

ESTUDIO SOBRE CIBERSEGURIDAD EN EMPRESAS, USUARIOS DE INTERNET Y PADRES DE FAMILIA EN MÉXICO 2021



Antecedentes

La ciberseguridad es una disciplina que abarca la protección de aquellos elementos que dependen de las tecnologías de la información y las comunicaciones (TIC).

En el mundo actual la mayoría de las actividades que realizamos, desde el entorno personal hasta el profesional, dependen de las TIC, por lo tanto, la ciberseguridad no solo se dedica a proteger la información o los equipos de cómputo y sistemas de información, sino a proteger todas las actividades que dependen de ellas, incluyendo la seguridad nacional así como la integridad de las personas que habitan un país.

De esta manera el estado de la ciberseguridad abarca las capacidades de respuesta, preparación, monitoreo e incidencia de eventos que vulneren o busquen vulnerar la confidencialidad integridad y disponibilidades los sistemas que soportan nuestras actividades diarias.

Para ayudar a identificar las brechas en materia de ciberseguridad y brindar información que permita al Estado Mexicano, organizaciones y personas, estar preparados para actuar ante las amenazas y riesgos que presenta el ciberespacio; se realizó la siguiente investigación, la cual está basada en una encuesta aplicada a distintos perfiles de usuarios de internet.

De este análisis se obtienen datos los cuales servirán para identificar las amenazas más comunes, la incidencia sobre eventos de ciberseguridad, los impactos generados en las organizaciones, los costos asociados a un incidente, la herramientas y controles utilizados, los montos de inversión, así como la percepción general de organizaciones, empresas y usuarios sobre el estado de la ciberseguridad a nivel estatal, de los distintos sectores productivos y a nivel nacional.

Probabilístico, dividido en etapas, estratificado y por conglomerados, por bolas de nieve distribuidas con perfiles líderes representativos de cada perfil de la parte interesada.

El método de captación fue por cuestionarios a través de una página web que se distribuyeron por distintos medios en foros abiertos, redes sociales y grupos afines a los perfiles establecidos.

Tamaño de la muestra

- 410 Usuarios de internet en México*
- 207 Madres y padres de niñas, niños y adolescentes usuarios de internet en México**

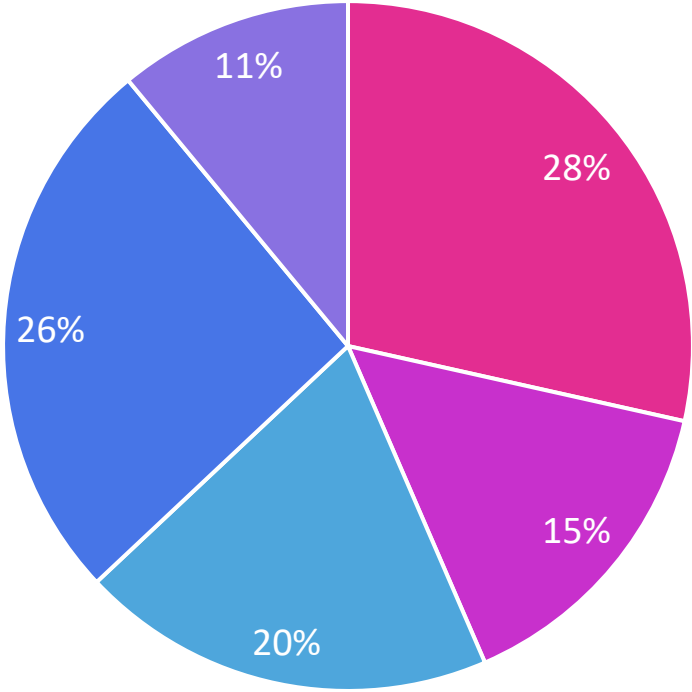
Los respondientes fueron:

* Usuarios de internet en general (margen de error 5%)

** Padres y madres de niñas, niños y adolescentes que son usuarios de internet (margen de error 6.8%)

CIBERSEGURIDAD EN: PADRES Y MADRES DE NIÑAS, NIÑOS Y ADOLESCENTES USUARIOS DE INTERNET

Rango de Edad de las Niñas, Niños y Adolescentes

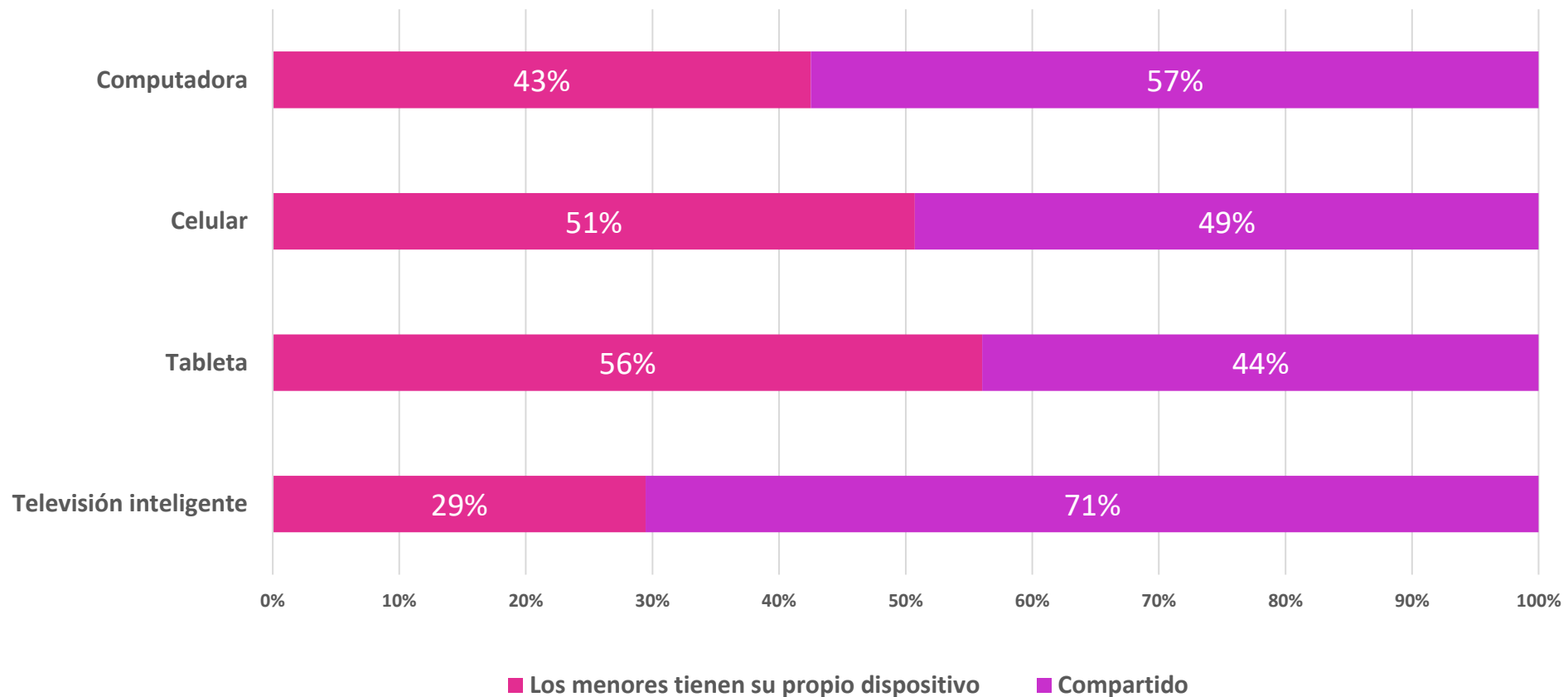


■ 6 a 9 años ■ 3 a 5 años ■ 12 a 15 años ■ 10 a 12 años ■ 16 a 18 años



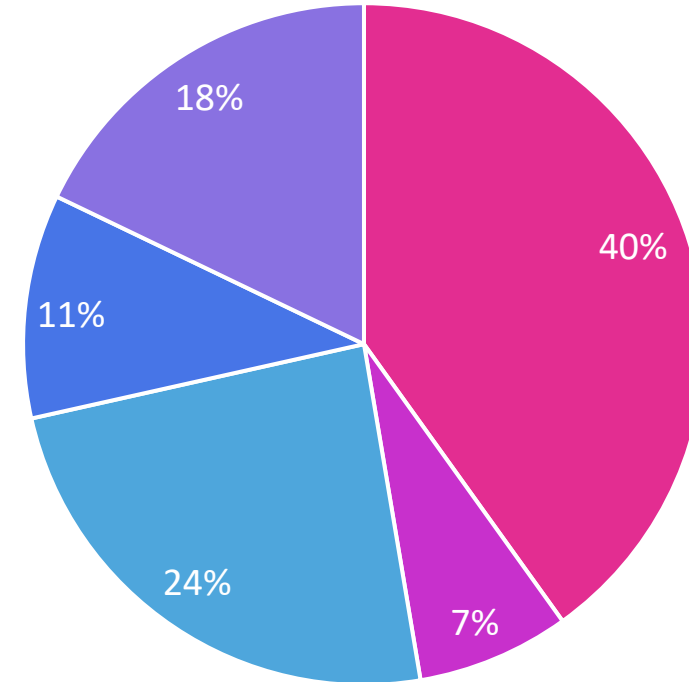
Dispositivos Propios o Compartidos

- Más del 50% de las niñas, niños y adolescentes tiene un dispositivo propio, ya sea un teléfono inteligente o una tableta.
- En más del 50% de los casos cuentan con más de 2 dispositivos



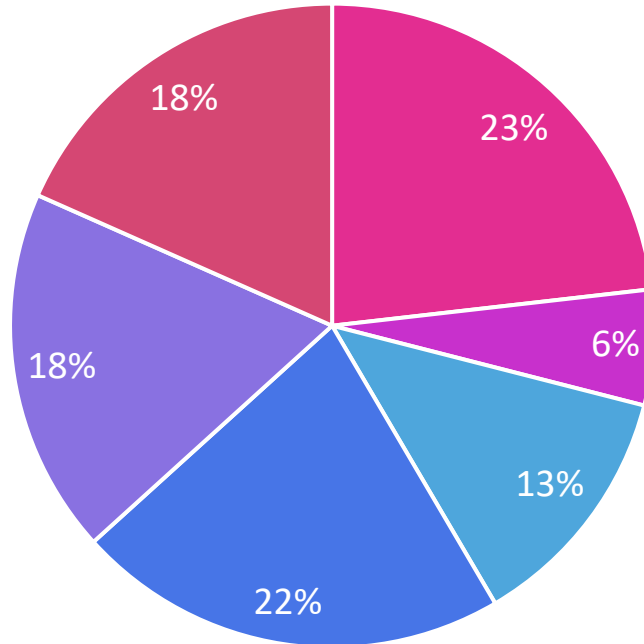
Sistemas de Control Parental

- El 47% de los padres no usa o no sabe qué es un sistema de control parental
- 14.9% de ellos por desconocimiento de la herramienta



