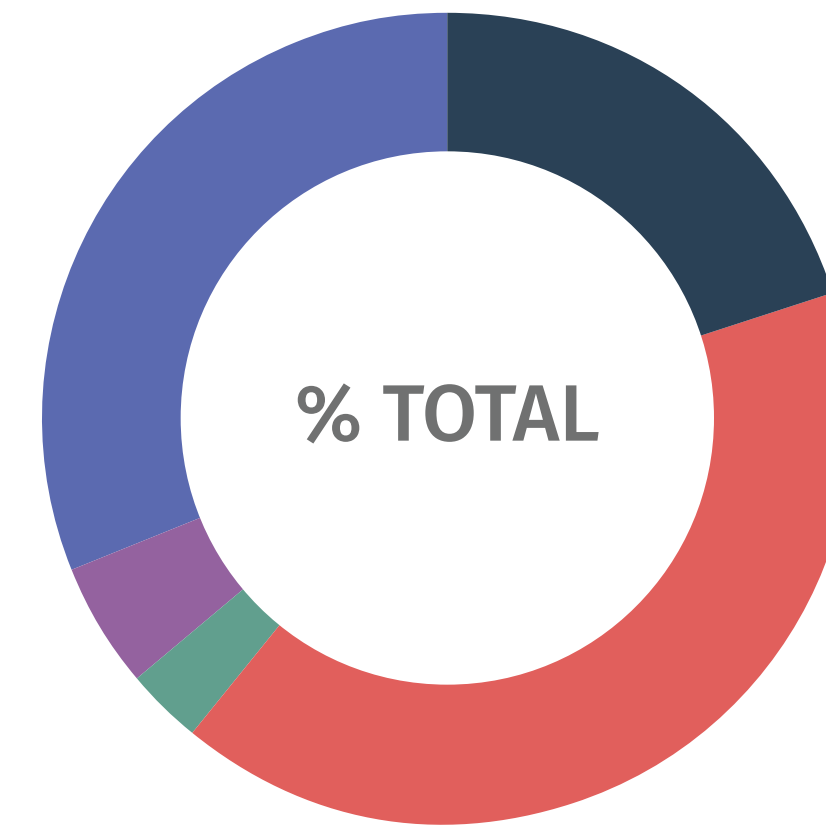
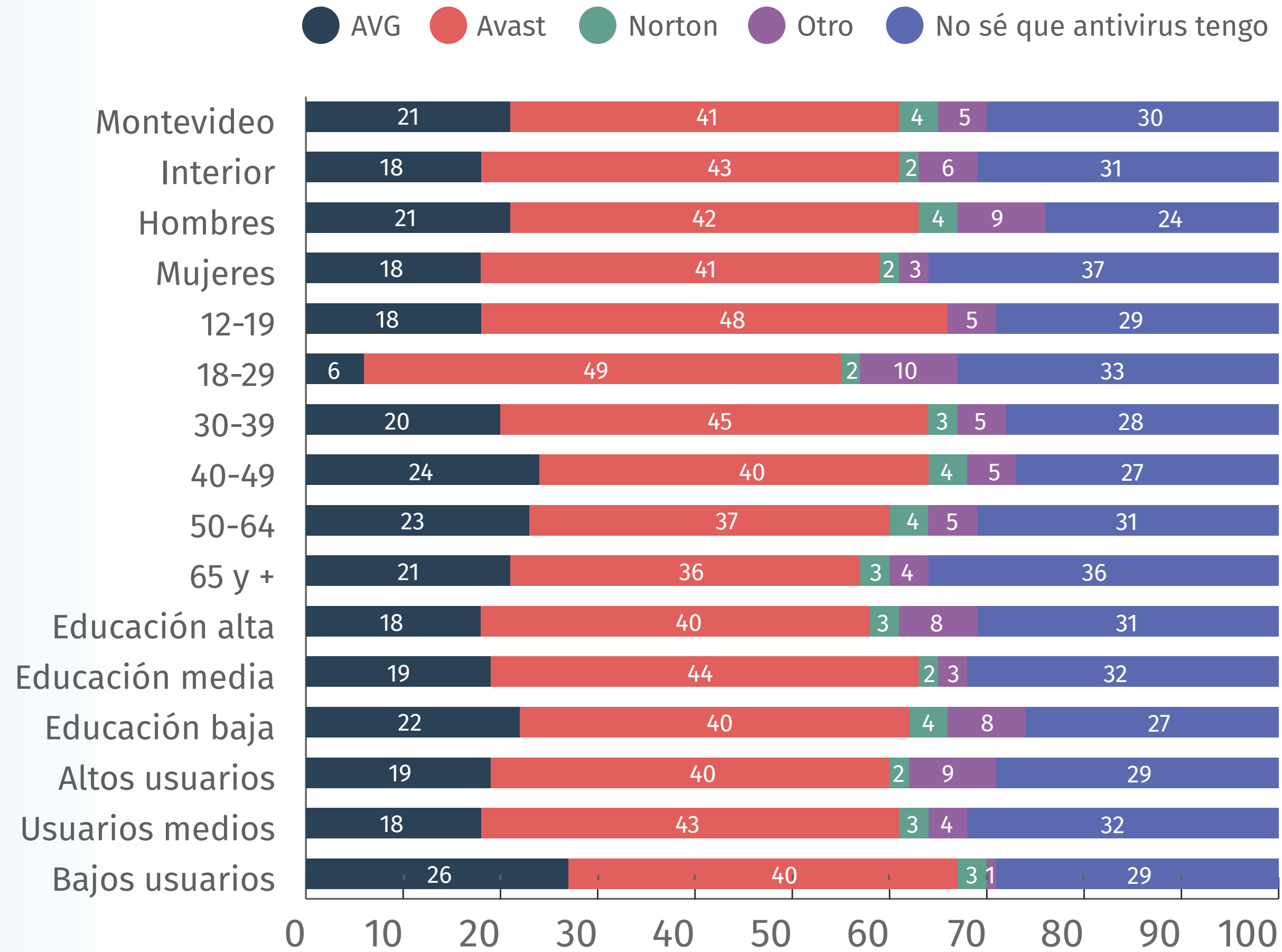
17%
No tengo antivirus

