

Encuesta sobre ciberdelitos

Mar del Plata, febrero 2022



InFo-Lab



UNIVERSIDAD
FASTA



Observatorio
Universitario
de la Ciudad

ENCUESTA SOBRE CIBERDELITOS

Mar del Plata, febrero 2022

Coordinación

Lic. Gabriel Coronello Aldao

Investigación y análisis

Lic. Mónica Pascual

Prof. Santiago Cueto

Lic. Leticia Brea

Sebastián Romani

Julieta Campero

Agradecimiento

Ing. Leandro Vega

Autoridades UFASTA

• Decano FI:

Esp. Ing. Roberto Giordano Lerena

• Directora Info-Lab:

Esp. Ing. Ana Di Iorio

• Líder I+D Ciberseguridad Info-Lab:

Ing. Santiago Trigo



INTRODUCCIÓN

La pandemia de COVID 19 provocó que desde comienzos de 2020 millones de personas se vieran obligadas a utilizar diferentes herramientas tecnológicas para continuar desarrollando sus actividades cotidianas, tales como realizar compras, trámites bancarios o mantener interacciones sociales.

En ese marco el uso de la tecnología como medio o como fin para cometer delitos también ha aumentado exponencialmente.

Según las estadísticas oficiales del Ministerio Público Fiscal del Departamento Judicial de Mar del Plata, los delitos informáticos registraron un incremento de entre un 700% y 800% con respecto al año 2019.

No obstante, más allá de estas cifras globales, se carece de datos precisos que permitan determinar las particularidades de este tipo de hechos, debido a que los mismos no se encuentran categorizados de manera detallada.

Aún así, se sabe que entre los delitos que registraron los mayores incrementos figuran las estafas virtuales, predominando las bancarias; las extorsiones sexuales, la distribución de material de abuso sexual infantil, el grooming y actos de violencia, destacándose la violencia de género.

Es sabido, además, que los llamados delitos informáticos o delitos cometidos a través de medios digitales, presentan una elevada cifra negra, es decir, que muchos de ellos no se denuncian, y por tal razón, no se encuentran asentados en las estadísticas oficiales.

INTRODUCCIÓN

Este estudio realizado por el “Observatorio de la Ciudad” de la Universidad FASTA tiene como objeto investigar y relevar información sobre la comisión de delitos mediados por la tecnología en la ciudad de Mar del Plata.

Para la concreción de este informe, fueron realizadas 500 encuestas de manera online y presencial sobre victimización con el fin de conocer la percepción de la seguridad de los encuestados marplatenses, detectar potenciales víctimas, determinar los canales adecuados para prevención y concientización, conocer las medidas de seguridad adoptadas por los ciudadanos, cuantificar los tipos de delitos sufridos y explorar el nivel de cifra “negra” de los mismos.

Este proyecto (RDFI 156 - 2021) fue realizado junto al Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InFo-Lab), en coordinación con las Facultades de Ingeniería y de Ciencias Jurídicas y Sociales de la Universidad FASTA, el cual posee una vasta experiencia en investigaciones vinculadas al fraude electrónico y violencia digital.

En una primera sección de este informe se indaga sobre cuáles son las medidas de seguridad que adoptan los ciudadanos al navegar o realizar trámites online y sobre si se sienten o no seguros al utilizar este tipo de herramientas.

En segundo término, se presentan datos sobre cuáles son los medios que la sociedad utiliza para informarse sobre este fenómeno a los efectos de direccionar los mecanismos de prevención y concientización.

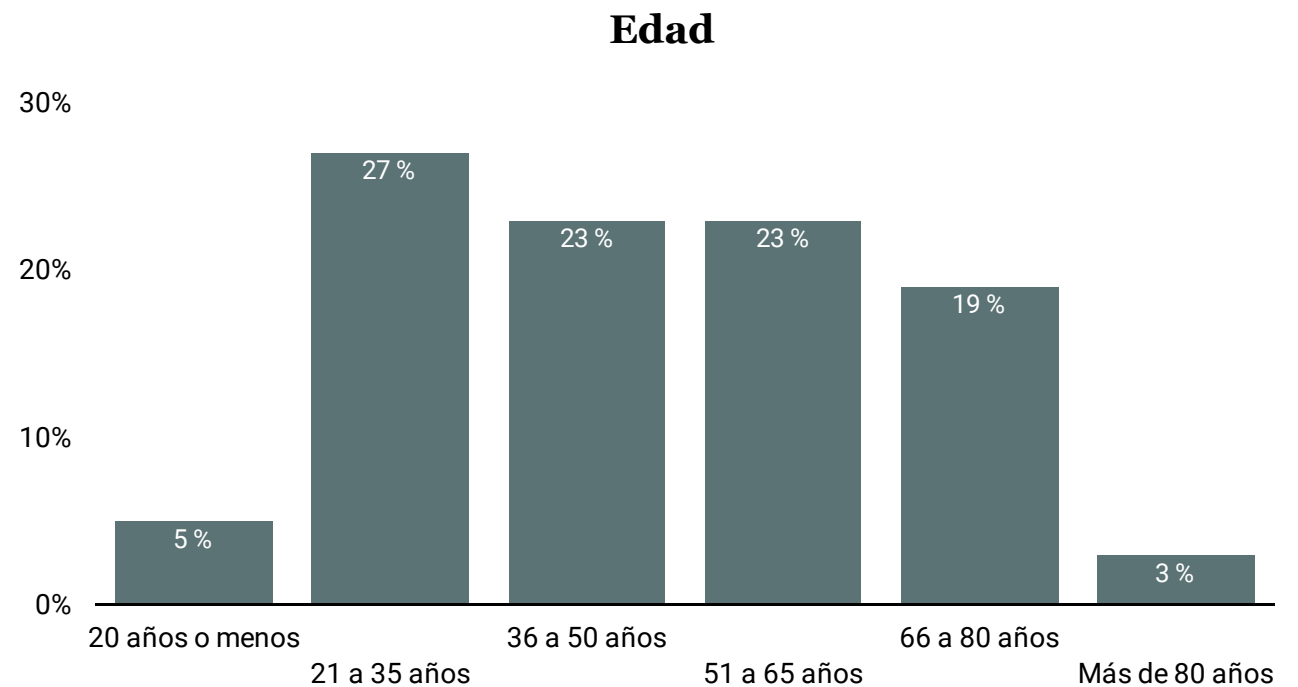
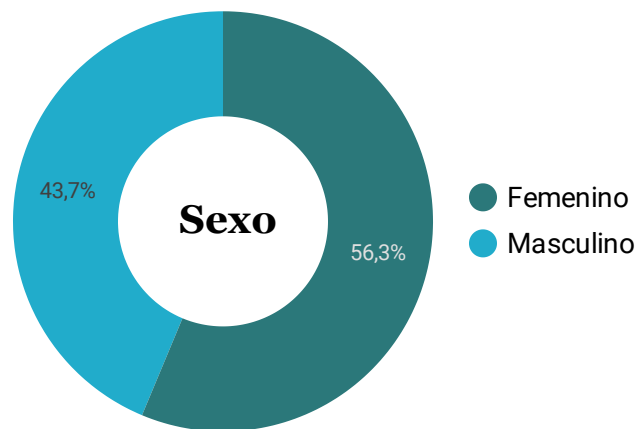
En tercer lugar, se indaga sobre si los encuestados fueron víctimas de algún delito y por último, se pregunta sobre las reacciones frente a esas circunstancias.

PERFIL DE LA MUESTRA

Se trabajó en base a una muestra integrada por 503 personas con al menos 18 años cumplidos.

Para el trabajo de campo se implementó una encuesta presencial, semiestructurada, con algunas preguntas abiertas, en distintos puntos de la ciudad.