- No
- No sé qué es un programa de control parental
- Sí, con una aplicación instalada en cada dispositivo
- Sí, con un equipo que bloquea contenido en la red
- Sí, con un sistema que permite monitorear cada dispositivo y establecer reglas

Horarios para el Uso de Internet (sin considerar horas de estudio)



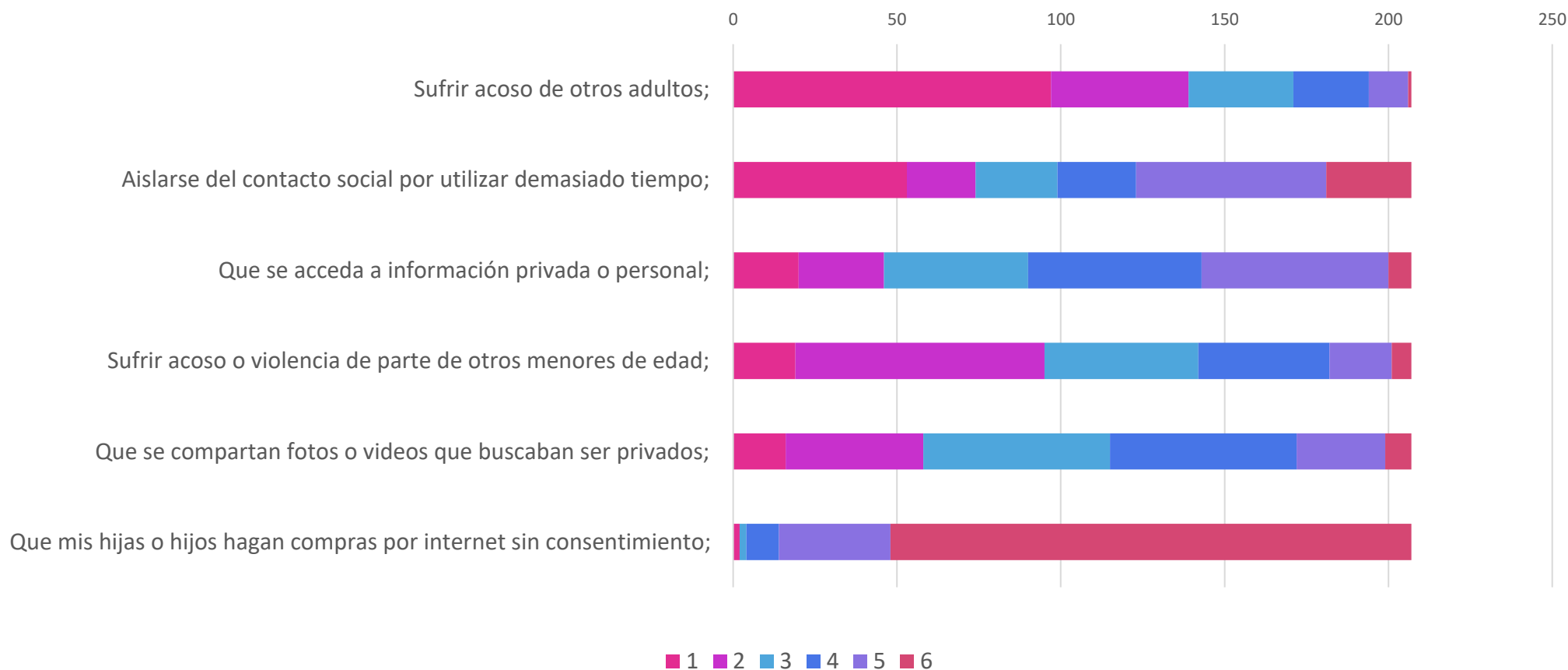
■ No, pueden utilizarlo el tiempo que quieran
■ Entre media hora y una hora al día
■ Entre dos y tres horas al día

■ Menos de media hora al día
■ Entre una hora y dos horas al día
■ Más de tres horas al día

- El 23% de los padres no establecen límites para el uso de los dispositivos con respecto del tiempo que pueden utilizarlo los menores
- Solamente 18% de los padres de las niñas, niños y adolescentes les permiten estar mas de 3 horas al día en el internet

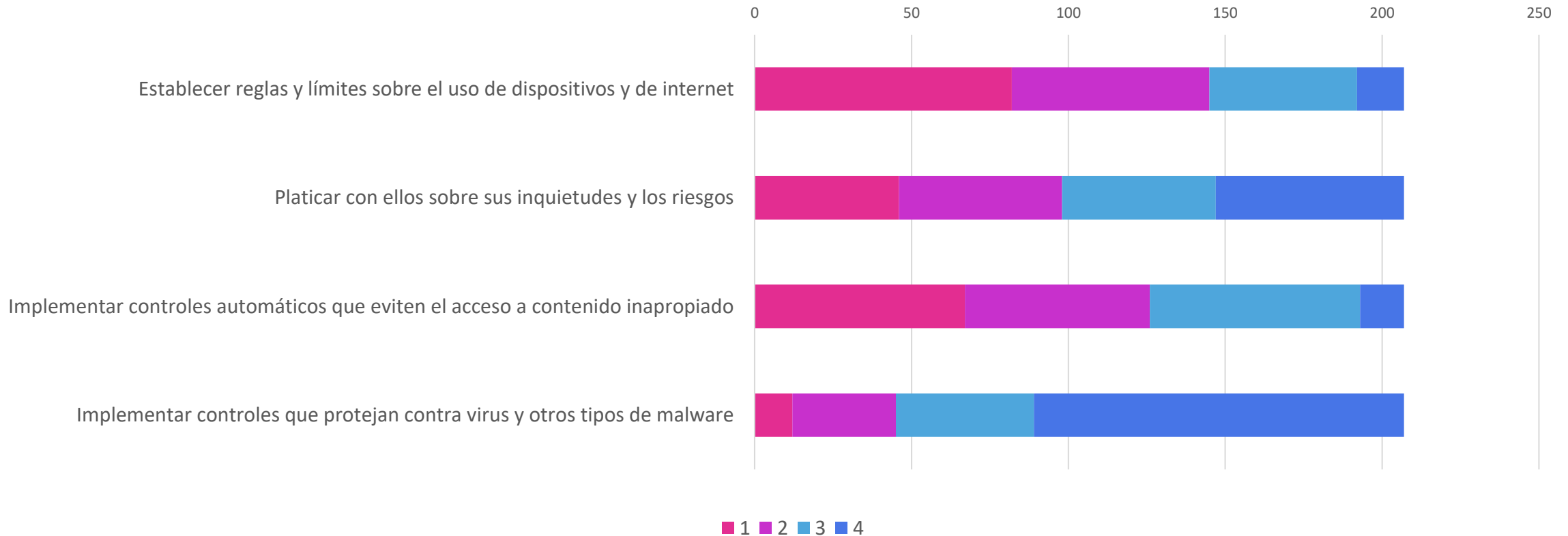
Principales Preocupaciones sobre la Seguridad en el Uso de Internet

- La mayor preocupación para los padres sobre los riesgos en internet para niñas, niños y adolescentes es sufrir el acoso de parte de otros adultos



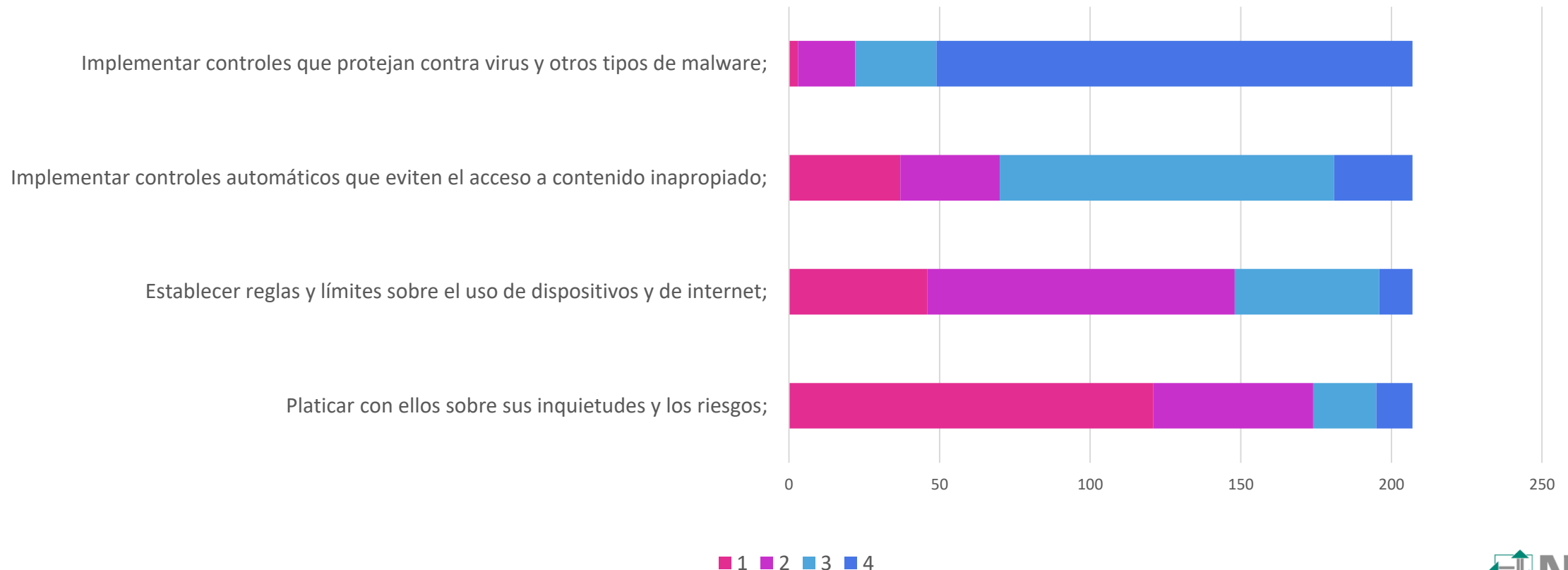
Principales Retos de Comunicación de los Padres con sus Hijos en el Uso de Internet