31%
No tengo computadora

1 de cada 4 personas con computadora no tiene antivirus

¿Qué antivirus tenés?

BASE: 996 que declaran tener antivirus en su computadora



↓
20%
AVG

41%
Avast

3%
Norton

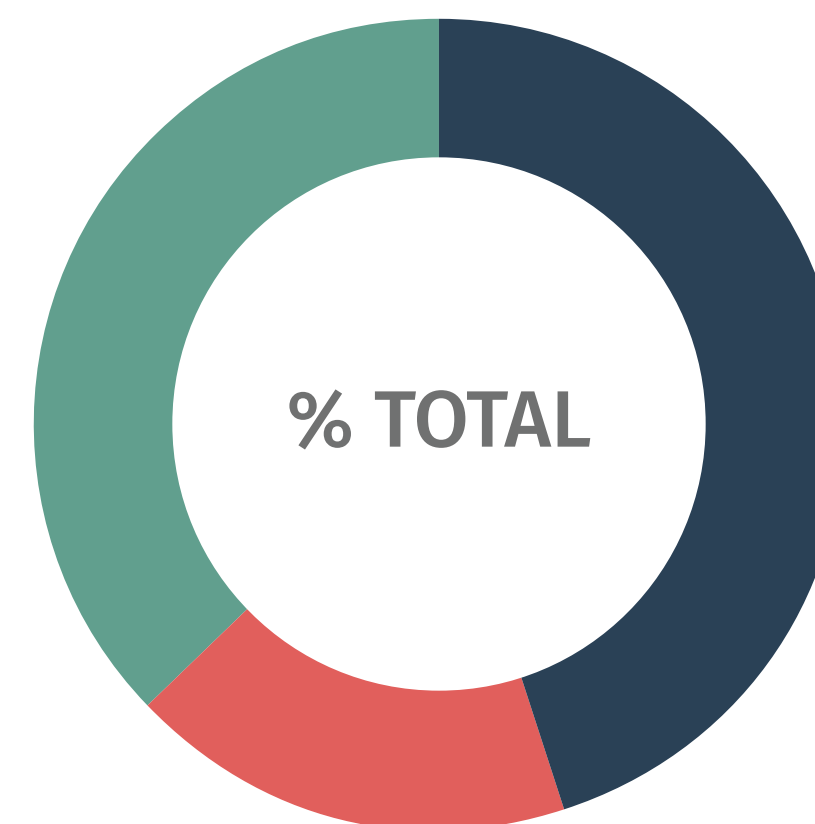
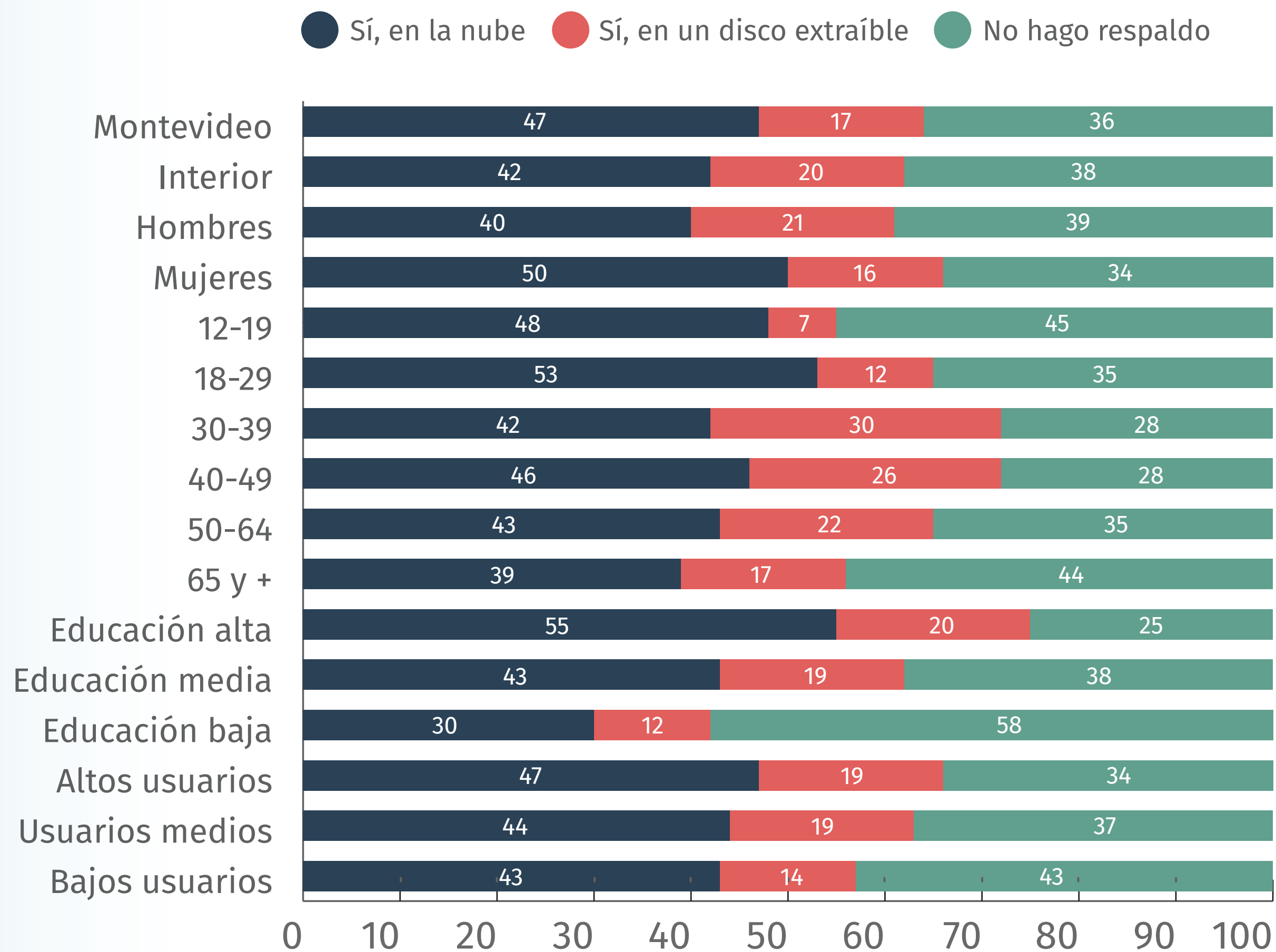
5%
Otro