n=503

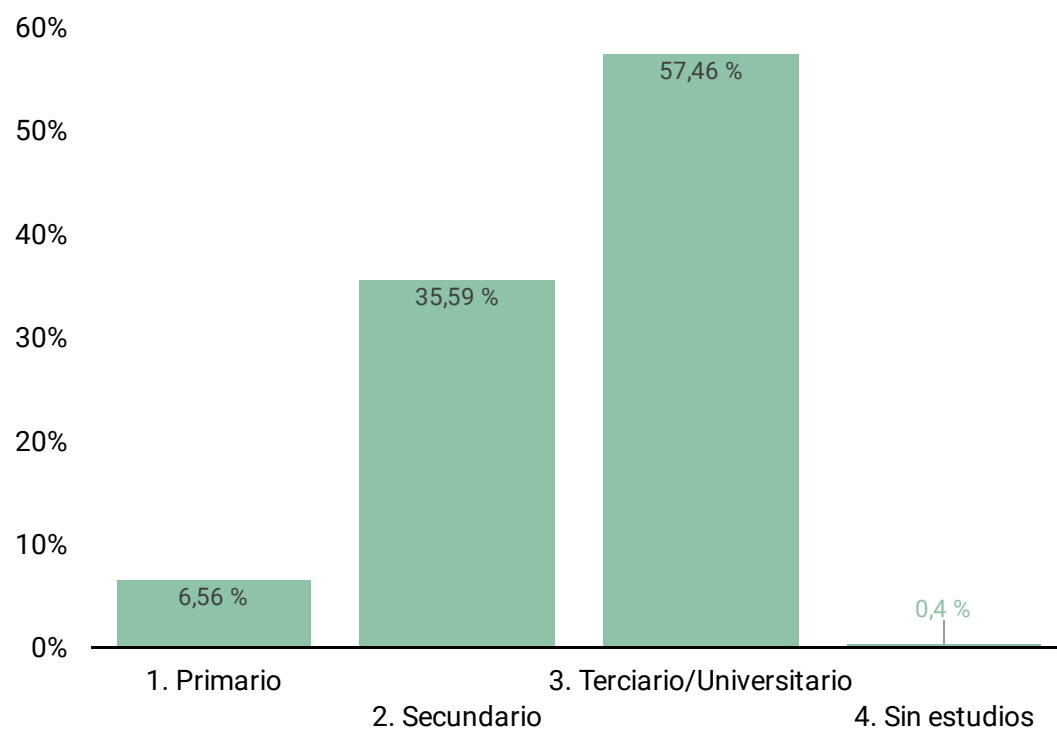


EDAD MEDIA
48,12

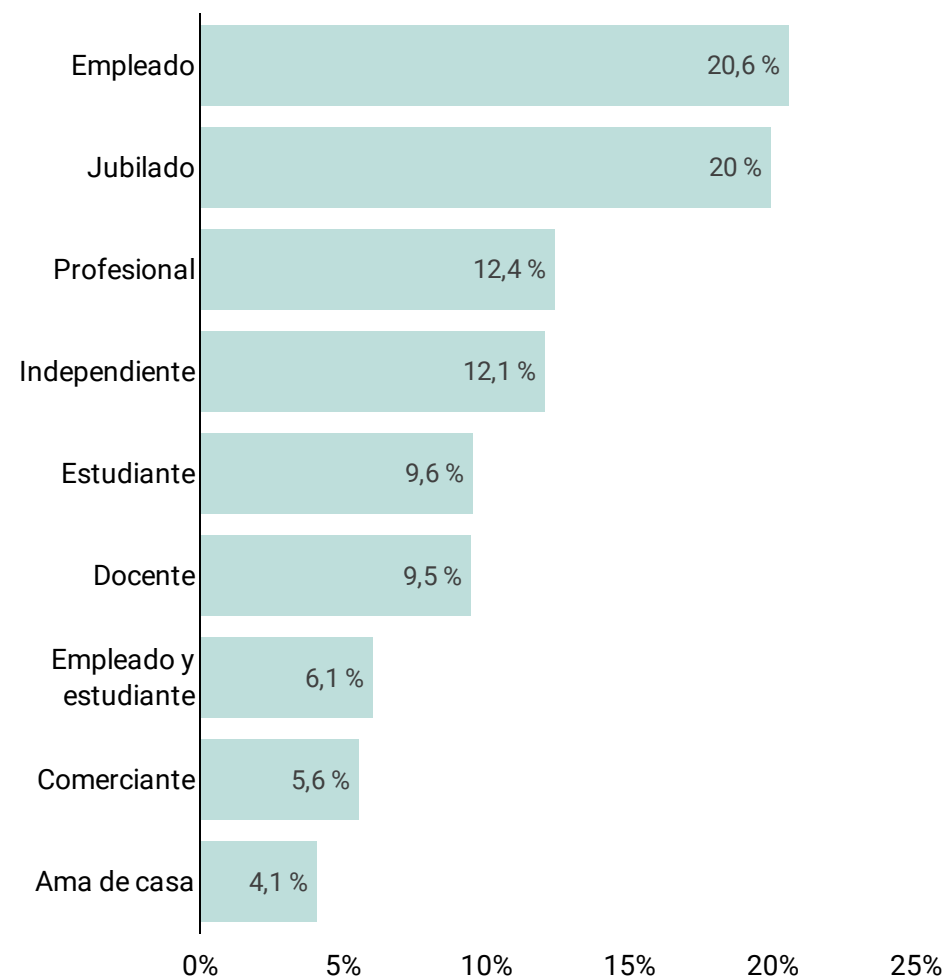
DESVÍO ESTÁNDAR
18,83

PERFIL DE LA MUESTRA

Nivel de estudio

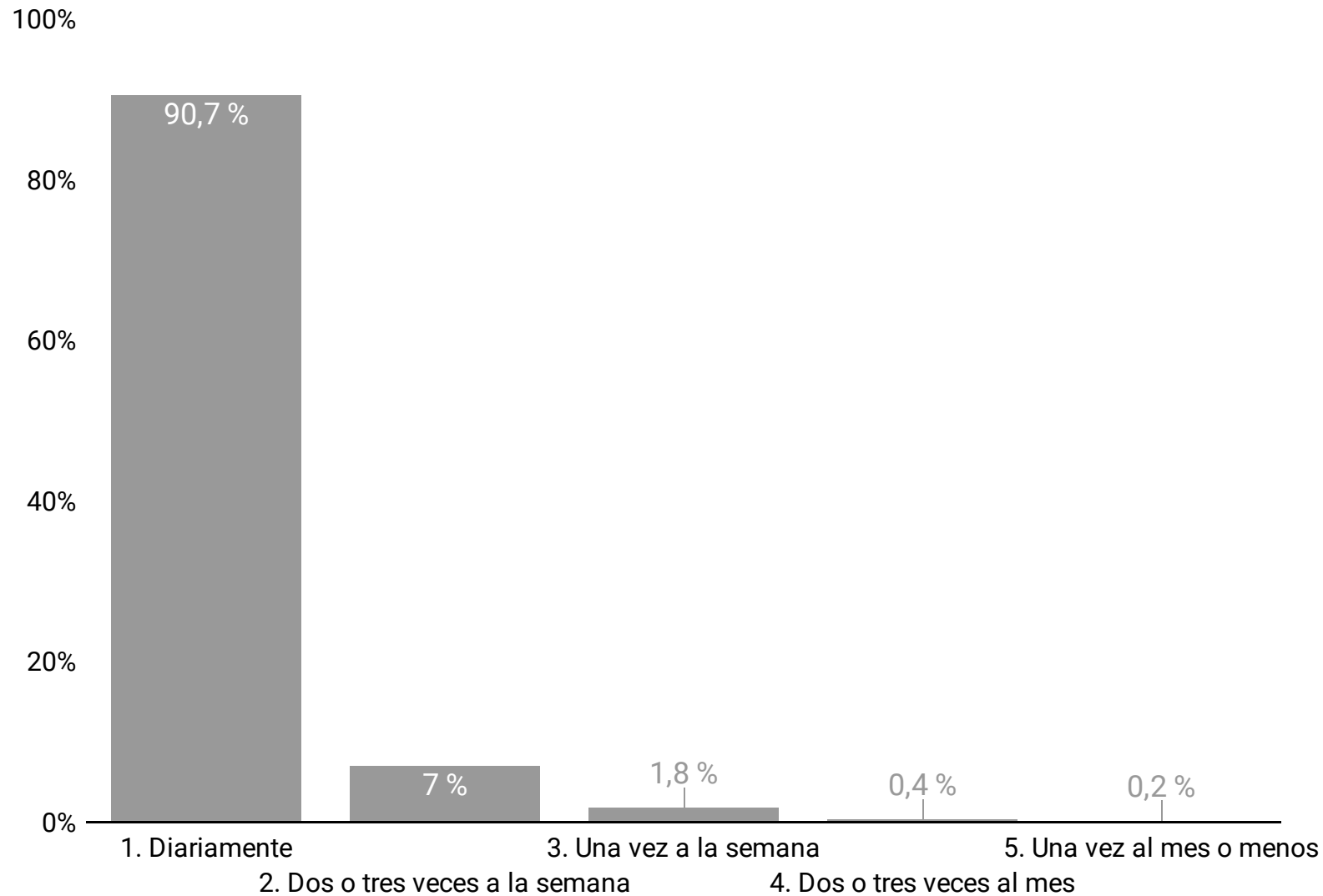


Ocupación



USO DE INTERNET FRECUENCIA DE ACCESO

¿Con qué frecuencia accede a internet? (redes sociales, noticias, banco, etc.)



El 90,7% de los encuestados asegura acceder a internet en forma diaria.

USO DE INTERNET POR SEXO, EDAD Y NIVEL EDUCATIVO

¿Con qué frecuencia accede a internet? (redes sociales, noticias, banco, etc.)

	Diariamente	Dos o tres veces a la semana	Una vez a la semana	Dos o tres veces al mes	Una vez al mes o menos
Femenino	90%	7%	2%	1%	0%
Masculino	91%	7%	2%	0%	0%
20 años o menos	100%	0%	0%	0%	0%
21-35 años	98%	1%	1%	0%	0%
36-50 años	98%	2%	0%	0%	0%
51-65 años	91%	6%	2%	1%	0%
66-80 años	72%	22%	4%	1%	0%
más de 80 años	54%	31%	8%	0%	8%
Primario	76%	15%	6%	3%	0%
Secundario	97%	3%	0%	0%	0%
Terciario/Universitario	89%	8%	2%	0%	0%

Al segmentar las respuestas por características sociodemográficas se destacan las siguientes conclusiones.

No se observan diferencias significativas en relación al sexo.

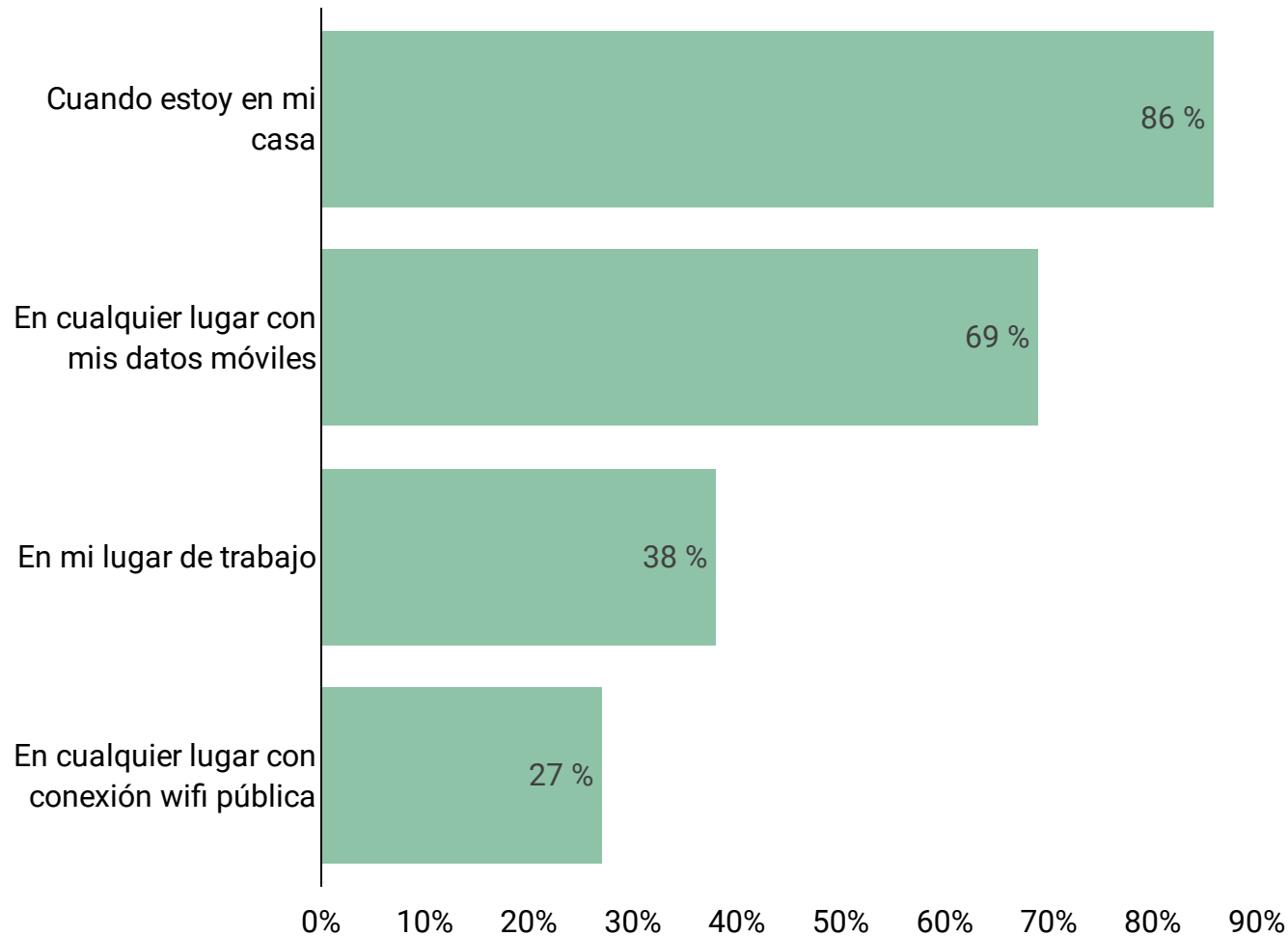
Existen diferencias significativas en la distribución por edades entre los menores y los mayores de 66 años. Los más propensos a usar internet diariamente son los menores de 66 años. Se aprecia que a medida que la edad avanza, las personas son menos propensas a utilizar internet diariamente.

Si bien la frecuencia de acceso a internet es elevada entre las personas más allá de su nivel educativo, se observa que su uso es ligeramente menor entre quienes sólo alcanzaron el nivel primario.



USO DE INTERNET. LUGARES

¿Dónde usa internet generalmente?



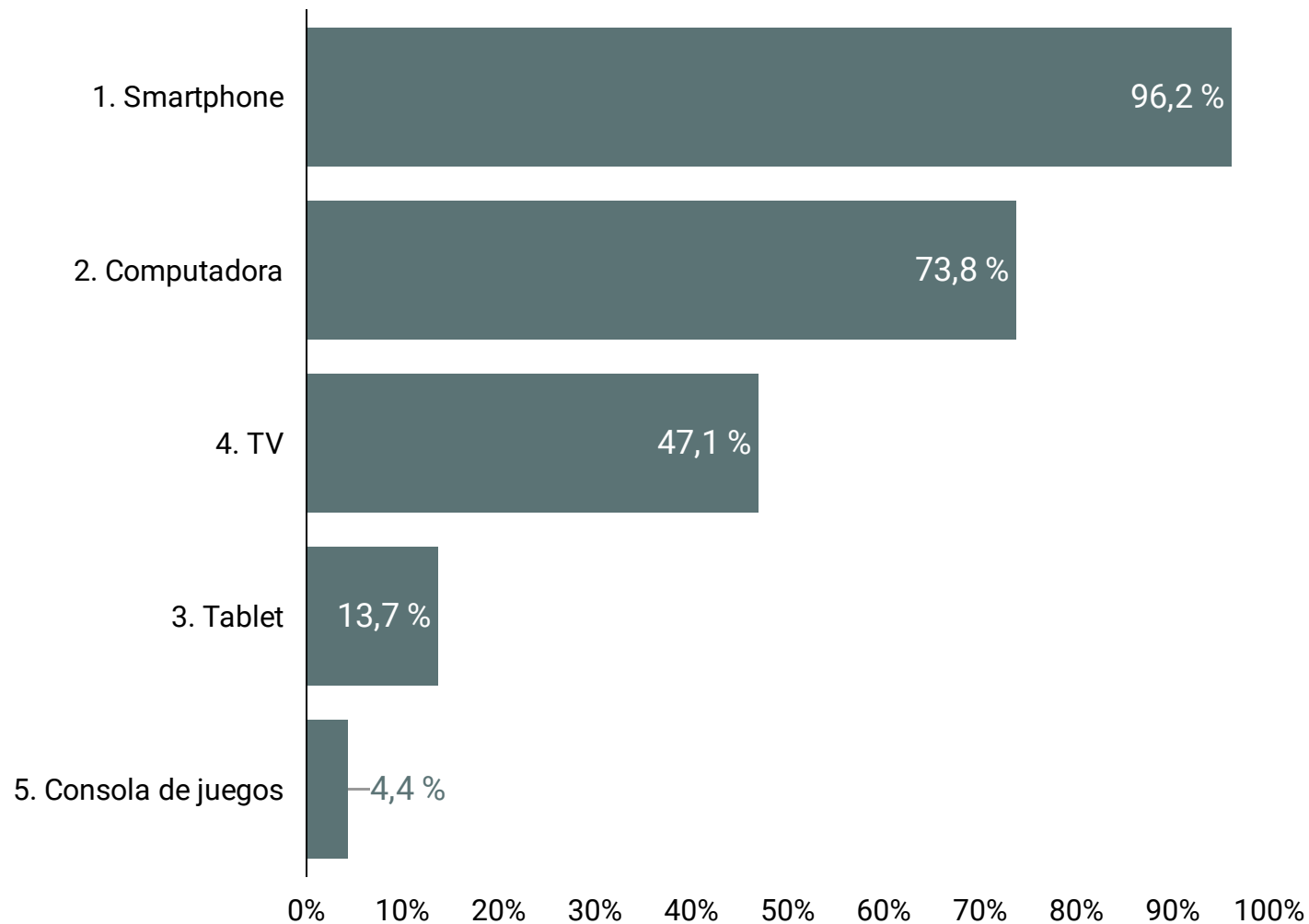
Los lugares desde donde los encuestados aseguran acceder a internet con mayor frecuencia son en sus viviendas y "en cualquier otro lugar con mis datos móviles".

La mayor mención de estas opciones permite inferir una preferencia por el uso de conexiones particulares.

En tercer y cuarto lugar se ubican el acceso a internet en el lugar de trabajo o en cualquier otro lugar donde se provea una conexión de wi-fi pública.

USO DE INTERNET. DISPOSITIVOS

¿Qué dispositivo usa para ingresar a internet?



Los dispositivos más utilizados para acceder a internet son los smartphones, los cuales fueron mencionados con una frecuencia del 96,2%.