- La mayor problemática que enfrentan los padres de familia es el establecimiento de reglas y límites para el uso de dispositivos e internet

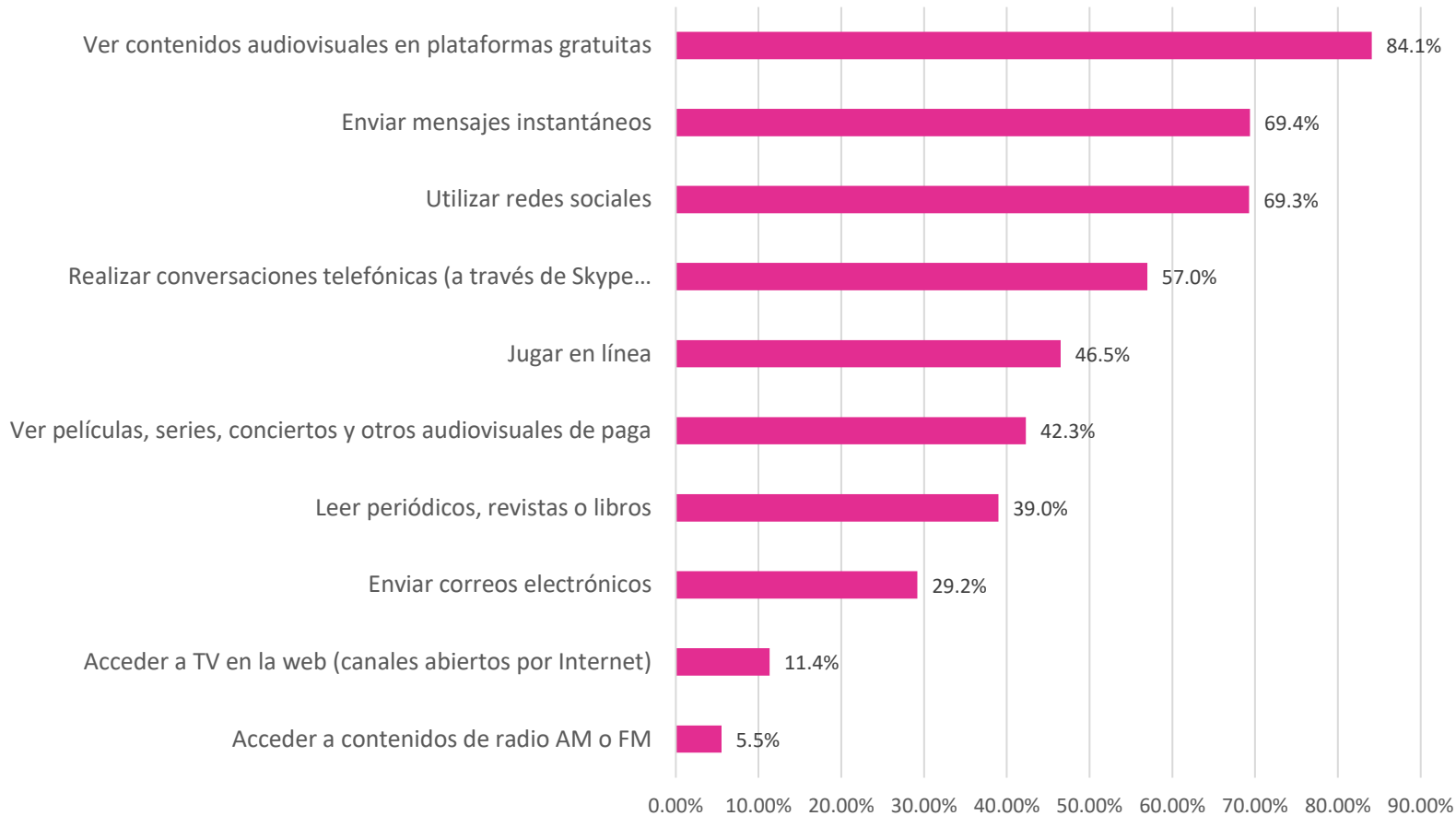


Principales Acciones para Proteger a los Niños y Adolescentes en el uso de Internet

- La acción considerada como de mayor relevancia para proteger a las niñas, niño y adolescentes fue el platicar con ellos sobre las inquietudes y los riesgos del uso de internet



Principales Usos de Internet



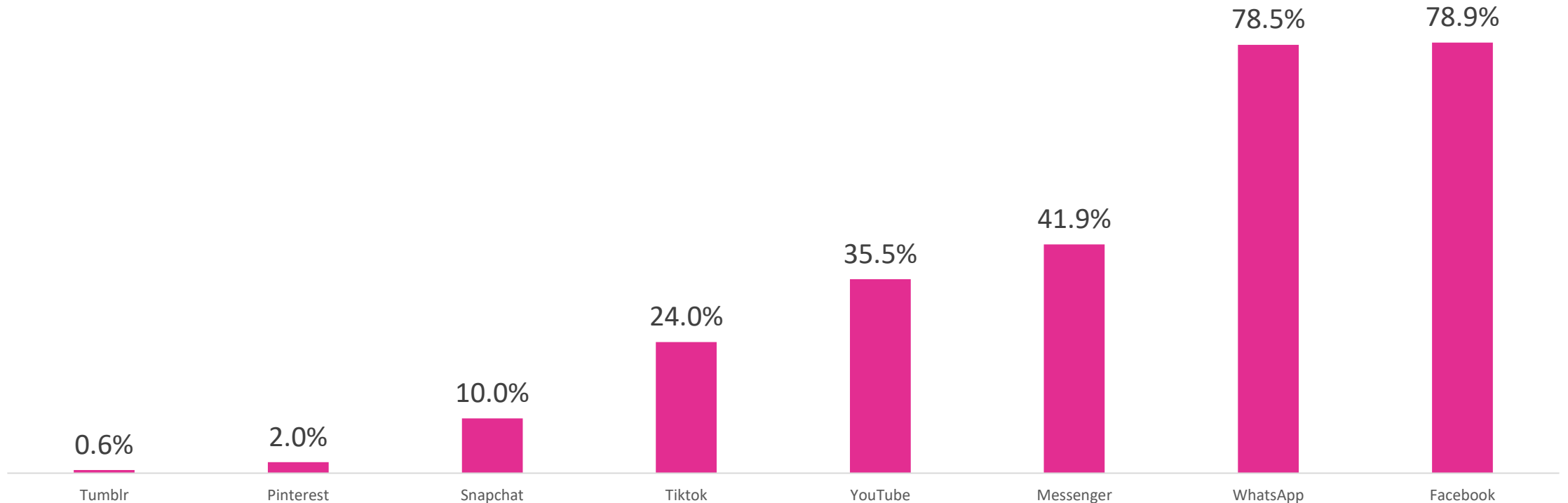
- La principal actividad de los jóvenes a través de internet es ver contenidos audiovisuales, aun por encima del uso redes sociales y mensajería instantánea

Nota: Cifras mostradas en porcentaje.

Las categorías no son excluyentes, por lo que la suma de las proporciones es superior al 100 por ciento.

Redes Sociales Utilizadas

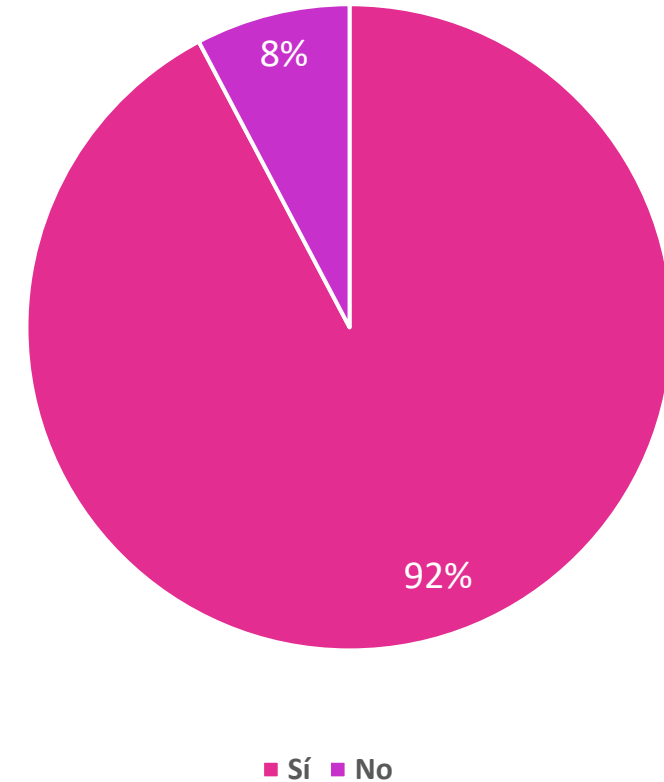
- Facebook y WhatsApp son las principales redes sociales usadas por los niños, niñas y adolescentes, muy por arriba del resto de las plataformas



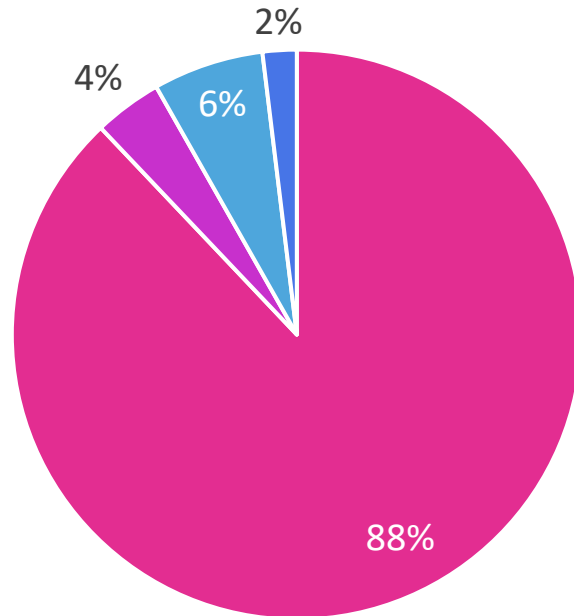
Nota: Cifras mostradas en porcentaje.
Las categorías no son excluyentes, por lo que la suma de las proporciones es superior al 100 por ciento.