31%
No sé que antivirus tengo

1 de cada 3 personas con antivirus no sabe cuál tiene - Avast es el más común

¿Hacés respaldos de lo que tenés en la computadora?

BASE: 1356 que tienen computadora



↓
45%
Sí, en la nube
(Drive, Dropbox u otro)

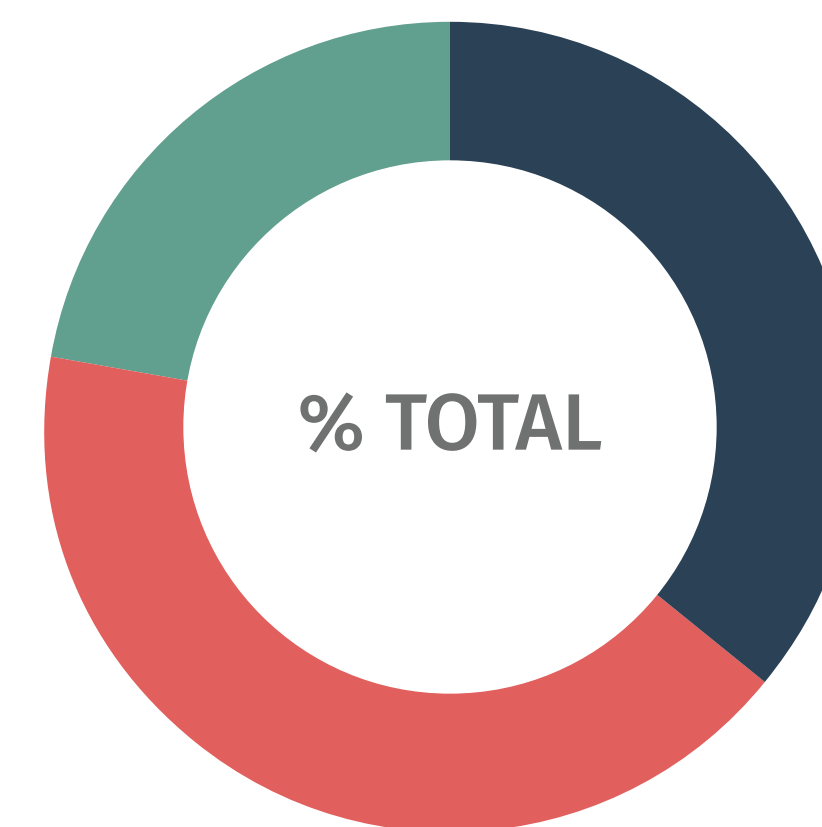
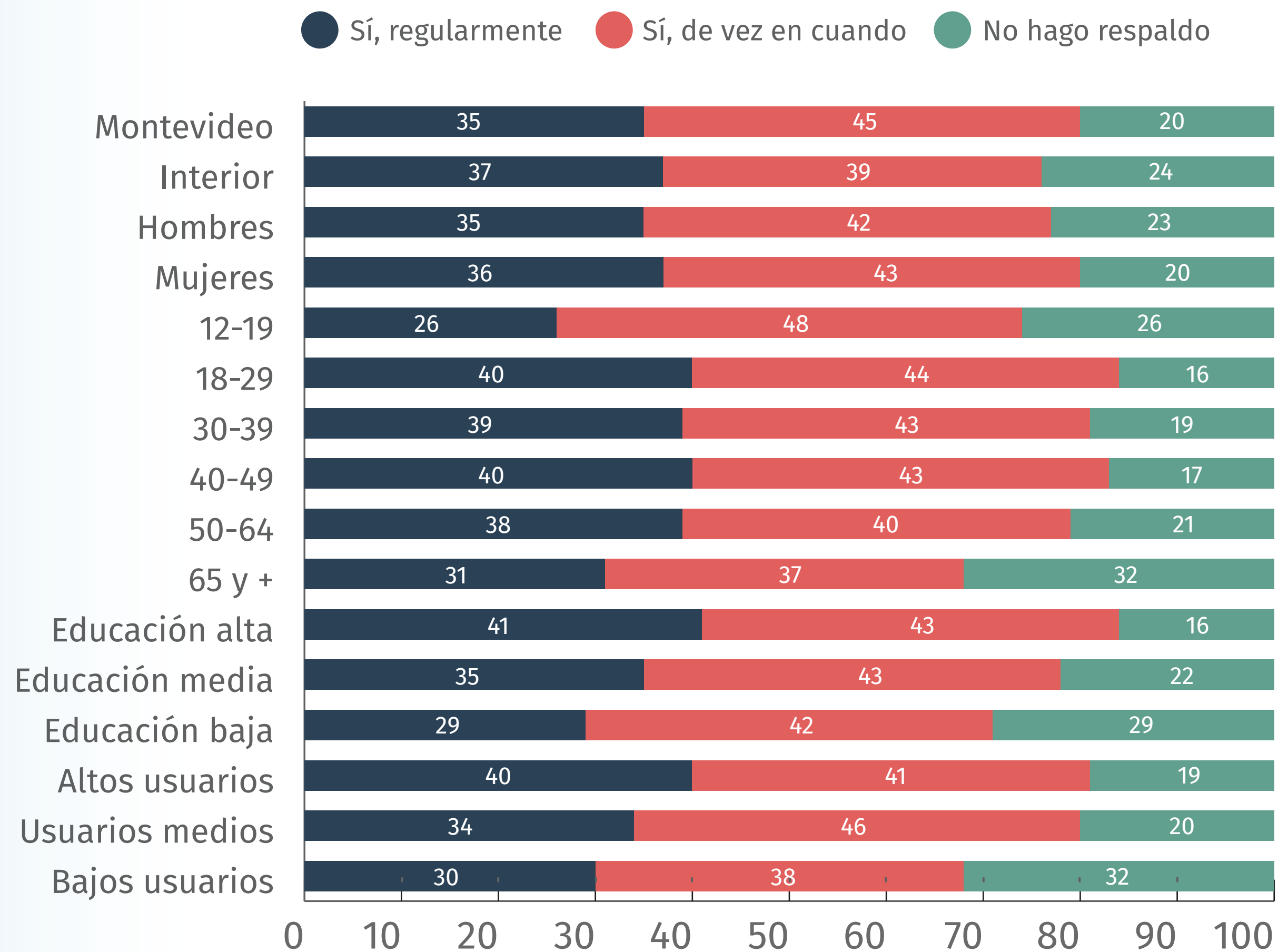
18%
Sí, en un disco extraíble