En segundo lugar se ubican las computadoras personales (PC).

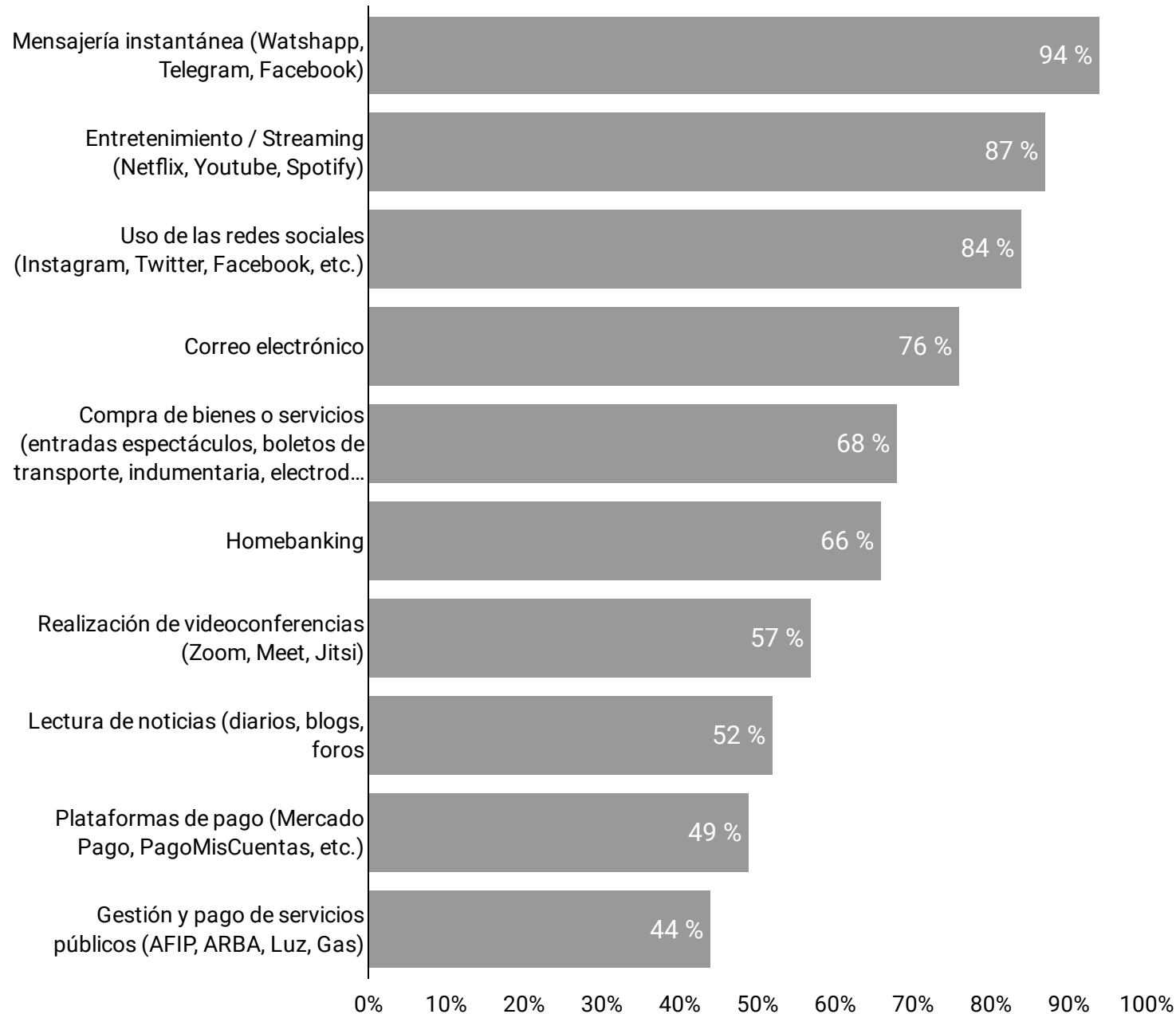
En tercer lugar aparecen los televisores.

Otros dispositivos mencionados con menor frecuencia son las tablets y las consolas de juegos.



USO DE INTERNET. ACTIVIDADES

Indique si usted realiza algunas de las siguientes actividades en internet.



La actividad más popular en internet es el uso de mensajería instantánea, la cual fue mencionada con una frecuencia del 94% por los encuestados.

La segunda actividad más habitual, mencionada con una frecuencia del 87%, es el uso de servicios de entretenimiento (Netflix, Youtube, Spotify). Casi la misma proporción accede a internet para usar redes sociales.

Un poco menos de encuestados accede a internet para enviar o recibir mails.

Con menor frecuencia aparecen realizar compras, gestiones en homebanking, asistir a videoconferencias, leer noticias o efectuar pagos por plataformas.



InFo-Lab



Observatorio
Universitario
de Mar del Plata

USO DE INTERNET. ACTIVIDADES

Indique si usted realiza algunas de las siguientes actividades en internet.

	Homebanking	Compra de bienes o servicios (entradas espectáculos, boletos de transporte, indumentaria, electrodomésticos, delivery, etc)	Venta de bienes o servicios	Uso de las redes sociales (Instagram, Twitter, Facebook, etc.)	Correo electrónico	Juegos en línea	Entretenimiento / Streaming (Netflix, Youtube, Spotify)	Lectura de noticias (diarios, blogs, foros)	Gestión y pago de servicios públicos (AFIP, ARBA, Luz, Gas)	E-Learning (Cursos en línea)	Mensajería instantánea (Watshapp, Telegram, Facebook)	Realización de videoconferencias (Zoom, Meet, Jitsi)	Plataformas de pago (Mercado Pago, PagoMisCuentas, etc.)	Plataformas de tarjetas de crédito (Visahome, Masterconsultas)
Femenino	63%	70%	23%	87%	80%	19%	87%	52%	45%	30%	94%	64%	48%	17%
Masculino	69%	65%	30%	80%	71%	22%	87%	52%	43%	20%	93%	48%	49%	17%
20 años o menos	16%	64%	28%	92%	84%	32%	92%	48%	20%	44%	100%	80%	36%	0%
21-35 años	72%	86%	38%	96%	86%	30%	96%	56%	41%	43%	95%	77%	62%	14%
36-50 años	89%	71%	32%	84%	84%	18%	88%	67%	59%	31%	91%	68%	72%	30%
51-65 años	74%	63%	22%	85%	75%	18%	81%	47%	50%	16%	94%	53%	43%	19%
66-80 años	35%	50%	7%	66%	54%	12%	79%	34%	29%	3%	96%	20%	15%	9%
más de 80 años	38%	31%	8%	54%	54%	0%	92%	46%	31%	0%	77%	8%	8%	8%
Primario	33%	21%	15%	79%	52%	24%	64%	36%	18%	6%	88%	18%	15%	9%
Secundario	59%	69%	33%	82%	69%	26%	89%	44%	34%	20%	93%	51%	50%	7%
Terciario/Universitario	74%	73%	23%	86%	83%	17%	89%	58%	53%	31%	95%	66%	52%	24%

Se observan algunas diferencias significativas en cuanto a las actividades realizadas a través de internet en función de las características sociodemográficas de los encuestados: sexo, edad y educación.



USO DE INTERNET. ACTIVIDADES

Indique si usted realiza algunas de las siguientes actividades en internet.

- 1. Homebanking:** Si bien no se observan diferencias significativas en cuanto al sexo, quienes realizan este tipo de operaciones con mayor frecuencia son los hombres, las personas de entre 36 y 65 años y los individuos con estudios terciarios/universitarios. Entre los que las realizan con menor frecuencia están las mujeres, las personas de menos de 20 y los mayores de 65 años, y los individuos con estudios primarios.
- 2. Compra de bienes o servicios:** Si bien no se observan diferencias significativas en cuanto al sexo, quienes realizan este tipo de actividad con mayor frecuencia son las mujeres, las personas de entre 21 y 35 años y quienes tienen estudios terciarios/universitarios. Los que menos las realizan son los hombres, las personas de más de 80 años y las que sólo alcanzaron estudios primarios.
- 3. Venta de bienes o servicios:** Quienes realizan este tipo de actividad con mayor frecuencia son los hombres, las personas de entre 21 y 50 años y los individuos con estudios secundarios. Los que menos las realizan son las mujeres, las personas de más de 66 años y las que sólo alcanzaron estudios primarios.
- 4. Uso de redes sociales:** No se observan diferencias significativas en cuanto al sexo. Quienes más realizan esta actividad son las personas menores de 35 años. Los que menos las realizan son las personas de más de 66 años. El uso de redes sociales disminuye a medida que se incrementa el valor de los rangos etarios.
- 5. Correo electrónico:** Quienes realizan este tipo de actividad con mayor frecuencia son las mujeres, las personas menores de 50 años e individuos con estudios terciarios/universitarios.
- 6. Juegos en línea:** Quienes realizan este tipo de actividad con mayor frecuencia son los varones, las personas menores de 35 años y los individuos con estudios secundarios. Los que menos las realizan son las mujeres, las personas de más de 80 años y las que poseen estudios terciarios/universitarios.
- 7. Entretenimiento/Streaming:** No se observan diferencias estadísticamente significativas por sexo, edad y educación. Se aprecia una frecuencia ligeramente menor entre las personas que poseen estudios primarios.

USO DE INTERNET. ACTIVIDADES

Indique si usted realiza algunas de las siguientes actividades en internet.

8. Lectura de noticias: No se observan diferencias en cuanto al sexo. Se aprecia que realizan esta actividad con mayor frecuencia quienes poseen entre 36 y 50 años y las personas con estudios terciarios/universitarios.

9. Gestión y pago de servicios: Quienes más realizan estas operaciones son las personas de entre 36 y 50 años y las que poseen estudios terciarios/universitarios

10 E-Learning: Se observa que esta actividad es realizada con mayor frecuencia por mujeres, por personas de menos de 35 años e individuos con estudios terciarios/universitarios. Se observa una marcada disminución de la tendencia a realizar esta actividad en función del aumento de la edad y del menor nivel educativo alcanzado.

11 Mensajería instantánea: No se observan diferencias en cuanto al sexo. En relación a la edad se aprecia que esta actividad es realizada por el 100% de los menores de 20 años. No se advierten diferencias relevantes con el resto de los rangos etarios, aunque se observa una menor frecuencia de uso entre los mayores de 80.

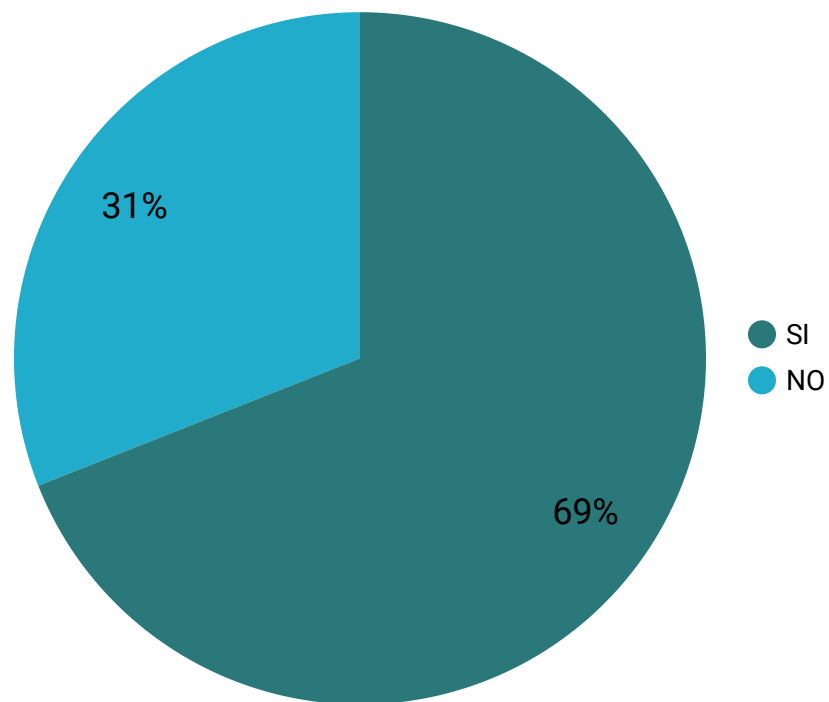
12 Videoconferencias: Quienes realizan este tipo de actividad con mayor frecuencia son las mujeres, los menores de 20 años y las personas con estudios terciarios/universitarios. Se observa una marcada disminución de la tendencia a realizar esta actividad en función del aumento de la edad y del menor nivel educativo alcanzado.

13 Plataformas de pago: No se observan diferencias por sexo. Las personas que realizan esta actividad con mayor frecuencia son las que poseen entre 36 y 50 años y estudios terciarios/universitarios.

14 Plataformas de tarjetas de crédito: No se observan diferencias por sexo. Las personas que realizan esta actividad con mayor frecuencia son las que poseen entre 36 y 50 años y los individuos que poseen estudios terciarios/universitarios.

USO DE INTERNET. PREOCUPACIÓN

¿Le genera algún tipo de preocupación realizar compras u operaciones bancarias a través de internet?



El 69% de las personas consultadas (7 de cada 10 encuestados) asegura que le genera algún tipo de preocupación realizar compras u operaciones bancarias a través de internet.

Por otra parte el 31% (3 de cada 10) afirma lo contrario.



USO DE INTERNET. PREOCUPACIÓN

¿Le genera algún tipo de preocupación realizar compras u operaciones bancarias a través de internet?