Pláticas Sobre los Peligros en el Uso de Internet

- El 92% de los padres y madres platica con sus hijos sobre el uso adecuado de internet
- Entre mayor es la edad de las niñas, niños y adolescentes, menor es la incidencia de este acercamiento



Pláticas Sobre las Actividades que Realizan en Internet

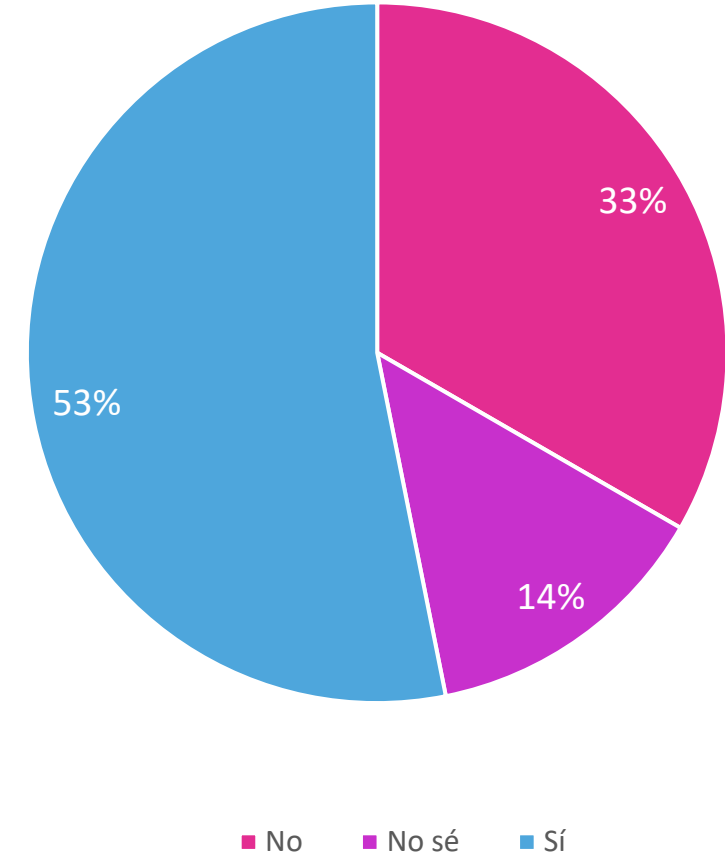


- Sí, les hago preguntas y provoco la conversación alrededor del tema
- Solo si ellos desean platicarlo
- Lo intento, pero ellos evaden responder
- No, nunca hablamos sobre lo que hacen en internet

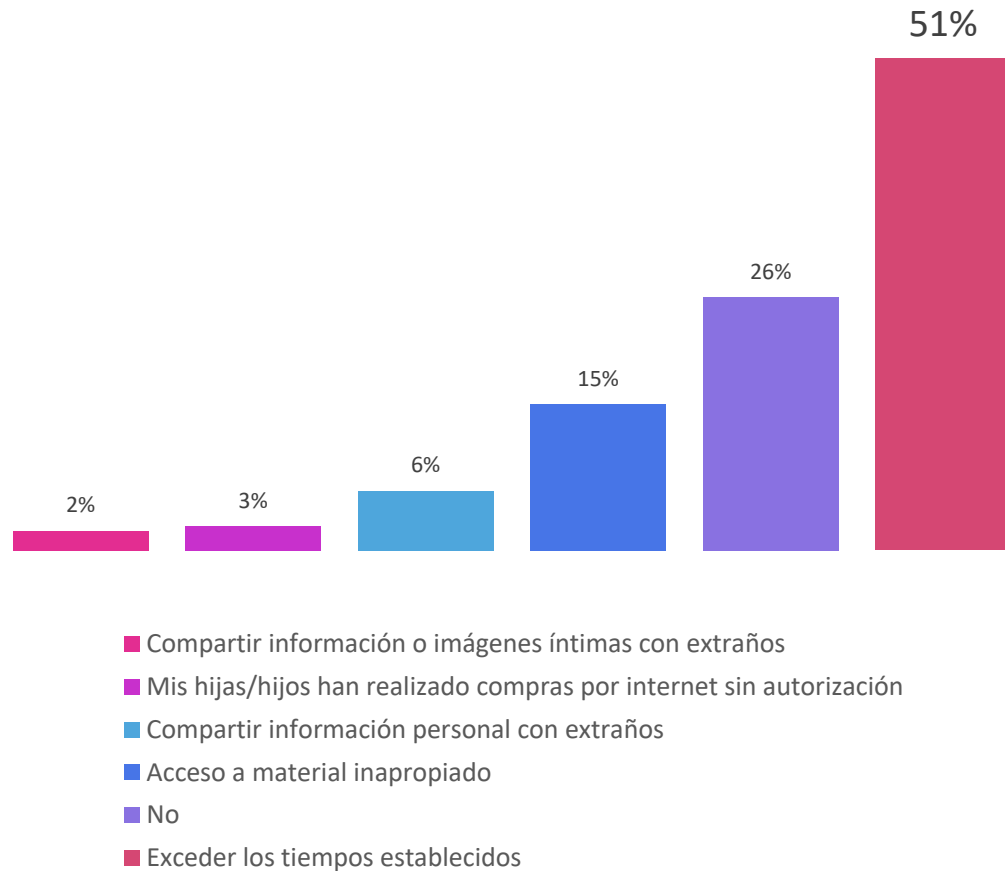
- Un alto porcentaje (88%) de los padres de familia están al tanto sobre las actividades de sus hijos e hijas en internet
- Solamente 8% de los padres no hablan o conocen las actividades de sus hijas e hijos en internet

Capacitación y Orientación sobre los Peligros en el Uso de Internet en la Escuela

- El 33% de las niñas, niños y adolescentes no recibe orientación en la escuela sobre los peligros que puede haber en internet.
- Según el estudio sobre ciberacoso del INEGI (MOCIBA 2019) el 23% de las niñas y niños de más de 12 años han sufrido algún tipo de ciberacoso

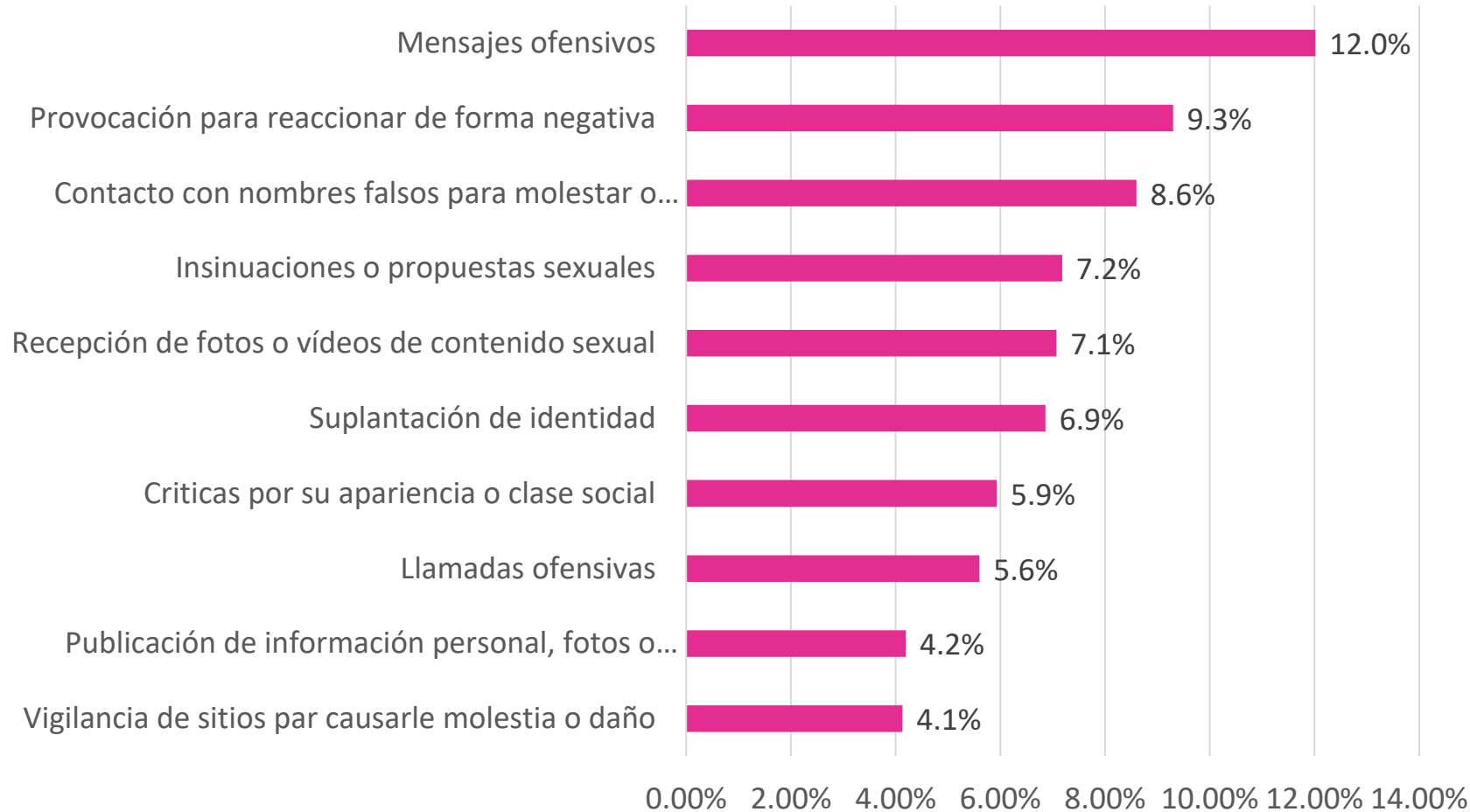


Experiencias Negativas en los Hábitos de Uso de Internet de los Hijos



- **El 15% de los padres manifestaron que sus hijos han tenido acceso a material inapropiado, el 2% compartió imágenes íntimas con extraños**
- **De los encuestados, el 26% no sabe cuál es la autoridad competente para reportar problemas de ciberseguridad**
- **Solo el 4 % de las personas encuestadas que tuvieron experiencias negativas con sus hijas o hijos, lo reportaron a las autoridades**
- **El 75% de las personas que reportaron tuvieron una experiencia adecuada y el 25% una experiencia pobre es esta interacción con la autoridad**