37%
No hago respaldo

Menos de la mitad de quienes tienen computadora declaran respaldar sus archivos

¿Hacés respaldos de lo que tenés en el celular?

BASE: 1812 con smartphone



36%
Sí, regularmente

42%
Sí, de vez en cuando

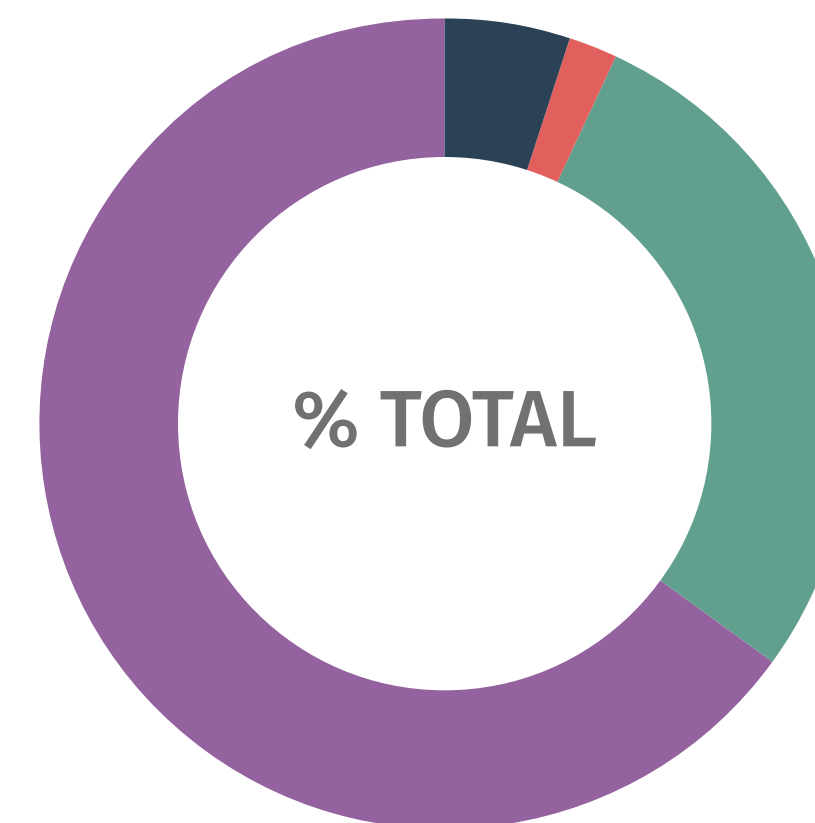
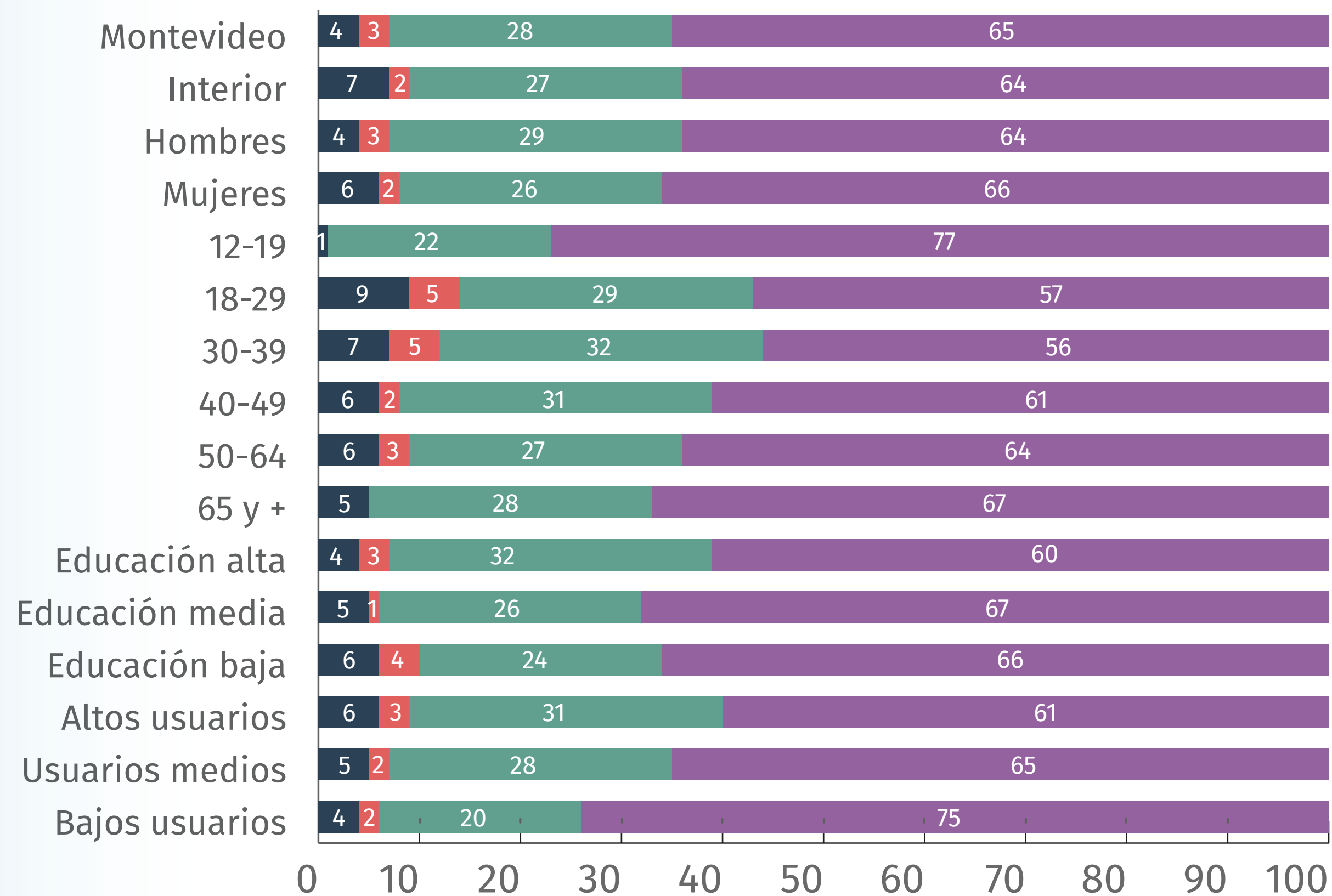
22%
No hago respaldo

4 de cada 5 personas con smartphone respalda lo que tiene en el mismo

¿En algún momento de este año fuiste víctima de algún intento de fraude, de engaño o de robo de información por internet?

BASE: 2000 usuarios de internet

● Sí, y perdió dinero
 ● Sí, y perdió información
 ● Sí, pero no perdió nada
 ● No tuvo ningún incidente