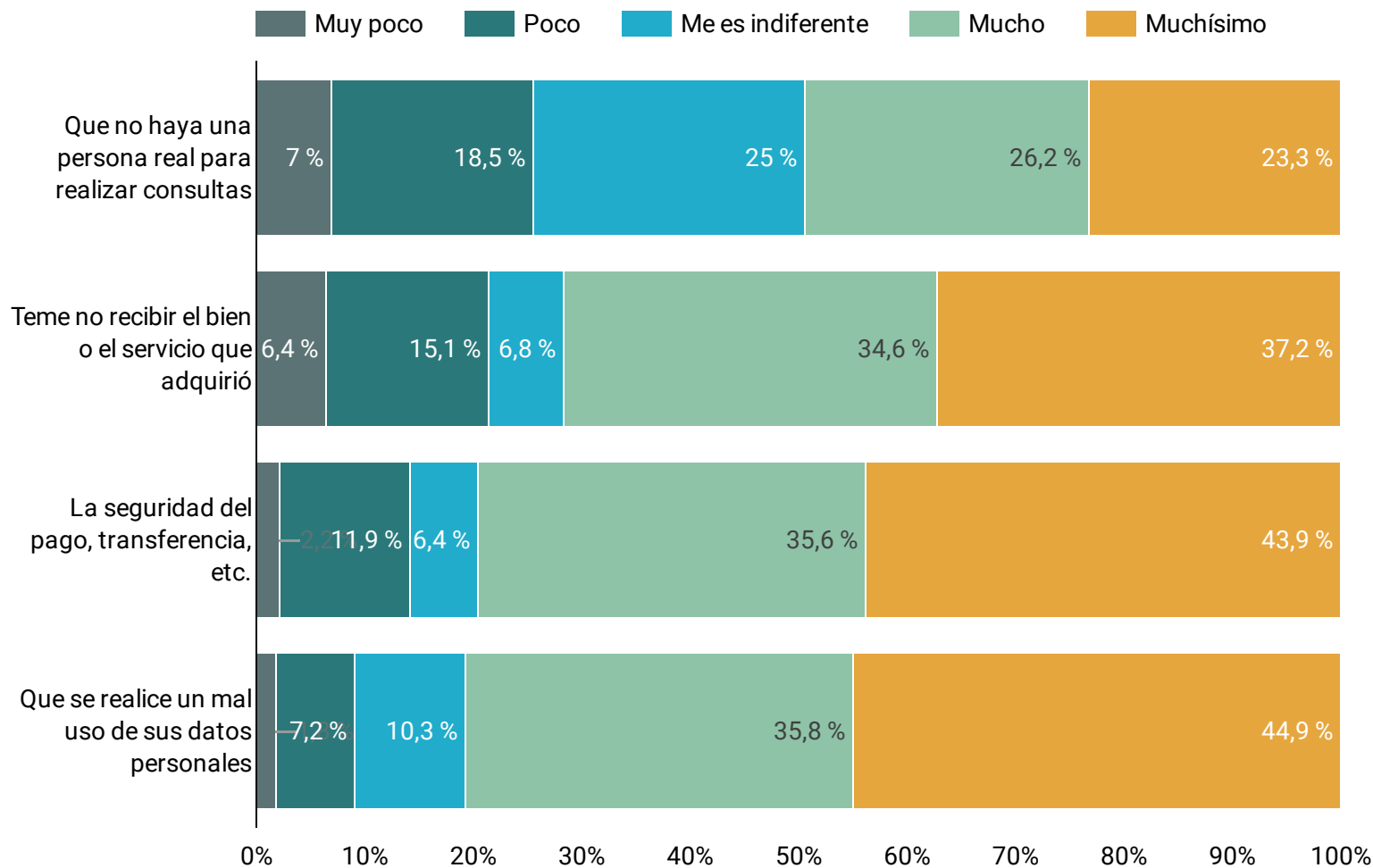
	NO	SI
Femenino	33%	67%
Masculino	29%	71%
20 años o menos	44%	56%
21-35 años	44%	56%
36-50 años	31%	69%
51-65 años	24%	76%
66-80 años	19%	81%
más de 80 años	23%	77%
Primario	30%	70%
Secundario	28%	72%
Terciario/Universitario	33%	67%

Se aprecia que la realización de estas actividades genera mayor preocupación entre las personas de mayor edad, en especial, entre las de más de 51 años.



TRANSACCIONES POR INTERNET. PREOCUPACIÓN

¿Cuánto le preocupan las siguientes situaciones al realizar compras u operaciones bancarias a través de internet?



Las situaciones que generan mayor preocupación entre los encuestados al realizar compras u operaciones bancarias a través de internet son:

1- Que se realice un mal uso de los datos personales suministrados.

2- La seguridad en el pago, la transferencia, etc

Al analizar los resultados por sexo, edad y nivel de estudios no se observan diferencias relevantes en las respuestas obtenidas en cada uno de los grupos.



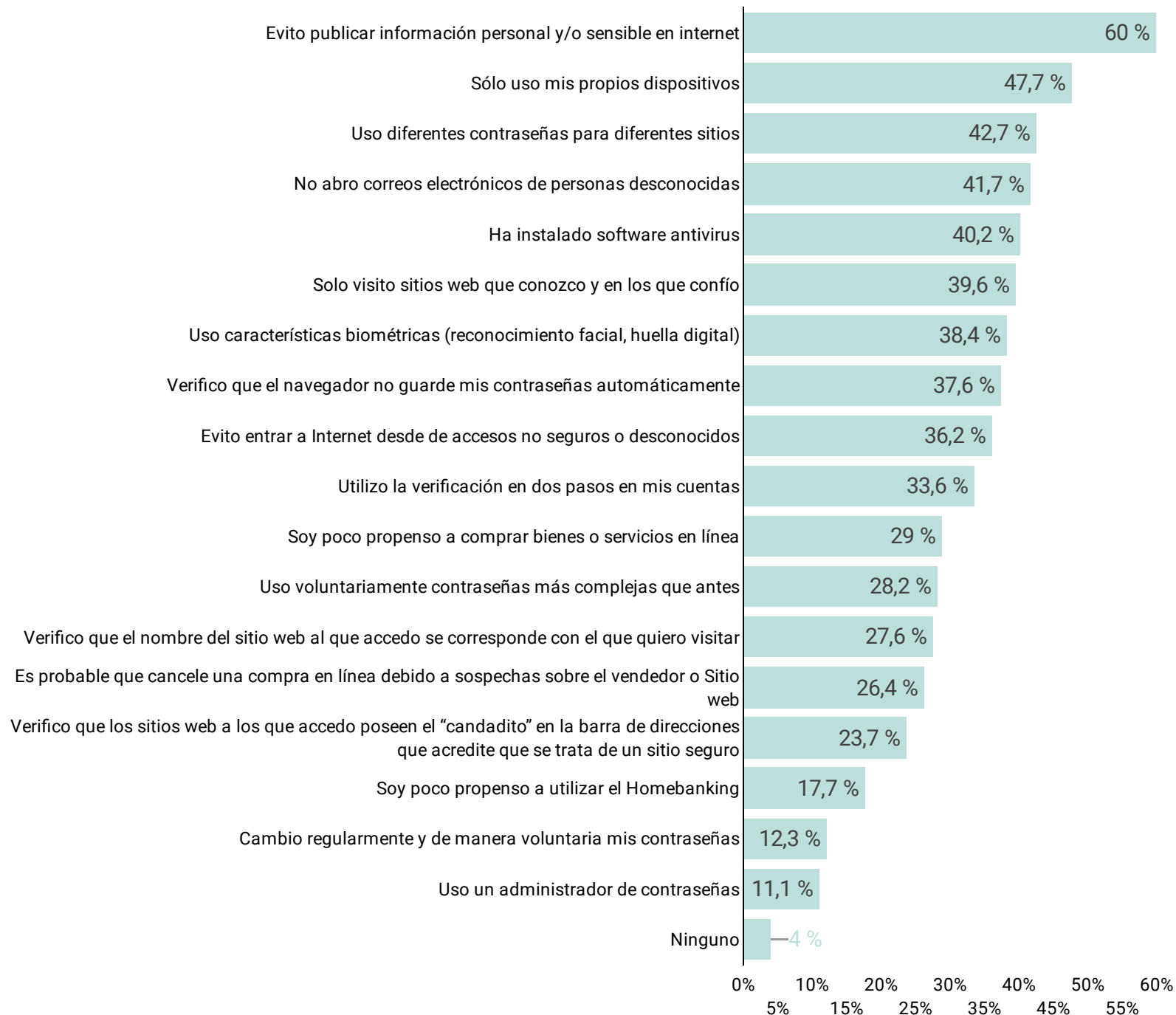
InFo-Lab



Observatorio
Universitario
de Mar del Plata

TRANSACCIONES POR INTERNET. MEDIDAS DE PREVENCIÓN

Indique si implementa algunas de las siguientes medidas por temor a ver vulnerada su seguridad en internet



La estrategia mencionada con mayor frecuencia como medida para evitar una vulneración de la seguridad consiste en evitar publicar información personal y/o sensible en la web.

Entre las más mencionadas también se destacan utilizar únicamente dispositivos propios, utilizar diferentes contraseñas en diferentes sitios, y no abrir correos electrónicos de origen desconocido



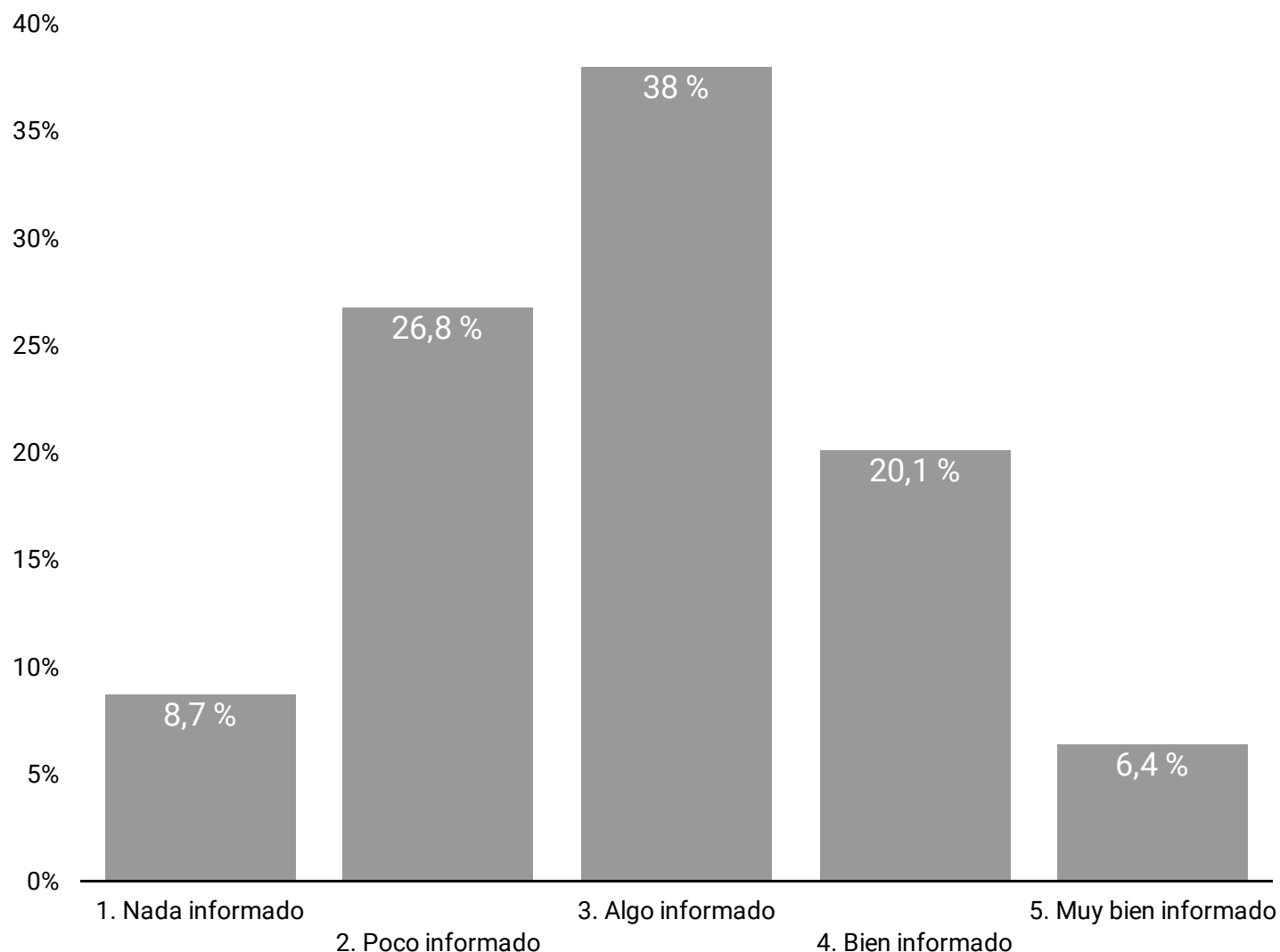
InFo-Lab



Observatorio
Universitario
de Mar del Plata

CIBERCRIMEN. INFORMACIÓN

¿Cuán bien informado considera que usted está acerca de los riesgos del cibercrimen?



El 26,5% de los encuestados considera estar bien o muy bien informado acerca de los riesgos del cibercrimen.

El 73,5% reconoce estar informado de manera deficiente, ya sea porque asume estar algo informado (38%), poco informado (26,8%) o nada informado (8,7%).