Penetración de las situaciones de ciberacoso experimentadas por adolescentes

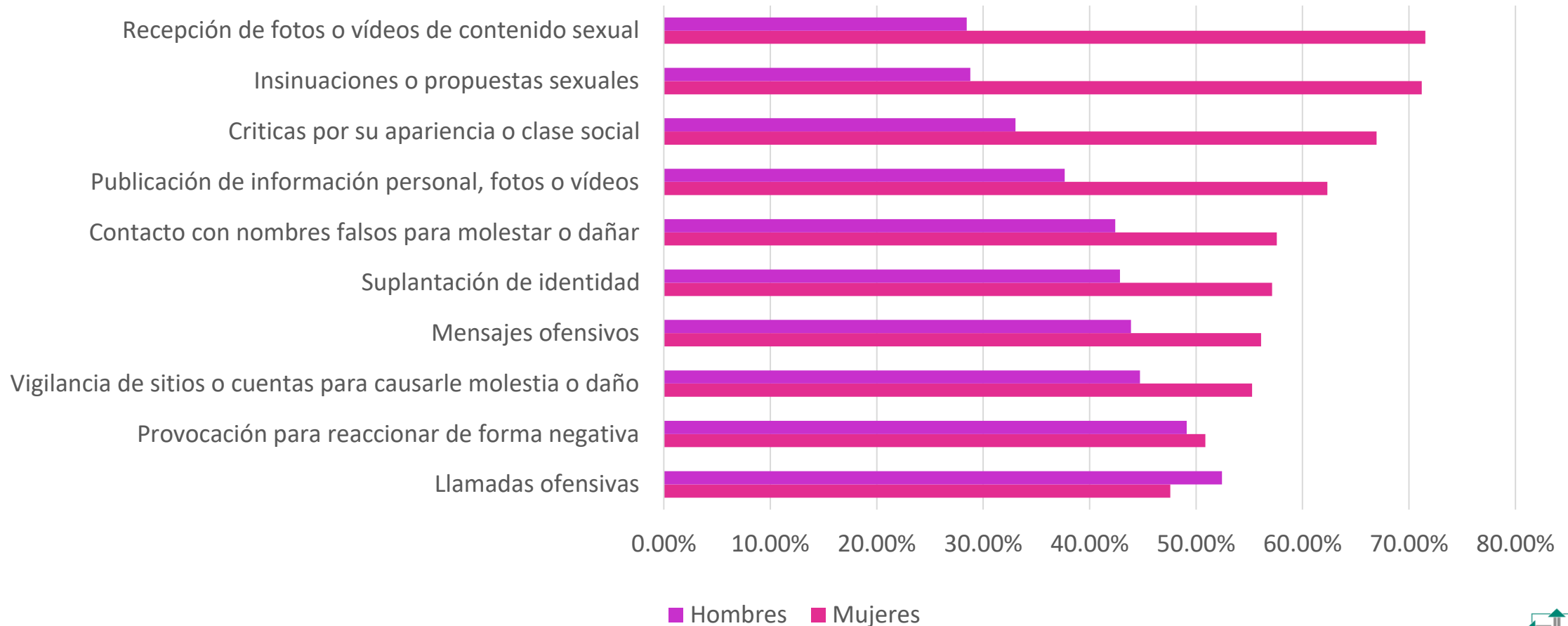


12% de los jóvenes percibe haber recibido mensajes ofensivos al usar internet

Datos de MOCIBA 2019

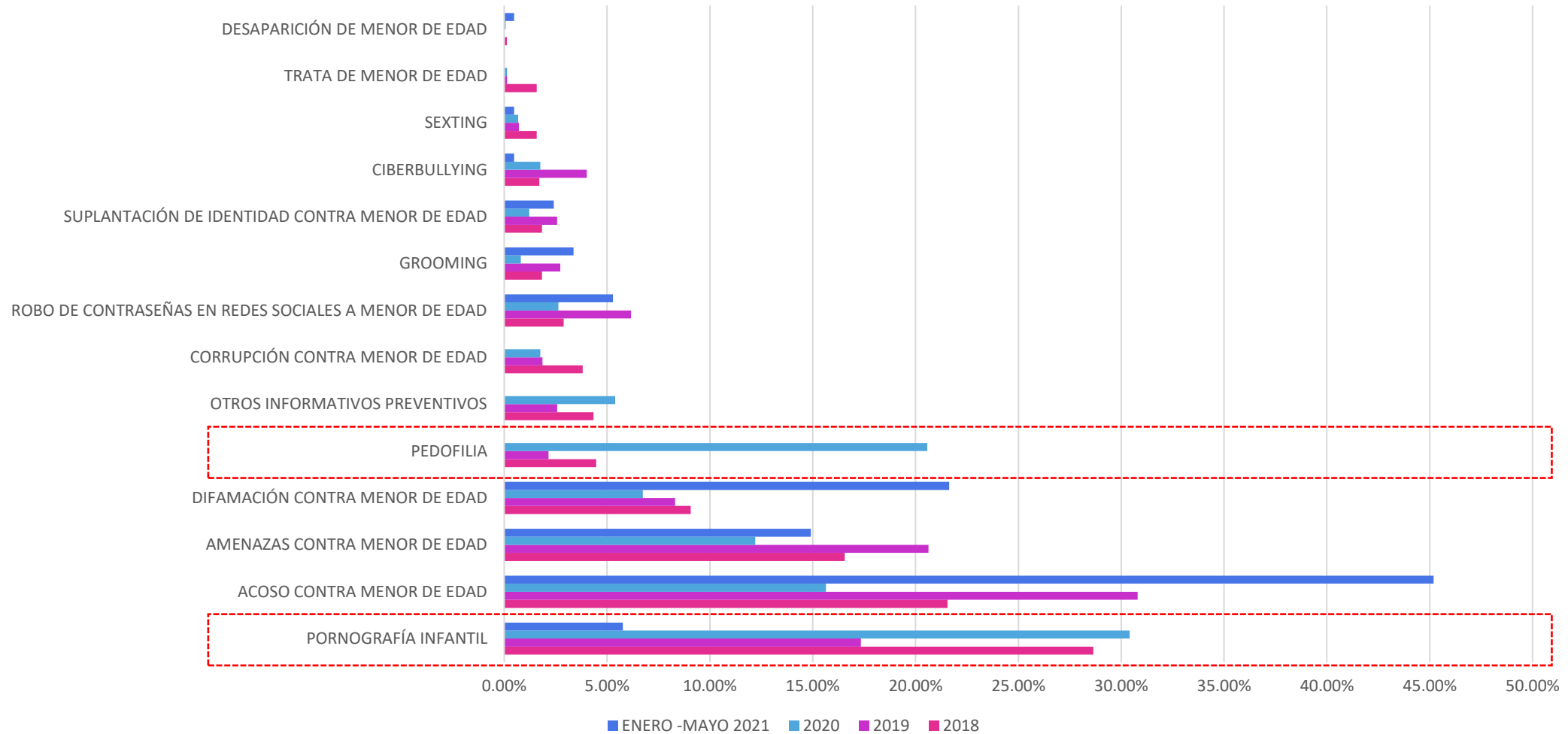
Distribución de Ciberacoso Experimentadas por Adolescentes

- A pesar de haber una equidad de género en el uso de internet, existen diferencias significativas en situaciones de ciberacoso



Denuncias por Ataques, Delitos Cibernéticos en Contra de Niñas, Niños y Adolescentes

- Durante el 2020, se dispararon drásticamente el número de denuncias por pedofilia y pornografía infantil



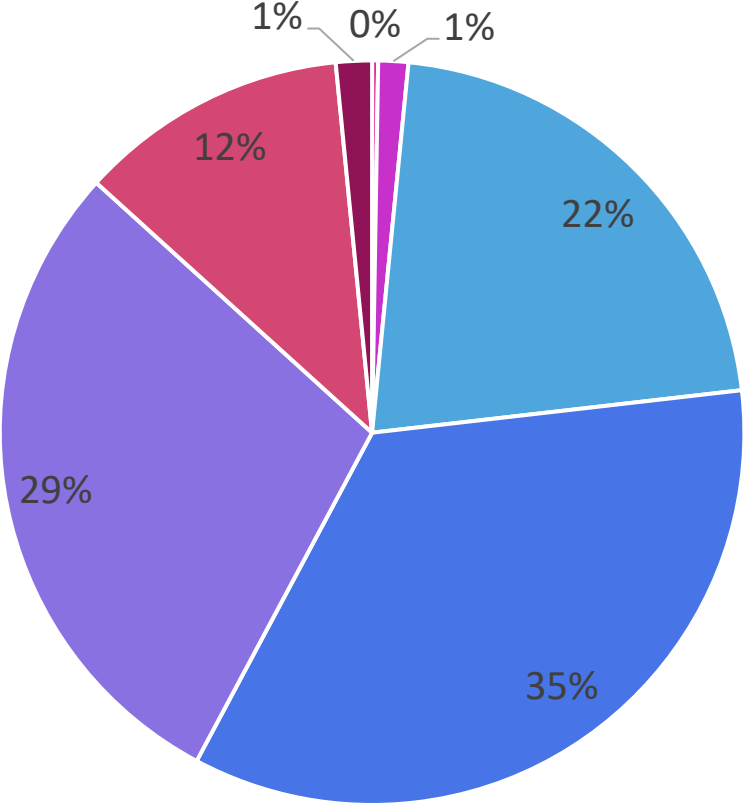
- De acuerdo con el Estudio de hábitos de los usuarios de Internet de la AIMX 2021, el **10% de los usuarios de internet son niños entre 6 y 11 años**, mientras que el **13.9% tienen entre 12 y 17 años**
- Más del 50% de las niñas, niños y adolescentes tiene un dispositivo propio, ya sea celular o tableta. En más del 50% de los casos cuentan con más de 2 dispositivos
- El 47% de los padres no usa o no sabe qué es un sistema de control parental y su principal problema es el establecimiento de límites para el uso de los dispositivos
- La mayor preocupación sobre los riesgos en internet para niñas, niños y adolescentes es sufrir acoso por parte de otros adultos
- La acción considerada como de mayor relevancia para proteger a las niñas, niños y adolescentes fue considerada el platicar con ellos sobre las inquietudes y los riesgos del uso de internet.
- El 8% de los padres no habla con sus hijos de las actividades que realizan en internet
- Las principales aplicaciones para teléfonos inteligentes que usan las niñas, los niños y los adolescentes del país son utilizadas para: **jugar (82.24%)**, **enviar mensajes instantáneos (71.24%)**, **acceder a redes sociales (67.97%)** y **acceder a contenidos audiovisuales (61.11%)**.