5%

Sí, y perdió dinero

2%

Sí, y perdió información

28%

Sí, pero no perdió nada

65%

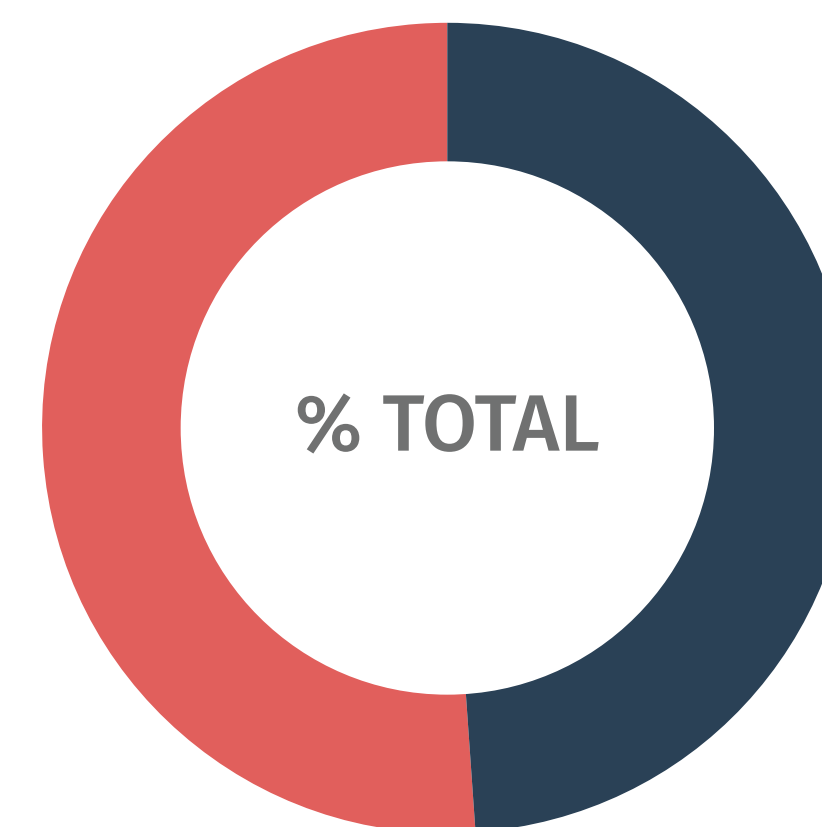
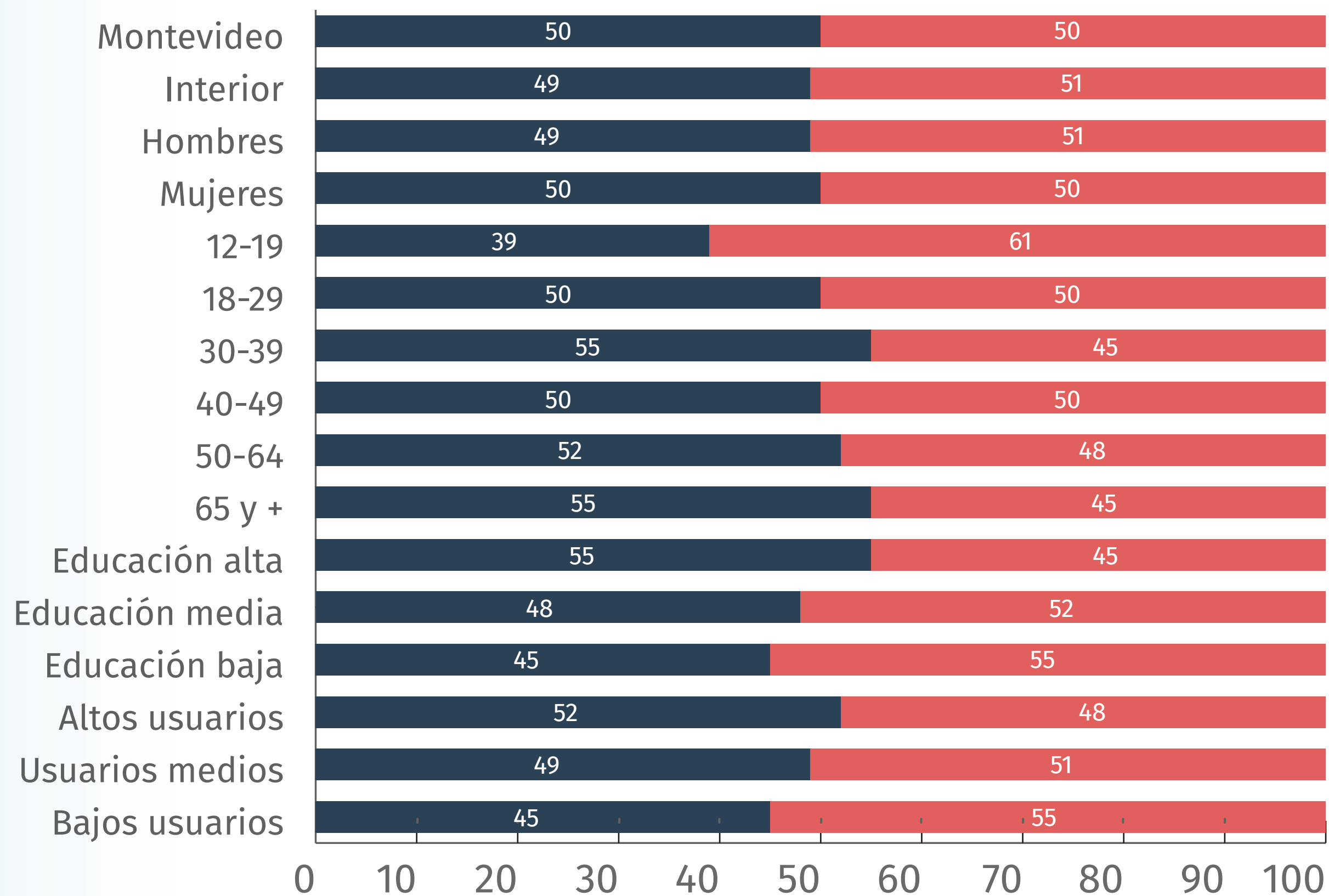
No tuvo ningún incidente

1 de cada 20 usuarios de internet perdió dinero en el último año por un fraude por internet

¿Considerás que has cambiado algún hábito debido a los intentos de fraude y estafas en internet?