CIBERCRIMEN. INFORMACIÓN

¿Cuán bien informado considera que usted está acerca de los riesgos del cibercrimen?

	Nada informado	Poco informado	Algo informado	Bien informado	Muy bien informado
Femenino	7%	27%	41%	21%	4%
Masculino	10%	27%	34%	19%	10%
20 años o menos	16%	24%	32%	28%	0%
21-35 años	5%	18%	41%	28%	8%
36-50 años	3%	26%	47%	16%	7%
51-65 años	9%	32%	34%	18%	7%
66-80 años	19%	35%	30%	12%	4%
más de 80 años	0%	31%	31%	31%	8%
Primario	27%	33%	33%	3%	3%
Secundario	10%	32%	39%	16%	3%
Terciario/Universitario	6%	23%	38%	25%	9%

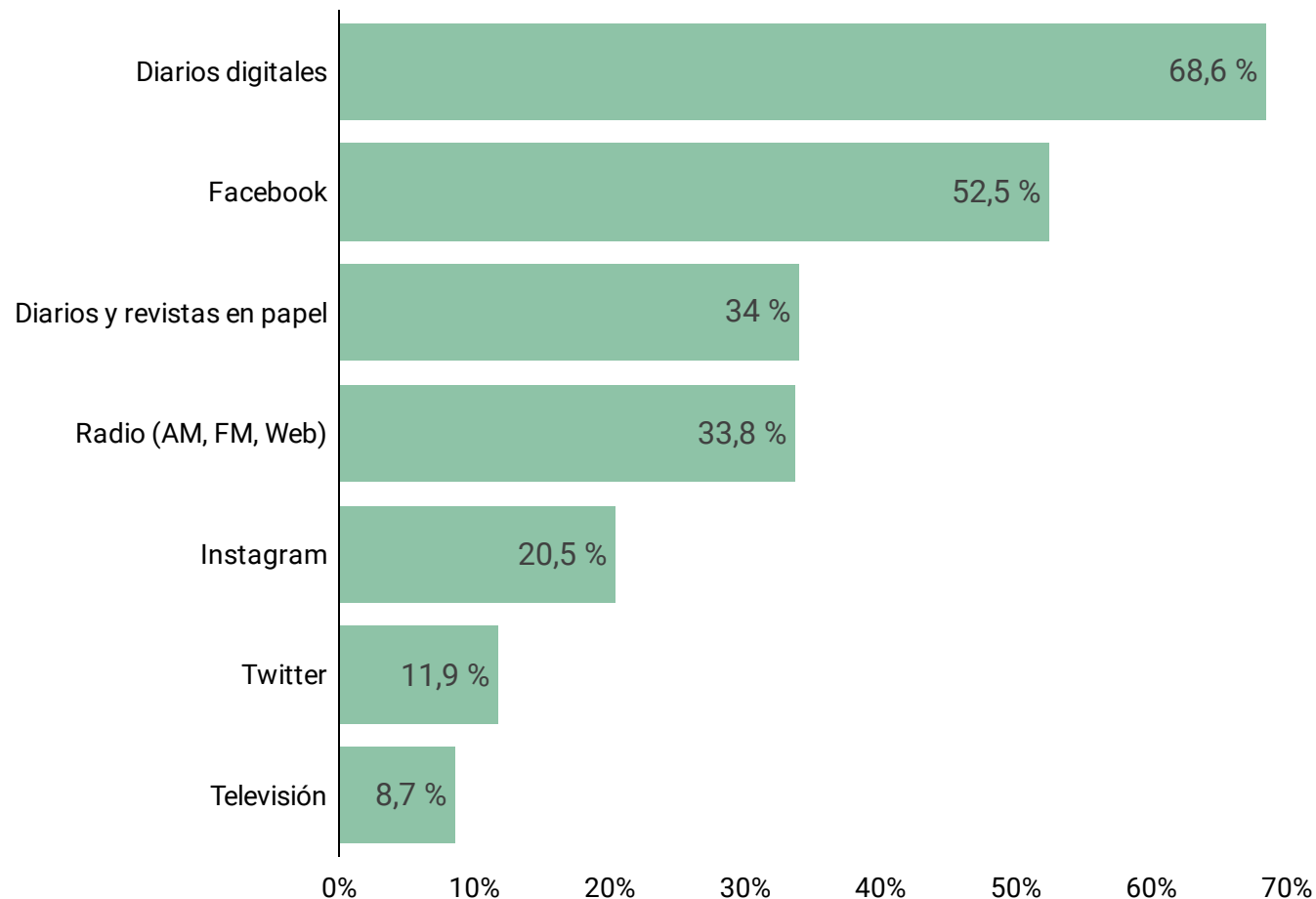
Se observa que la mayor frecuencia se registra en la opción algo informado.

En relación a la edad se advierte que la mayor proporción de quienes manifiestan tener algo de información se registra en el rango etario de 21 a 50 años.



CIBERCRIMEN. INFORMACIÓN

¿Qué medios utiliza principalmente para informarse sobre noticias de actualidad?

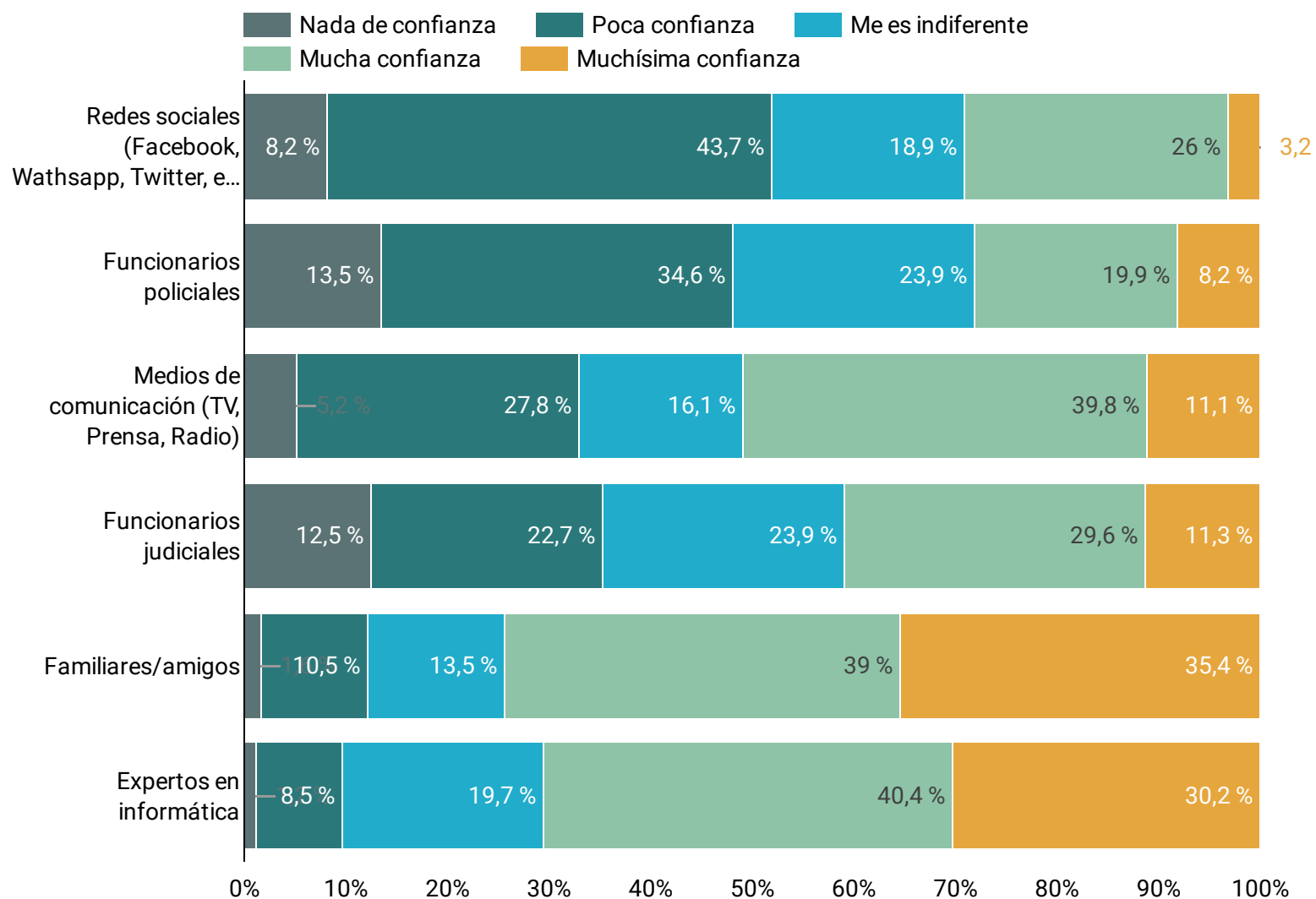


Los tres medios utilizados con mayor frecuencia para informarse sobre asuntos de actualidad son: diarios digitales, Facebook y diarios y revistas de en papel.



CIBERCRIMEN. INFORMACIÓN

¿Qué nivel de confianza les asigna a las siguientes fuentes de información en relación a la seguridad en internet?



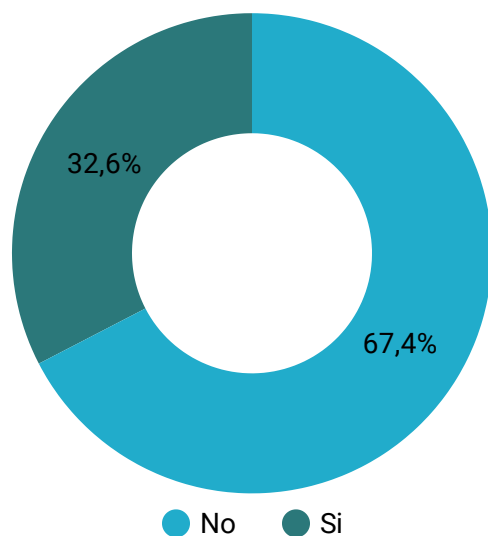
Las fuentes a las que se les asigna mayor confianza para informarse sobre seguridad en internet son familiares y/o amigos y expertos en informática.

Las fuentes a las que se les asigna menor confianza son las redes sociales y los funcionarios policiales y judiciales.

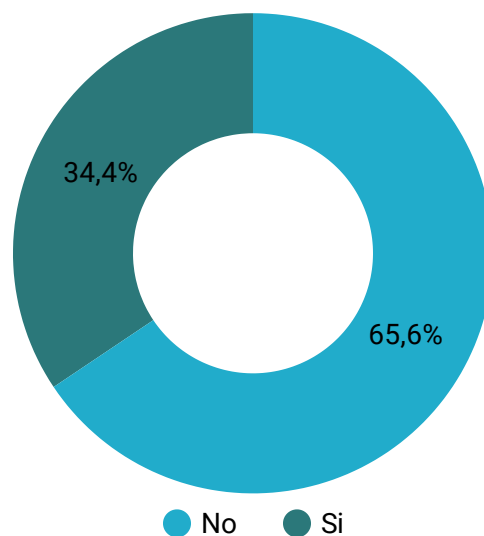


CIBERCRIMEN. INTERACCIÓN CON AMENAZAS

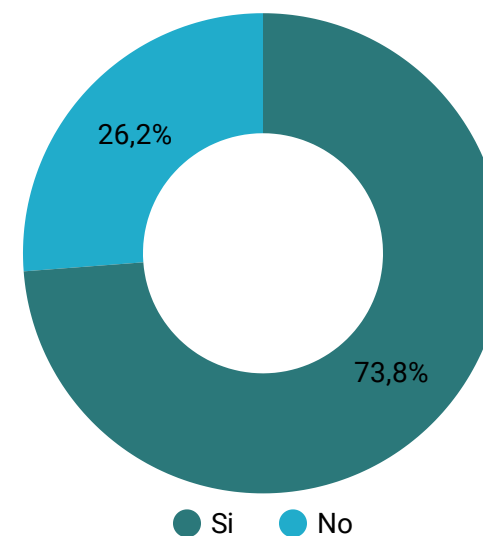
¿Ha recibido correos electrónicos, mensajes de texto o mensajería instantánea diciéndole que le habían bloqueado su cuenta y debía hacer clic en un link adjunto para volver a activarla?



¿Ha recibido llamados telefónicos solicitándole datos personales (números de tarjetas de crédito, claves de seguridad, tokens, documentos, etc.)?



¿Ha recibido mensajes de texto o mensajería instantánea diciéndole que había ganado un premio o cierta empresa estaba lanzando alguna oferta o beneficio?



Considerando las estrategias que pueden dar origen a un fraude a través de internet los encuestados fueron consultados sobre si experimentaron algunas de las siguientes situaciones de manera reciente. En ese sentido se observa que:

El 32,6% recibió correos o mensajes diciéndole que habían bloqueado su cuenta y que debía hacer clic en un link para volver a activarla.

El 34,4% recibió llamados telefónicos solicitándole datos personales.

El 73,8% recibió mensajes diciéndole que había ganado un premio o sobre el lanzamiento de una oferta o beneficio.