- El 33% de las niñas, niños y adolescentes no recibe orientación en la escuela sobre los peligros de internet, de acuerdo con el mismo estudio de CEPAL y UNICEF la escuela es el lugar de acceso en el 46% de los casos
- El 15% de los padres manifestaron que sus hijos han tenido acceso a material inapropiado, el 2% compartió imágenes íntimas con extraños
- De los encuestados, el 26% no sabe cuál es la autoridad competente para reportar problemas de ciberseguridad
- De acuerdo con el reporte de la Guardia Nacional, **los delitos cibernéticos cometidos contra menores de edad aumentaron 157%** y el delito de **pornografía infantil aumentó en 73%**
- Solo el 4 % de las personas encuestadas que tuvieron experiencias negativas con sus hijas o hijos, lo reportaron a las autoridades
- El 75% de las personas que reportaron tuvieron una experiencia adecuada y el 25% una experiencia pobre
- Al 2020 se presentan 5.4 millones de casos de abuso sexual infantil en México y el 27% de los casos de trata de personas, las víctimas son menores de edad

CIBERSEGURIDAD EN: USUARIOS DE INTERNET



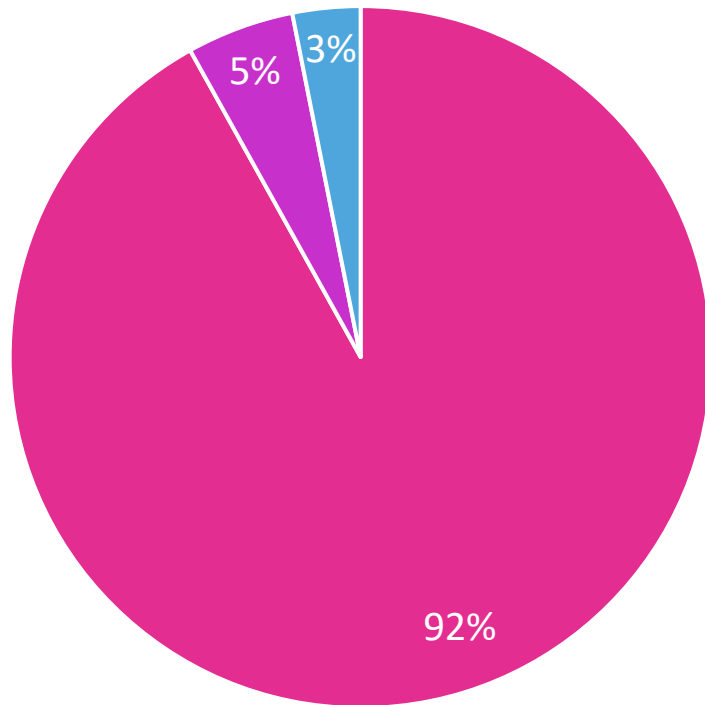
Rango de Edad de los Usuarios Encuestados



■ Menor de 16 años ■ De 16 a 20 años ■ De 20 a 30 años ■ De 30 a 40 años ■ De 40 a 50 años ■ De 50 a 65 años ■ Más de 65 años

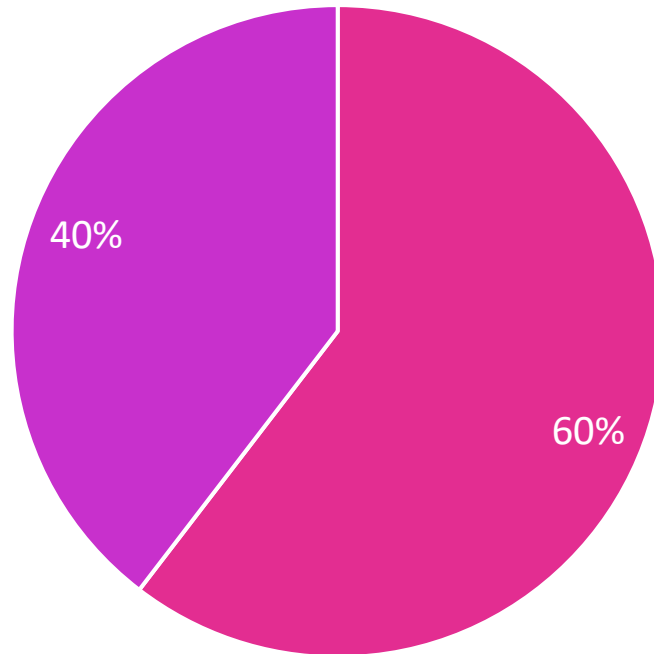


- El 92% de los usuarios considera que la ciberseguridad es una preocupación.



■ Sí ■ No ■ No sé cómo podría afectarme

- Según datos de la Guardia Nacional en 2020 se tuvieron 2,898 denuncias de delitos relacionados con ciberdelitos
 - Esto significó un crecimiento del más del doble comparado con el 2019

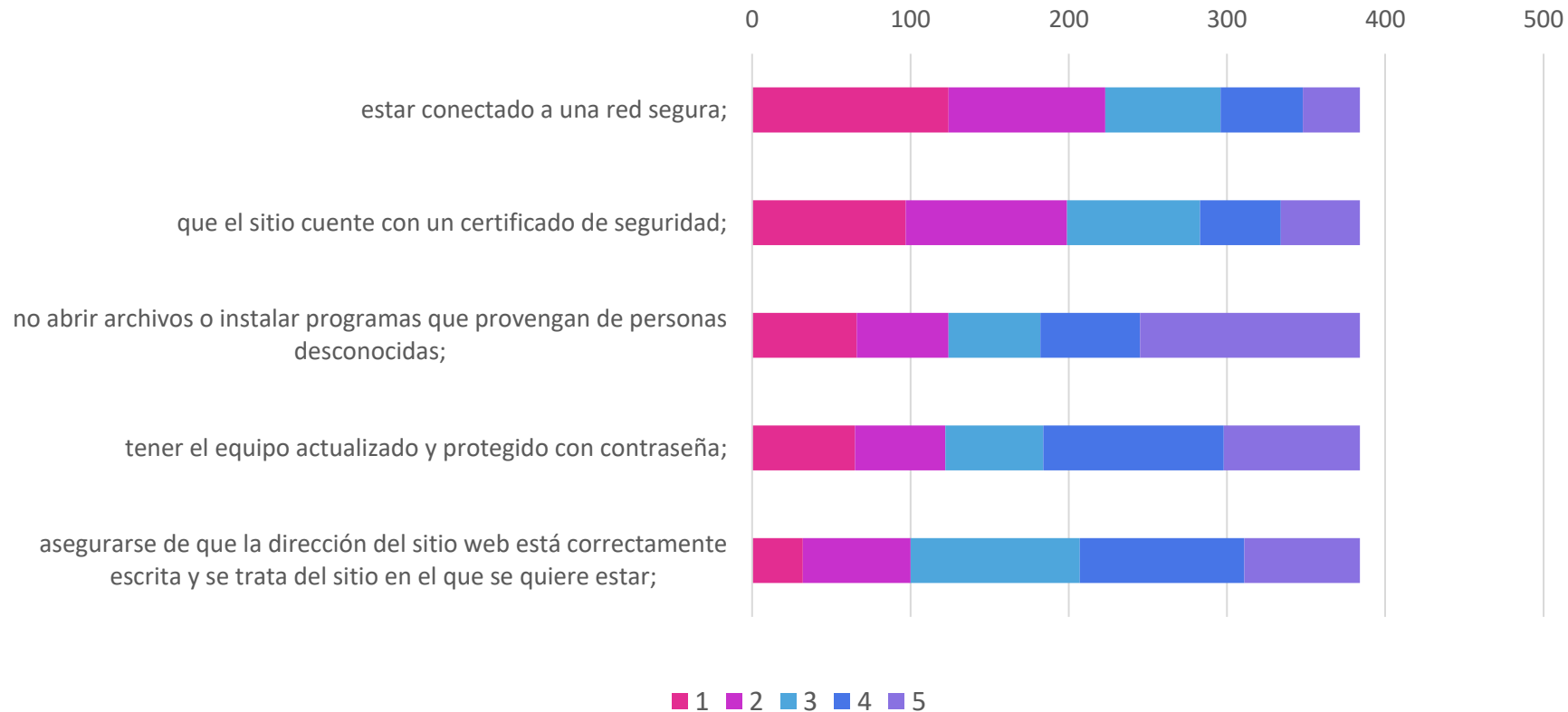


■ No ■ Sí

- **60% de los usuarios considera que su equipo no está protegido ante las amenazas que presenta el uso de internet**
- En 2020 se realizaron 47 mil millones de transacciones comparado con 35.5 mil millones de transacciones en 2019
 - Incremento de 29%