BASE: 2000 usuarios de internet

● Cambié hábitos ● No cambié hábitos



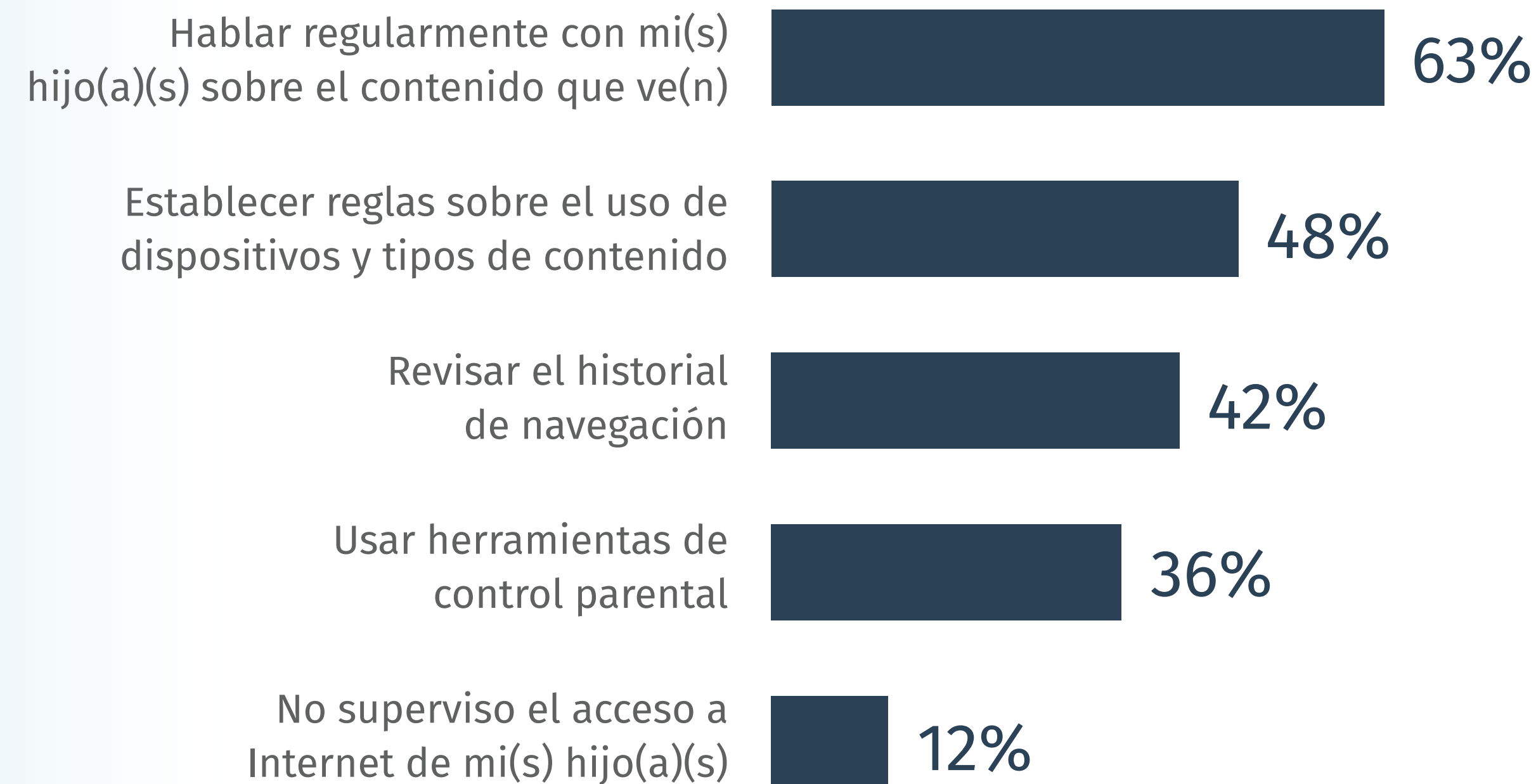
49%
Cambié hábitos

51%
No cambié hábitos

1 de cada 20 usuarios de internet perdió dinero en el último año por un fraude por internet

En tu experiencia como padre/madre, ¿has tomado alguna de estas medidas para supervisar el acceso de tu(s) hijo(a)(s) a Internet?