CIBERCRIMEN. INTERACCIÓN CON AMENAZAS

	¿Ha recibido correos electrónicos, mensajes de texto o mensajería instantánea diciéndole que le habían bloqueado su cuenta y debía hacer clic en un link adjunto para volver a activarla?	¿Ha recibido llamados telefónicos solicitándole datos personales (números de tarjetas de crédito, claves de seguridad, tokens, documentos, etc.)?	¿Ha recibido mensajes de texto o mensajería instantánea diciéndole que había ganado un premio o cierta empresa estaba lanzado alguna oferta o beneficio?
Femenino	33%	36%	77%
Masculino	32%	32%	70%
20 años o menos	24%	28%	72%
21-35 años	34%	28%	79%
36-50 años	44%	34%	81%
51-65 años	31%	36%	70%
66-80 años	22%	47%	64%
más de 80 años	23%	15%	62%
Primario	9%	30%	55%
Secundario	23%	32%	73%
Terciario/Universitario	41%	36%	77%

Al segmentar los datos por variable sociodemográficas no se perciben diferencias significativas en cuanto a sexo. En relación a la edad y al nivel de estudios se observa que reconocen con más frecuencia :

Haber recibido correos o mensajes diciéndole que habían bloqueado su cuenta y que debía hacer clic en un link para volver a activarla las personas de entre 21 y 50 años y los individuos con estudios terciarios/universitarios.

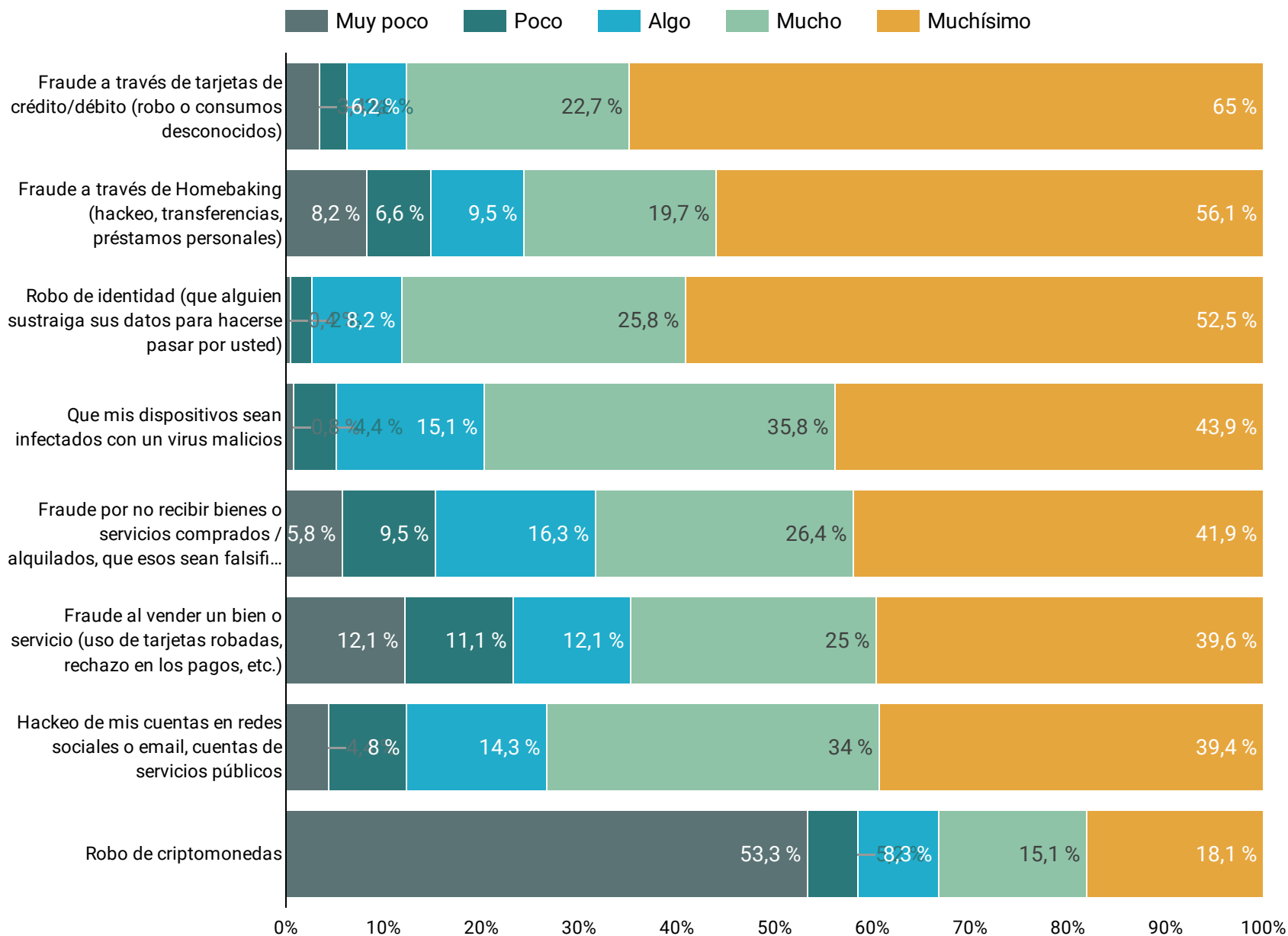
Haber recibido llamados telefónicos solicitándole datos personales, las personas de entre 66 y 80 años

Haber recibido mensajes diciéndole que había ganado un premio o sobre el lanzamiento de una oferta o beneficio, las personas de entre 36 y 50 años y los individuos con estudios terciarios/universitarios.



CIBERCRIMEN. PREOCUPACIÓN

El ciberdelito puede ser cometido de diversas maneras. ¿Cuánto le preocupa ser víctima de alguna de las siguientes modalidades?



Las modalidades de ciberdelito que más preocupan a los encuestados consisten en:

Ser víctima de un fraude a través de tarjetas de crédito/débito.

Ser víctima de un fraude a través del servicio de homebanking.

Sufrir un robo de identidad mediante el uso de datos personales.



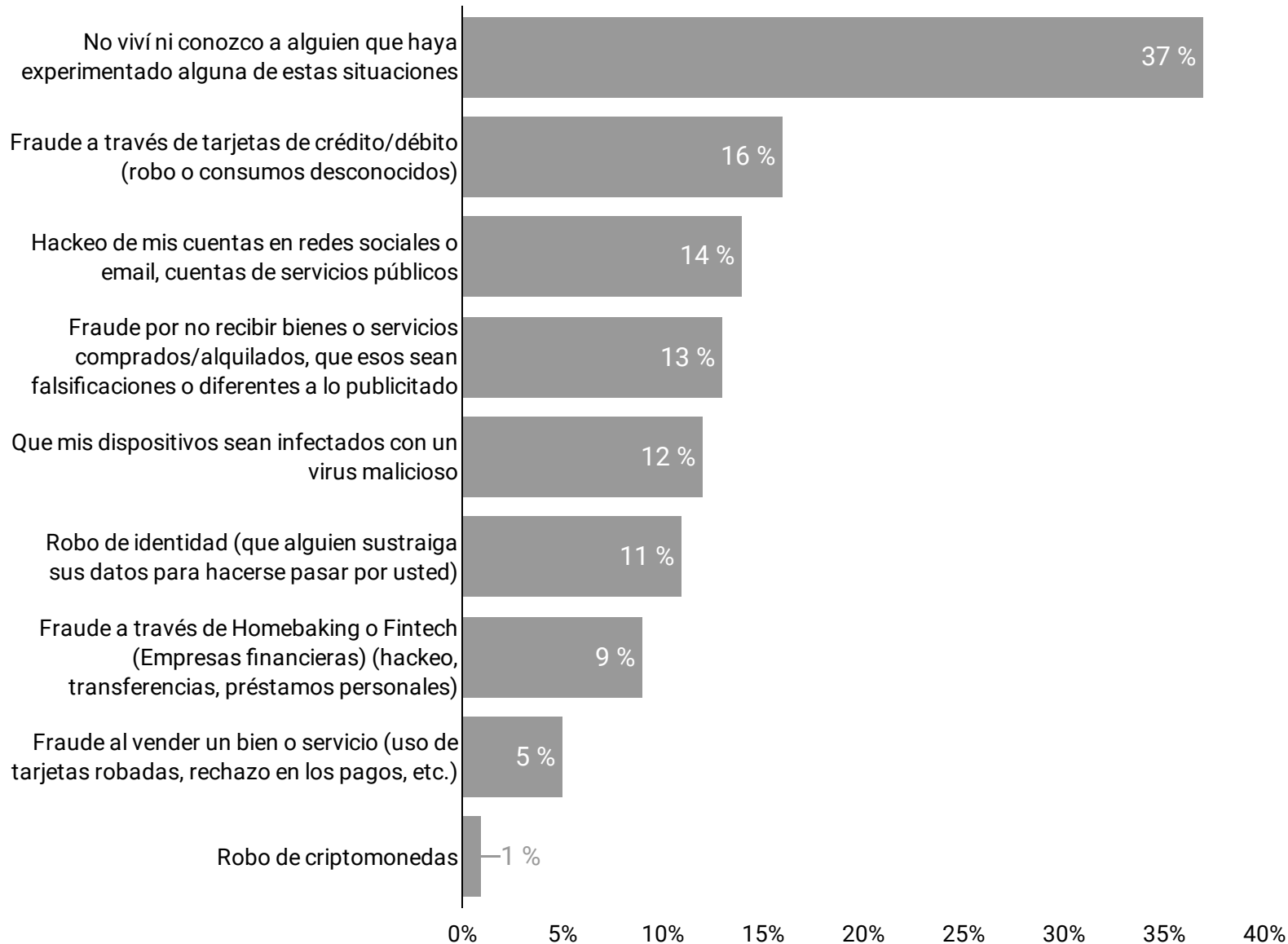
InFo-Lab



Observatorio
Universitario
de Mar del Plata

CIBERCRIMEN. EXPERIENCIAS

¿En el último año, usted, algún familiar, amigo o conocido ha vivido alguna de las siguientes situaciones?



El 63% (6 de cada 10 personas) de los encuestados sí vivió o supo que algún allegado sufrió en el último año algunas de las modalidades de ciberdelito consideradas.

Las tres mencionadas de manera más frecuentes son:

Fraude a través de tarjeta crédito/débito.

Hackeo de cuentas en redes sociales, mail, etc

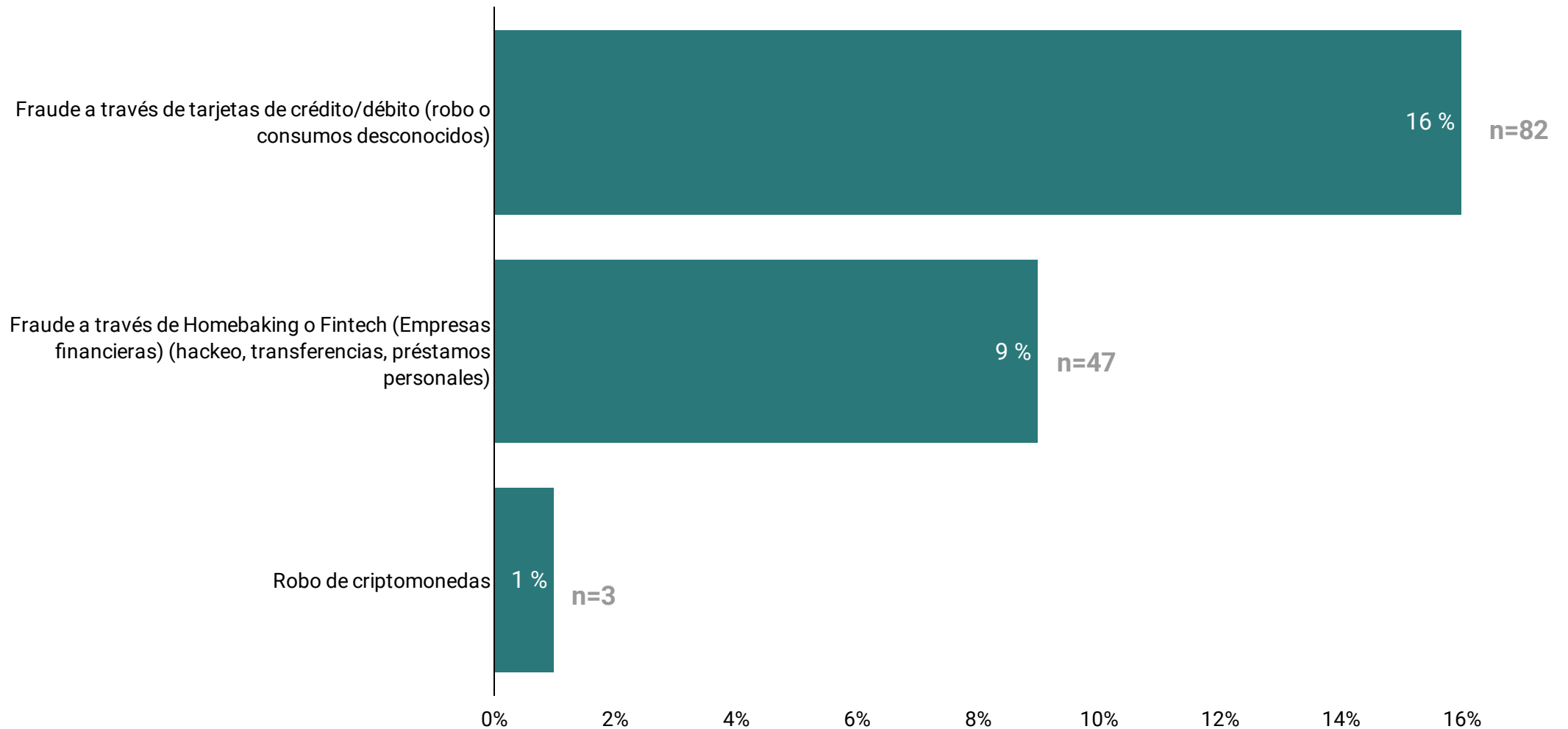
No haber recibido bienes o servicios en las condiciones adquiridas.