Medidas de Seguridad para Navegar de Forma Segura en Internet

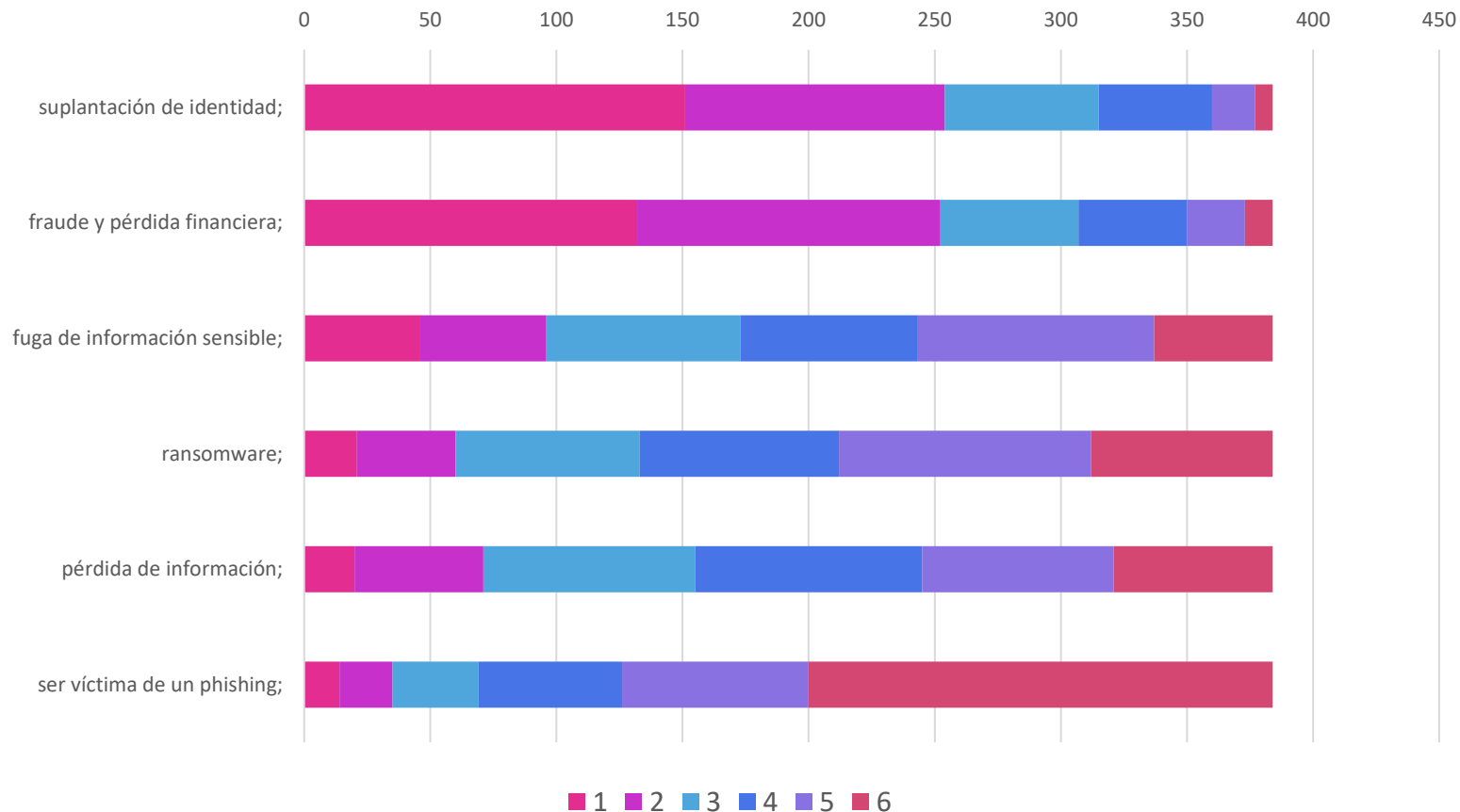
- Los usuarios consideran que la medida más importante para el uso seguro de internet es la conexión a una red segura



Estar conectado a una red segura puede no ser suficiente si no se verifica que la dirección de los sitios que se visitan sea legítima y segura

Preocupaciones Relevantes en Materia de Ciberseguridad

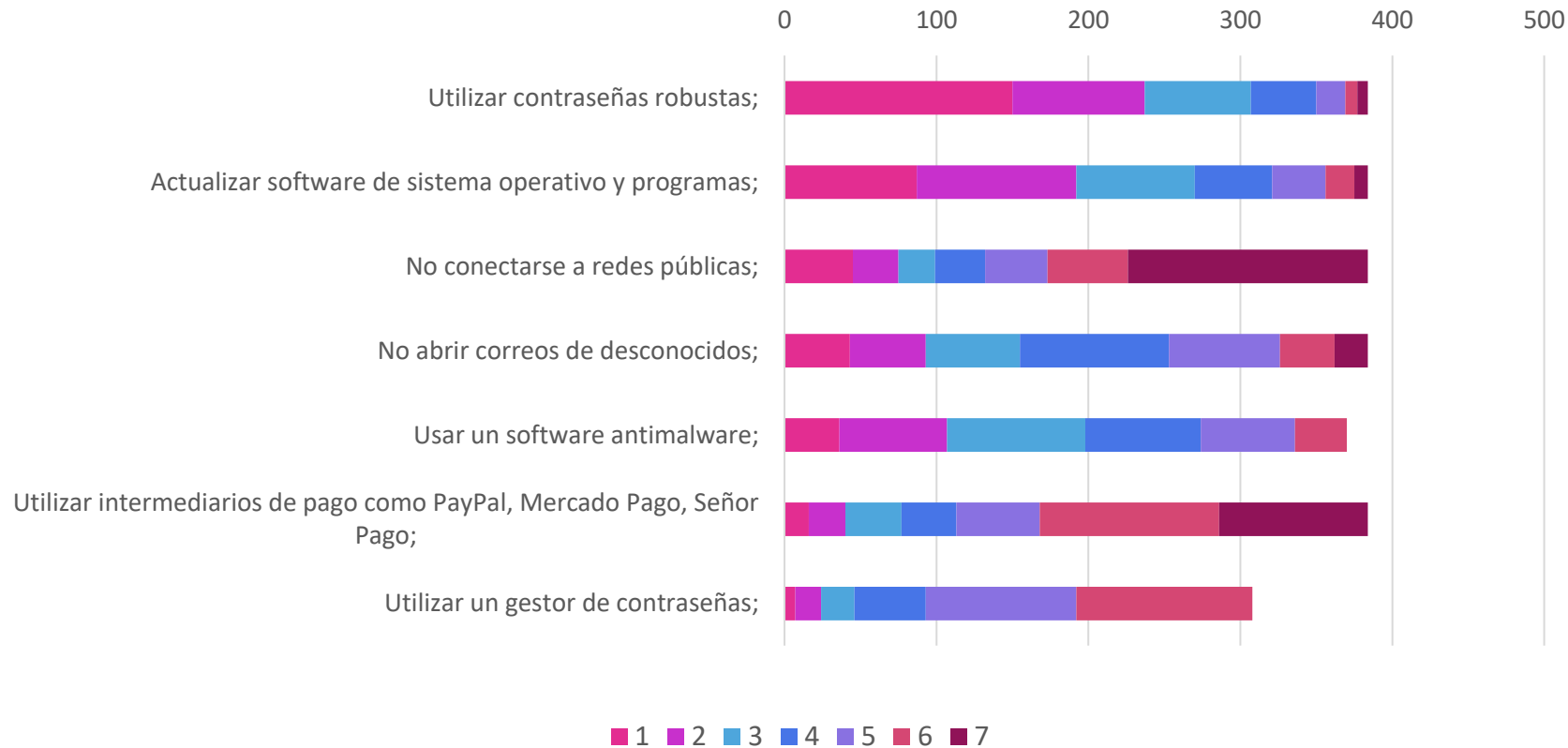
- La preocupación más grande de los usuarios de internet en la suplantación de identidad, seguida por el fraude y pérdidas financieras



- CONDUSEF** atendió un total de 16,500 reclamos, 34% menor respecto a lo atendido en 2019
- La disminución puede atribuirse en parte a la pandemia, pero disminución fue menor que en otros sectores

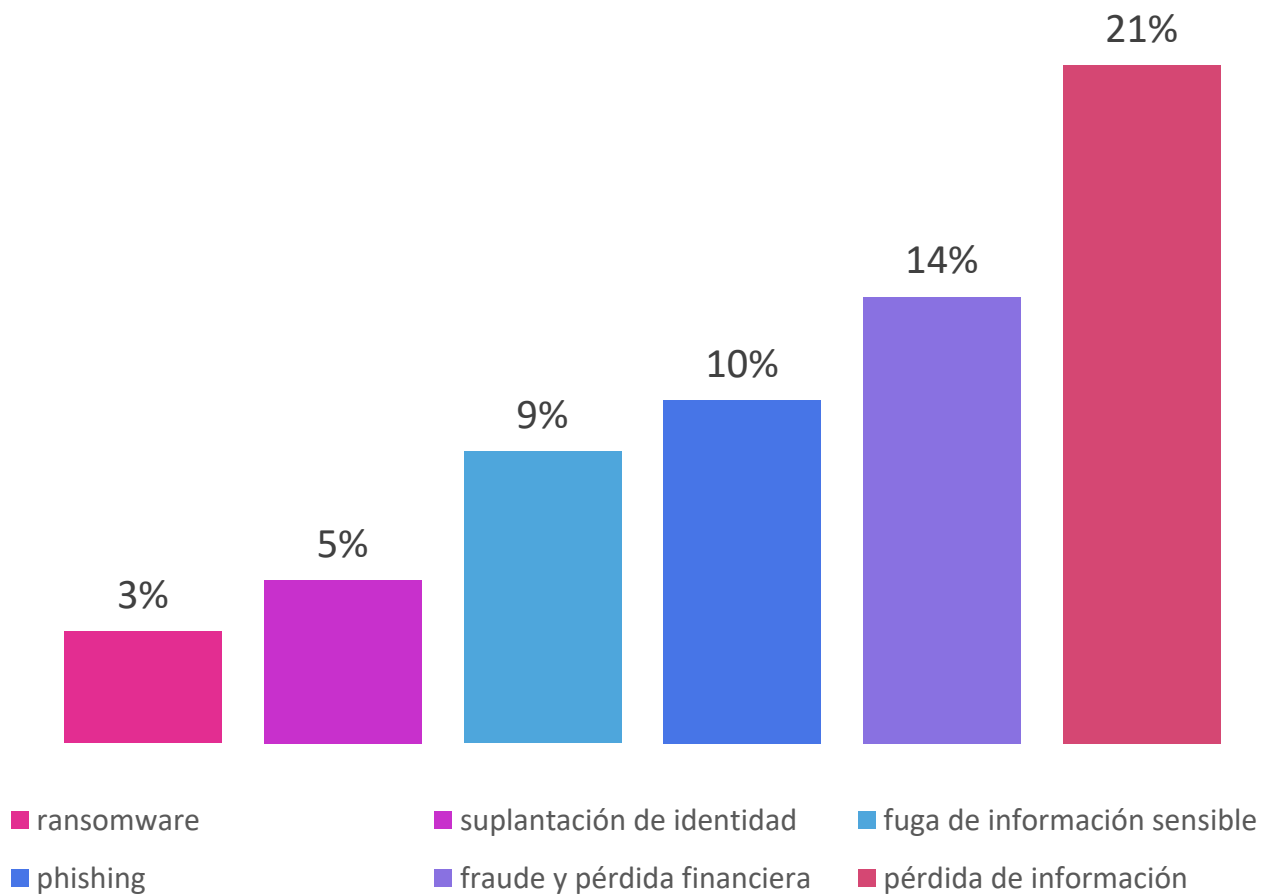
Principales Medidas de Protección de Información y Dispositivos