BASE: 380 con hijos menores



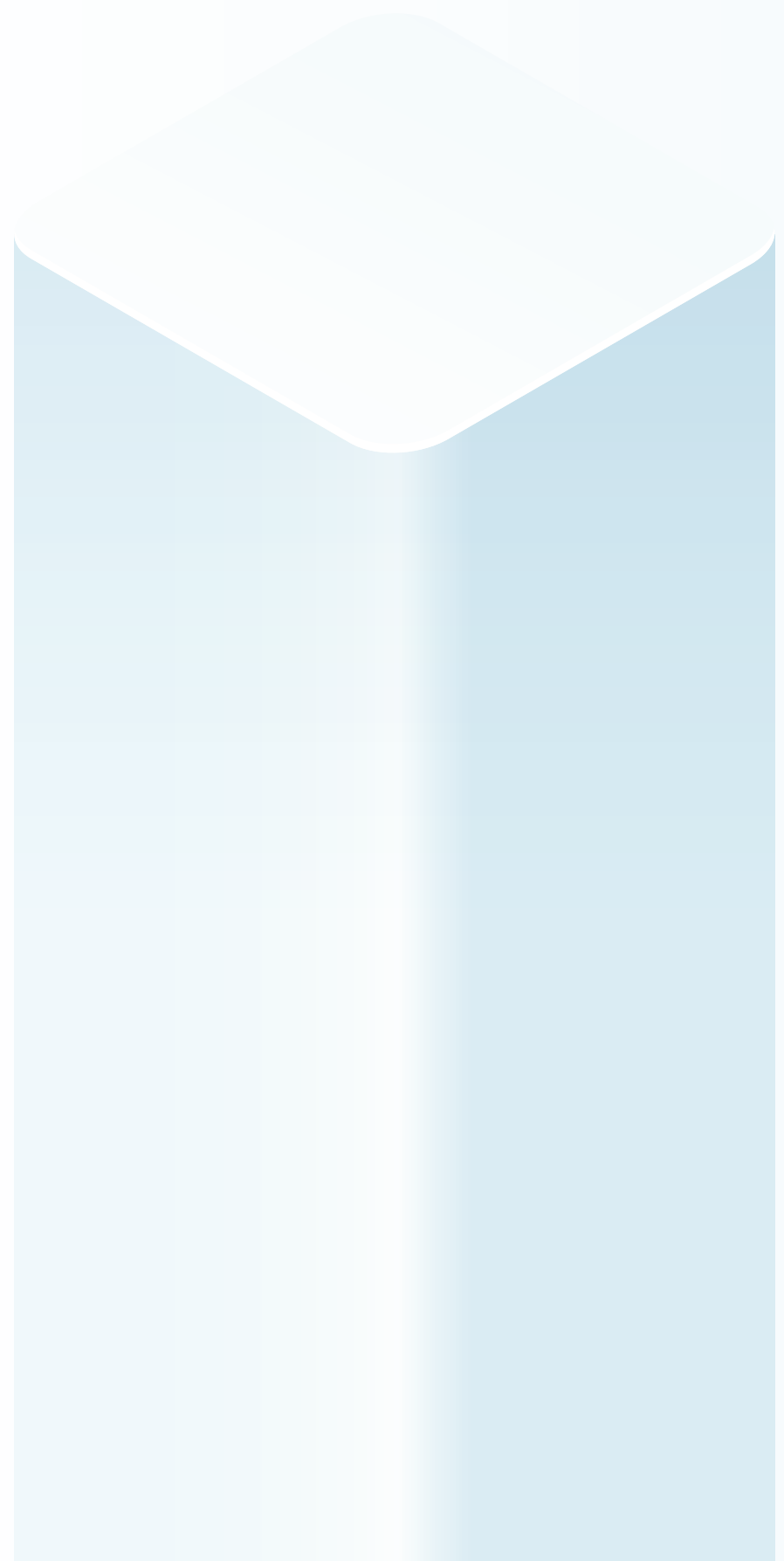
Entre quienes tienen hijos menores, 88% dice haber tomado alguna medida para supervisar el acceso a internet de los mismos

A menor Nivel Socio Económico crece notoriamente el % de personas que revisan el historial de navegación de sus hijos y usan herramientas de control parental

Conclusiones



Uruguay y la Ciberseguridad: Un Desafío Urgente



El análisis de la Encuesta de Ciberseguridad 2024 refleja avances y desafíos en la protección digital en Uruguay. El aumento de incidentes cibernéticos y el crecimiento en la sofisticación de las amenazas demuestran la necesidad de fortalecer continuamente las estrategias de ciberseguridad, tanto en el ámbito público como privado.

A lo largo de los últimos años, distintas iniciativas han buscado estructurar una respuesta integral a estos desafíos. En 2024, el sector público y el privado colaboró en el desarrollo de una nueva Estrategia Nacional de Ciberseguridad, un paso clave hacia una mayor protección digital. Sin embargo, como toda estrategia de largo plazo, su implementación requiere inversión en infraestructura, formación de profesionales y el fortalecimiento de capacidades en todos los sectores.

Un reciente relevamiento conjunto entre Agesic y la academia ha permitido identificar necesidades clave y desarrollar propuestas educativas para atender la creciente demanda de talento en ciberseguridad, una iniciativa fundamental para el futuro del país. Los resultados del informe también evidencian la creciente vulnerabilidad de los usuarios individuales.