Por otro lado, 37% de los encuestados asegura no haber vivido ni sabido de que algún allegado haya sufrido alguna de estas situaciones.



CIBERCRIMEN. EXPERIENCIAS

¿En el último año, usted, algún familiar, amigo o conocido ha vivido alguna de las siguientes situaciones?



CIBERCRIMEN. EXPERIENCIAS

Antes de haberse dado cuenta de qué le sucedió ¿recuerda que haya vivido alguna de estas situaciones?

Los encuestados que reconocen haber sido víctimas de fraude a través de tarjetas de crédito/débito recordaron que antes de haber detectado lo ocurrido vivieron las siguientes situaciones:

Respuesta	4. Fraude a través de tarjetas de crédito/débito (robo o consumos desconocidos) ▾
Recibí una llamada telefónica de una persona diciendo que era de un banco, entidad pública, etc. en la cual me pedían datos personales como número de tarjeta de crédito/débito, me hizo ir a un cajero automático para brindarle un número o código de seguridad	29,3 %
No recuerdo	23,2 %
Accedí a un correo electrónico donde me informaban que mi cuenta de la tarjeta o banco estaba suspendida y debía acceder a un enlace en dicho correo	18,3 %
Ingresé a una tienda online, realicé una compra y luego vi consumos desconocidos en mi tarjeta de crédito/débito	14,6 %
Busqué en Google o similar el sitio web de esa empresa o institución	6,1 %
Me hackearon mi cuenta de correo y a través de eso accedieron y/o restablecieron mis cuentas bancarias y/o de servicios públicos y/o billeteras de criptomonedas	1,2 %
Perdí o me robaron el celular y accedieron a mi cuenta	1,2 %
Me comuniqué con la cuenta o perfil de una empresa o institución en una red social	1,2 %



CIBERCRIMEN. EXPERIENCIAS

Antes de haberse dado cuenta de qué le sucedió ¿recuerda que haya vivido alguna de estas situaciones?

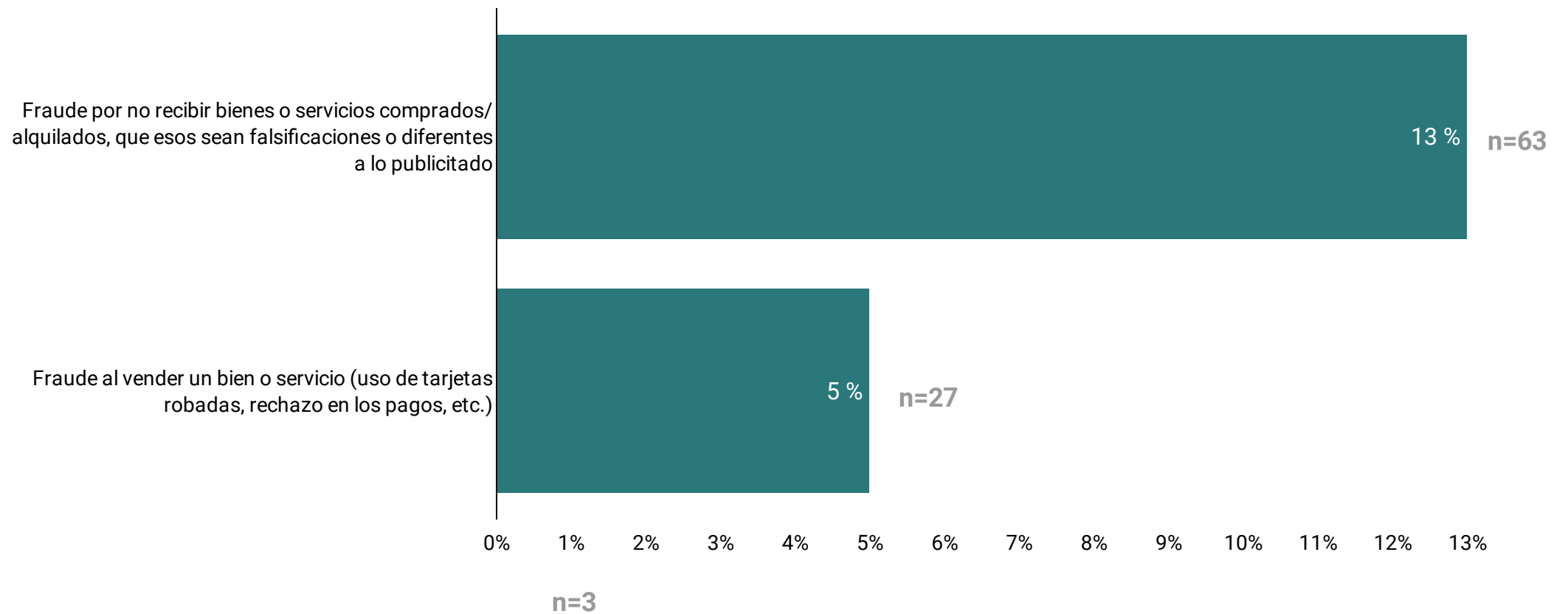
Los encuestados que reconocen haber sido víctimas de fraude a través de Homebanking o Fintech recordaron que antes de haber detectado lo ocurrido vivieron las siguientes situaciones:

Respuesta	5. Fraude a través de Homebaking o Fintech (Empresas financieras) (hackeo, transferencias, préstamos personales)
Me comuniqué con la cuenta o perfil de una empresa o institución en una red social	25,02 %
No recuerdo	23,04 %
Busqué en Google o similar el sitio web de esa empresa o institución	15,36 %
Accedí a un correo electrónico donde me informaban que mi cuenta de la tarjeta o banco estaba suspendida y debía acceder a un enlace en dicho correo	13,46 %
Recibí una llamada telefónica de una persona diciendo que era de un banco, entidad pública, etc. en la cual me pedían datos personales como número de tarjeta de crédito/débito, me hizo ir a un cajero automático para brindarle un número o código de seguridad	13,46 %
Ingresé a una tienda online, realicé una compra y luego vi consumos desconocidos en mi tarjeta de crédito/débito	5,78 %
Perdí o me robaron el celular y accedieron a mi cuenta	3,88 %
Me hackearon mi cuenta de correo y a través de eso accedieron y/o restablecieron mis cuentas bancarias y/o de servicios públicos y/o billeteras de criptomonedas	0 %



CIBERCRIMEN. EXPERIENCIAS

¿En el último año, usted, algún familiar, amigo o conocido ha vivido alguna de las siguientes situaciones?



CIBERCRIMEN. EXPERIENCIAS

¿Por qué canal realizó la operación?

Los encuestados que reconocen haber sido víctimas de fraude por no recibir bienes o servicios comprados/alquilados, que sean falsificados o diferentes a lo publicitado o haber sufrido fraude al vender un bien o servicio indicaron haber realizado estas operaciones mediante los siguientes canales:

Canal de la operación	7. Fraude por no recibir bienes o servicios comprados/alquilados, que esos sean falsificaciones o diferentes a lo publicitado	8. Fraude al vender un bien o servicio (uso de tarjetas robadas, rechazo en los pagos, etc.)
Redes sociales (Market Place o similar)	61,3 %	57,7 %
Sitio online dedicado a compra y venta de bienes y servicios (Mercado Libre, TiendaMía, etc.)	29 %	23,1 %
Tienda online empresa	6,5 %	7,7 %
Mensajería instantánea	3,2 %	11,5 %



CIBERCRIMEN. EXPERIENCIAS

¿Recuerda haber realizado alguna de las siguientes operaciones?

Los encuestados que reconocen haber sido víctimas de fraude por no recibir bienes o servicios comprados/alquilados, que sean falsificados o diferentes a lo publicitado o haber sufrido fraude al vender un bien o servicio indicaron haber realizado los siguientes tipo de operaciones:

Operaciones	7. Fraude por no recibir bienes o servicios comprados/alquilados, que esos sean falsificaciones o diferentes a lo publicitado ▾	8. Fraude al vender un bien o servicio (uso de tarjetas robadas, rechazo en los pagos, etc.)
Alquilé un inmueble y éste no existía	25,43 %	7,4 %
No recuerdo / no contesta	20,62 %	25,9 %
Ingresé a una tienda online, me hicieron hacer una transferencia o pago (Ripsa, Rapi pago, etc.) y no recibí el producto	20,62 %	3,7 %
Realicé una compra/venta a través de redes sociales o mensajería instantánea y no recibí el dinero o producto	19,02 %	18,5 %
Vendí un producto, me mandaron un comprobante de transferencia o pago y que era falso o el mismo fue rechazado posteriormente	14,31 %	44,4 %



CIBERCRIMEN. EXPERIENCIAS

¿Cuál fue su reacción cuando usted experimentó alguna de las siguientes situaciones?

Tras haber detectado situaciones anómalas que potencialmente podrían ser el origen de un ciberdelito, los encuestados aseguraron haber reaccionado del siguiente modo:

Respuesta	1. Recibí una llamada telefónica de una persona diciendo que era de un banco, entidad pública, etc. en la cual me pedían datos personales como número de tarjeta de crédito/débito, me hizo ir a un cajero automático para brindarle un número o código de seguridad	2. Accedí a un correo electrónico donde me informaban que mi cuenta de la tarjeta o banco estaba suspendida y debía acceder a un enlace en dicho correo	3. Me comuniqué con la cuenta o perfil de una empresa o institución en una red social
Contacté al sitio web/ proveedor	22,4 %	36,4 %	37,1 %
Reporté la situación al sitio o al mail de contacto	15,5 %	34,5 %	30 %
Contacté al banco	13,8 %	23,6 %	14,3 %
Contacté a la policía/fiscalía	13,8 %	23,6 %	14,3 %
Contacté a mi proveedor de tarjeta de crédito/débito	12,1 %	20 %	12,9 %
No sabe / No recuerda	10,3 %	12,7 %	12,9 %
Nada	17,2 %	12,7 %	17,1 %
Contacté a un organismo de defensa del consumidor	6,9 %	12,7 %	10 %
Contacté a mi proveedor de internet	3,4 %	10,9 %	8,6 %

CIBERCRIMEN. EXPERIENCIAS

¿Cuál fue su reacción cuando usted experimentó alguna de las situaciones anteriores?

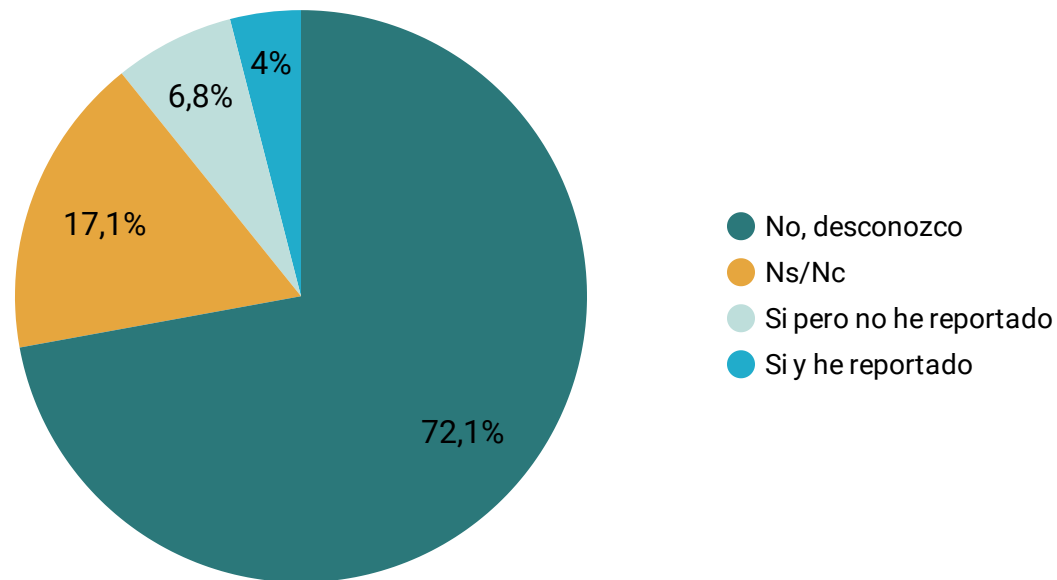
Tras haber constatado ser víctimas de un ciberdelito de fraude, los encuestados aseguraron haber reaccionado del siguiente modo:

Respuesta	4. Fraude a través de tarjetas de crédito/débito (robo o consumos desconocidos)	5. Fraude a través de Homebaking o Fintech (Empresas financieras) (hackeo, transferencias, préstamos personales)
Contacté al sitio web/ proveedor	20,6 %	29,6 %
Reporté la situación al sitio o al mail de contacto	22,2 %	51,9 %
Contacté al banco	68,3 %	51,9 %
Contacté a la policía/fiscalía	30,2 %	22,2 %
Contacté a mi proveedor de tarjeta de crédito/débito	42,9 %	25,9 %
No sabe / No recuerda	11,1 %	29,6 %
Nada	9,5 %	29,6 %
Contacté a un organismo de defensa del consumidor	22,2 %	11,1 %
Contacté a mi proveedor de internet	6,3 %	7,4 %



CIBERCRIMEN. EXPERIENCIAS

¿Conoce sobre la existencia de algún sitio en internet, e mail oficiales donde pueda reportar la existencia de un ciberdelito?