En 2024, aproximadamente 175.000 uruguayos perdieron dinero debido a fraudes en línea, y 70.000 personas experimentaron la pérdida de información personal. Este dato subraya la necesidad de reforzar la educación y concienciación en seguridad digital, promoviendo buenas prácticas entre ciudadanos, empresas e instituciones.

En este contexto, es fundamental continuar avanzando en la consolidación de un ecosistema de ciberseguridad robusto, que incluya una mayor inversión en prevención, desarrollo de normativas alineadas con estándares internacionales y un esfuerzo sostenido en la capacitación de profesionales

especializados. La ciberseguridad es un pilar esencial para la estabilidad digital del país, y su fortalecimiento requiere el compromiso conjunto de empresas, ciudadanos y organismos públicos.

Para conocer la evolución de la ciberseguridad en las empresas uruguayas en los últimos años, se pueden consultar los informes anteriores en el siguiente enlace:

<https://datasec-soft.com/ciberseguridad-en-las-empresas-uruguayas/>

Fuentes:

Elsner, M., Atkinson, G., & Zahidi, S. (2025). Global Risks Report 2025. World Economic Forum. <https://www.weforum.org/publications/global-risks-report-2025/>

Centro Nacional de Respuesta a Incidentes de Seguridad Informática. (2025, 23 de enero). Estadísticas de incidentes de seguridad de la información en 2024. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. <https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/datos-y-estadisticas/estadisticas/estadisticas-incidentes-seguridad-informacion-2024>

***D*atasec**