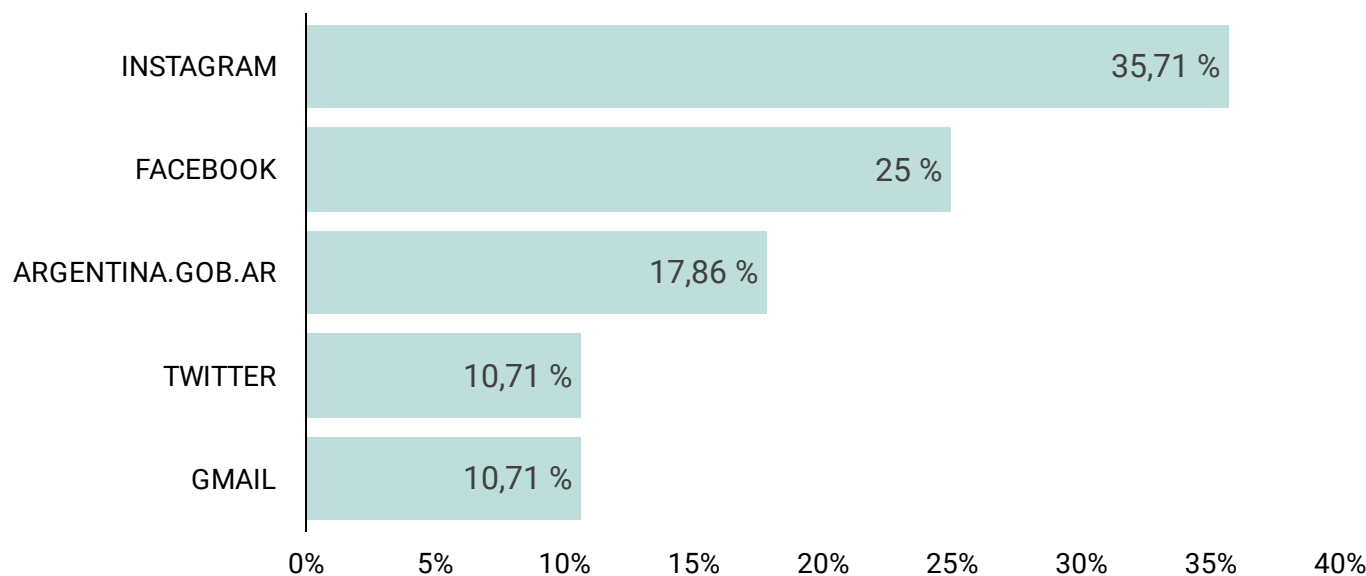
El 72,1% asegura desconocer dónde reportar mediante internet un ciberdelito y el 17,1% no sabe o no contesta a la pregunta.

Sólo el 10,8% afirma conocer dónde denunciar un caso.

Entre quienes aseguran sí conocer dónde reportar la situación el 82,14% alude a las empresas proveedoras de servicios como Instagram, Facebook, Twitter o Gmail.

En tanto que el 17,86% menciona al sitio web argentina.gob.ar

Si contestó que conoce, ¿Cuál?



CONCLUSIONES

El 90,7% de los encuestados asegura acceder a internet en forma diaria.

Al segmentar las respuestas por características sociodemográficas no se observan diferencias significativas en relación al sexo. Existen diferencias significativas en la distribución por edades entre los menores y los mayores de 66 años. Los más propensos a usar internet diariamente son los menores de 66 años. Se aprecia que a medida que la edad avanza, las personas son menos propensas a utilizar internet diariamente. Si bien la frecuencia de acceso a internet es elevada entre las personas más allá de su nivel educativo, se observa que su uso es ligeramente menor entre quienes sólo alcanzaron el nivel primario.

Los lugares desde donde los encuestados aseguran acceder a internet con mayor frecuencia son en sus viviendas y "en cualquier otro lugar con mis datos móviles". La mayor mención de estas opciones permite inferir una preferencia por el uso de conexiones particulares.

Los dispositivos más utilizados para acceder a internet son los smartphones, los cuales fueron mencionados con una frecuencia del 96,2%. En segundo lugar se ubican las computadoras personales (PC). En tercer lugar aparecen los televisores. Otros dispositivos mencionados con menor frecuencia son las tablets y las consolas de juegos.

La actividad más popular en internet es el uso de mensajería instantánea, la cual fue mencionada con una frecuencia del 94% por los encuestados. La segunda actividad más habitual, mencionada con una frecuencia del 87%, es el uso de servicios de entretenimiento (Netflix, Youtube, Spotify) Casi la misma proporción accede a internet para usar redes sociales. Un poco menos de encuestados accede a internet para enviar o recibir mails. Con menor frecuencia aparecen realizar compras, gestiones en homebanking, asistir a videoconferencias, leer noticias o efectuar pagos por plataformas.

Se observan diversas diferencias significativas en cuanto a las actividades realizadas a través de internet en función de las características sociodemográficas de los encuestados: sexo, edad y educación.



CONCLUSIONES

El 69% de las personas consultadas (7 de cada 10 encuestados) asegura que le genera algún tipo de preocupación realizar compras u operaciones bancarias a través de internet. Por otra parte el 31% (3 de cada 10) afirma lo contrario.

Se aprecia que realizar compras u operaciones bancarias a través de internet genera mayor preocupación entre las personas de mayor edad, en especial, entre las de más de 51 años. Las situaciones que generan mayor preocupación entre los encuestados al realizar compras u operaciones bancarias a través de internet son: Que se realice un mal uso de los datos personales suministrados y la seguridad en el pago, la transferencia, etc Al analizar los resultados por sexo, edad y nivel de estudios no se observan diferencias relevantes en las respuestas obtenidas en cada uno de los grupos.

La estrategia mencionada con mayor frecuencia para evitar una vulneración de la seguridad consiste en evitar publicar información personal y/o sensible en la web. Entre las más mencionadas también se destacan utilizar únicamente dispositivos propios, utilizar diferentes contraseñas en diferentes sitios, y no abrir correos electrónicos de origen desconocido.

Desde la línea de ciberseguridad del Info-Lab se considera que una de las medidas más importantes para proteger nuestras cuentas, es la implementación de la verificación en dos pasos o doble factor de autenticación. Esta característica imposibilita a que, delincuentes, puedan acceder a nuestras cuentas con solo poseer la clave.

Sin embargo, lo que se observa en estos resultados, es que solo un 33.6% han implementado esta medida. Esto es una de las cuestiones que se deben fomentar sobre el uso de esta medida en particular. Por otro parte, sólo el 27,6% verifica que el nombre del sitio web al que accede se corresponda con el sitio al que quiere visitar. Esta es otra de las medidas de las cuales hay que fomentar. Hoy en día, el phishing o suplantación de identidad, es una de las técnicas más habituales para robar información a los usuarios de Internet y, si las personas no verifican que el nombre de la URL o sitio web al que acceden sea correcto, podrían caer en este engaño y les roben sus datos personales, acceso a sus cuentas o datos de tarjetas, entre otros.

Otro de los aspectos que se desprenden de estos resultados es que, las personas encuestadas, están muy preocupadas por la publicación de sus datos personales en Internet. Un 60% de los encuestados han resaltado que evitan publicar información personal en Internet. Es importante que las personas estén atentas a publicar este tipo de información, para que no pueda realizarse un mal uso de sus datos personales.



CONCLUSIONES

El 26,5% de los encuestados considera estar bien o muy bien informado acerca de los riesgos del cibercrimen. El 73,5% reconoce estar informado de manera deficiente, ya sea porque asume estar algo informado (38%), poco informado (26,8%) o nada informado (8,7%).

Las fuentes a las que se les asigna mayor confianza para informarse sobre seguridad en internet son familiares y/o amigos y expertos en informática. Las fuentes a las que se les asigna menor confianza son las redes sociales y los funcionarios policiales y judiciales.

Entre las fuentes a las que se le asigna menor confianza aparecen las redes sociales. Sin embargo, en base a los resultados de las fuentes de información que utilizan las personas encuestadas, Facebook, aparece como la segunda fuente a la que hacen referencia las personas a la hora de informarse. Si bien, a partir de esta red social, se accede a un diario digital, por ejemplo, es importante que se destaque que las redes sociales no deben ser utilizadas para informarse, ya que en ellas, aparecen gran cantidad de fuentes de información, ya sean confiables o no, y además suelen difundirse gran cantidad de "Fake News" o noticias falsas. Es necesario orientar a las personas sobre los sitios a los cuales se deben informar mediante fuentes confiables.

Considerando las estrategias que pueden dar origen a un fraude a través de internet los encuestados fueron consultados sobre si experimentaron algunas de las siguientes situaciones de manera reciente. En ese sentido se observa que: El 32,6% recibió correos o mensajes diciéndole que habían bloqueado su cuenta y que debía hacer clic en un link para volver a activarla. El 34,4% recibió llamados telefónicos solicitándole datos personales. El 73,8% recibió mensajes diciéndole que había ganado un premio o sobre el lanzamiento de una oferta o beneficio.

Al segmentar los datos por variable sociodemográficas no se perciben diferencias significativas en cuanto a sexo. En relación a la edad y al nivel de estudios se observa que reconocen con más frecuencia : Haber recibido correos o mensajes diciéndole que habían bloqueado su cuenta y que debía hacer clic en un link para volver a activarla las personas de entre 21 y 50 años y los individuos con estudios terciarios/universitarios. Haber recibido llamados telefónicos solicitándole datos personales las personas de entre 66 y 80 años Haber recibido mensajes diciéndole que había ganado un premio o sobre el lanzamiento de una oferta o beneficio las personas de entre 36 y 50 años y los individuos con estudios terciarios/universitarios.



CONCLUSIONES

Las modalidades de ciberdelito que más preocupan a los encuestados consisten en: Ser víctima de un fraude a través de tarjetas de crédito/débito. Ser víctima de un fraude a través del servicio de homebanking. Sufrir un robo de identidad mediante el uso de datos personales.

El 63% (6 de cada 10 personas) de los encuestados sí vivió o supo que algún allegado sufrió en el último año algunas de las modalidades de ciberdelito consideradas. Las tres de ellas mencionadas de manera más frecuentes son: Fraude a través de tarjeta crédito/débito. Hackeo de cuentas en redes sociales, mail, etc No haber recibido bienes o servicios en las condiciones adquiridas. Por otro lado, 37% de los encuestados asegura no haber vivido ni sabido de que algún allegado haya sufrido alguna de estas situaciones

Entre quienes señalaron haber sufrido fraude a través de tarjeta crédito/débito el 29,3% recordó que antes de haberse dado cuenta de esa situación recibió una llamada telefónica solicitándole datos personales para obligarlo a concurrir a un cajero automático y brindar un número o código de seguridad.

Entre quienes reconocen haber sido víctimas de fraude a través de Homebanking o Fintech, el 25,02% recordó que antes de haber detectado la situación inició alguna operación a través de una comunicación con la cuenta o el perfil de una empresa o institución en una red social.

El 61,03% de los encuestados que reconocen haber sido víctimas de fraude por no recibir bienes o servicios comprados/alquilados, que sean falsificados o diferentes a lo publicitado señaló haber realizado la operación a través de redes sociales, un market place o similar.

El 57,07% de los encuestados que reconocen haber sufrido fraude al vender un bien o servicio indicaron haber realizado estas operaciones mediante redes sociales, un market place o similar

El 25,43% de los encuestados que reconocen haber sufrido un fraude por no recibir bienes o servicios comprados/alquilados, señaló haber sido víctima de esta situación al alquilar un inmueble.

El 44,44% de los encuestados que reconocen haber sufrido fraude al vender un bien o servicio indicaron haber sufrido esta situación al recibir un comprobante de pago falso o que fue rechazado.



CONCLUSIONES

Tras haber detectado situaciones anómalas que potencialmente podrían ser el origen de un ciberdelito, la reacción mencionada con mayor frecuencia por los encuestados consistió en haberse contactado con el sitio web o proveedor con el cual se había interactuado.

Tras haber constatado ser víctimas de un hecho de fraude con tarjeta de débito/crédito, la reacción más frecuente de los encuestados consistió en haberse contactado con el banco.

Tras haber constatado ser víctimas de un hecho de fraude a través de homebanking o fintech, la reacción más frecuente de los encuestados consistió en haberse contactado con el banco y/o con un mail de contacto.

Sólo el 27,9% (aprox. 3 de cada 10 personas) conocen algún organismo para denunciar ciberdelitos. De ese porcentaje, las redes sociales como Instagram o Facebook han sido las más frecuentes a la hora de denunciar un ciberdelito. Sin embargo, estos no son los canales adecuados. Las redes sociales, podrán tomar medidas sobre cuentas denunciadas, pero son pocas las ocasiones en las que reportarán a la justicia para que se investigue y menos en nuestro país. Los canales adecuados para denunciar un ciberdelito son siempre los organismos del estado. El sitio de argentina.gob.ar provee mecanismos para denunciar este tipo de situaciones y aparece por debajo de las redes sociales con un porcentaje bastante bajo. En la ciudad de Mar del Plata, los delitos pueden ser denunciados por correo electrónico directamente ante la Fiscalía General de esta ciudad a la casilla denunciasmardelplata@mpba.gov.ar. Este es el canal más adecuado cuando las personas del partido de Gral. Pueyrredón sufren algún tipo de delito, cualquiera sea, incluidos los ciberdelitos





Observatorio Universitario de la Ciudad

 www.ufasta.edu.ar/observatorio

 observatorio@ufasta.edu.ar

 [observatorioUFASTA](https://www.facebook.com/observatorioUFASTA)

 [@observatoriofas](https://twitter.com/observatoriofas)