- Utilizar contraseñas robustas fue considerada como la medida de seguridad más importante, seguida de mantener actualizados los sistemas



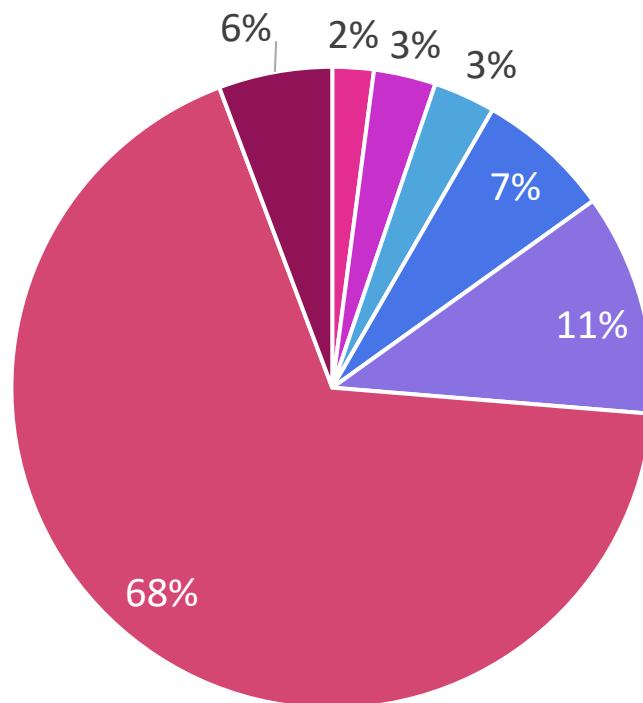
El 57% de las personas que ya han sido estafadas en ataques de phishing aún no han cambiado sus contraseñas.

Victimas de Alguna Vulneración



- El 53% de los usuarios han sido víctimas de alguna vulneración en los últimos 12 meses
- Principalmente de pérdida de información, fraudes y pérdidas financieras
 - 3% de los usuarios reportaron casos de vulneraciones por ransomware

Frecuencia de Actualización de Sistemas Operativos y Software

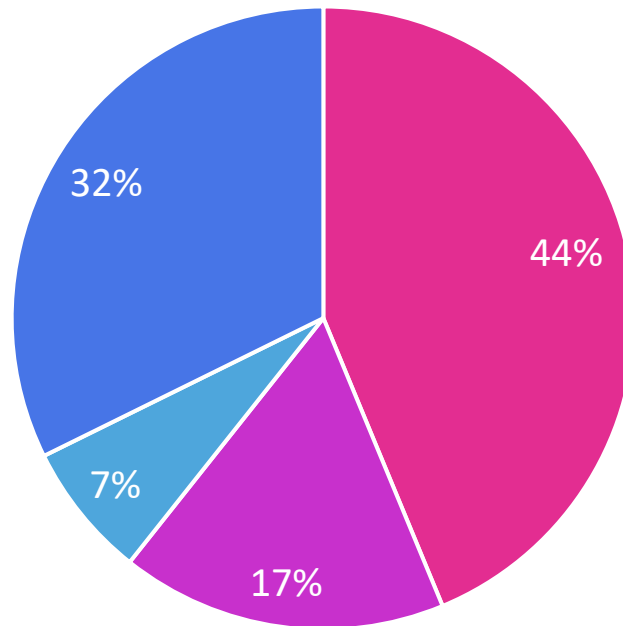


- Nunca
- Al menos dos veces a la semana
- De vez en cuando, cuando recuerdo
- No sé cómo actualizar
- Al menos una vez por semana
- Al menos una vez al mes
- Está configurado para actualizarse automáticamente

- **6% de los encuestados desconoce como actualizar su sistema operativo y software**
- Solamente 3% de los encuestados actualiza sus sistemas operativos y software una vez por semana

La mayoría de los ataques utilizan vulnerabilidades que ya han sido corregidas por los desarrolladores de los sistemas, actualizarlos disminuye la posibilidad de ser vulnerado

Propiedad del Equipo de Cómputo para Actividades Relacionadas con el Trabajo



- 32% de las personas encuestada utilizando equipo personal para actividades de la empresa para la que trabajan (BYOD), sin considerar aquellos que son autoempleados

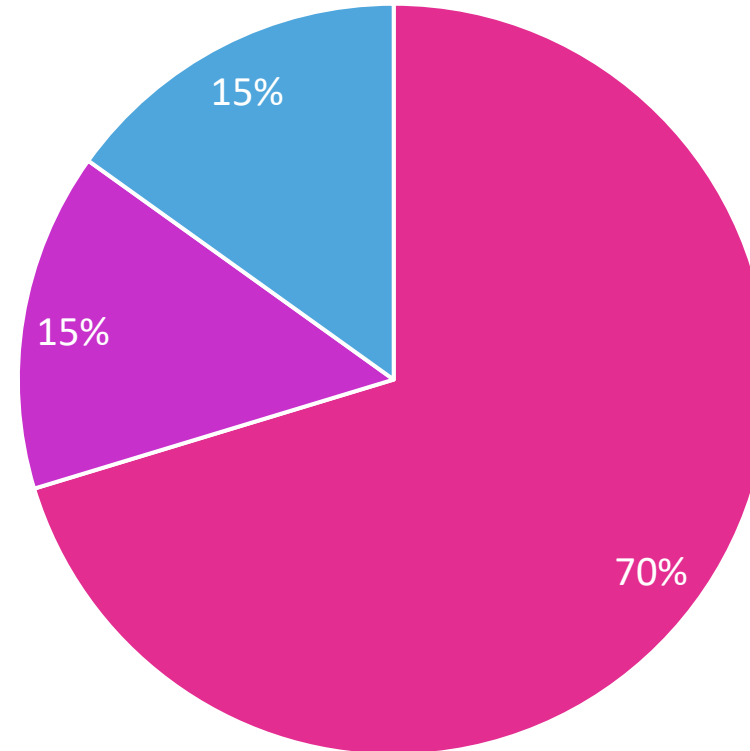
- No, trabajo en una empresa y utilizo un equipo propiedad de la empresa
- Sí, soy autoempleado o tengo mi propia empresa y utilizo el mismo equipo para fines personales, de entretenimiento y de trabajo
- No, soy autoempleado o tengo mi propia empresa y utilizo equipos para fines personales, de entretenimiento y de trabajo

Software Antimalware (antivirus) en Computadoras

- 30% de los usuarios no saben que cuentan o no cuentan con software antimalware

La mayoría de los sistemas actuales incluye de forma predeterminada algún software antimalware

- Sin embargo los atacantes modifican sus técnicas constantemente y **este tipo de sistemas debe ser complementado con otras acciones para evitar vulneraciones**



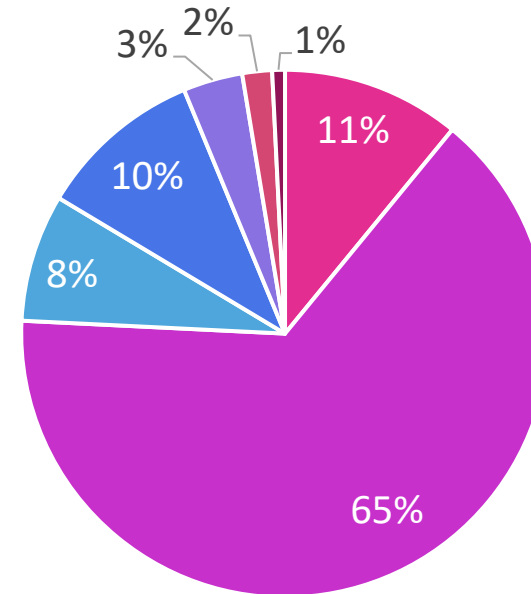
■ Sí ■ No lo sé ■ No



Frecuencia de actualización de antimalware (antivirus)

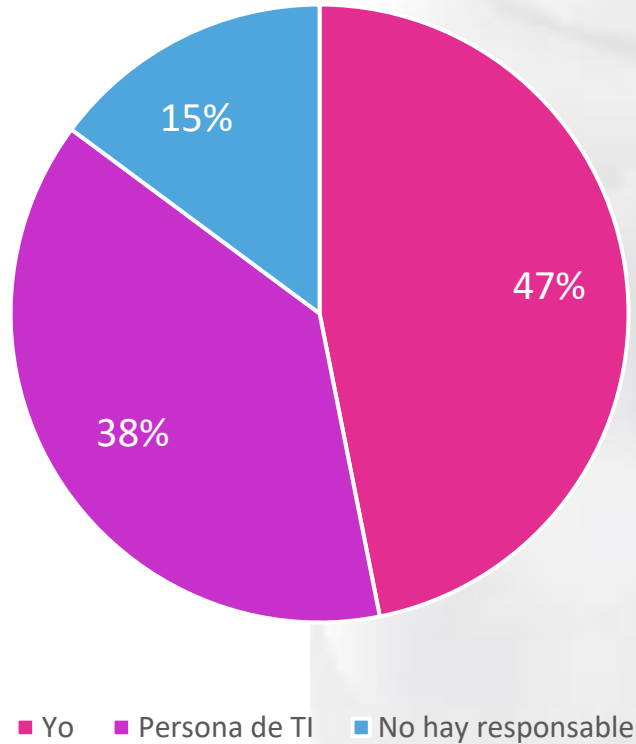
- El 10% de la gente no actualiza nunca su software antimalware

Un software de seguridad no actualizado puede ser incapaz de detener las amenazas en los sistemas



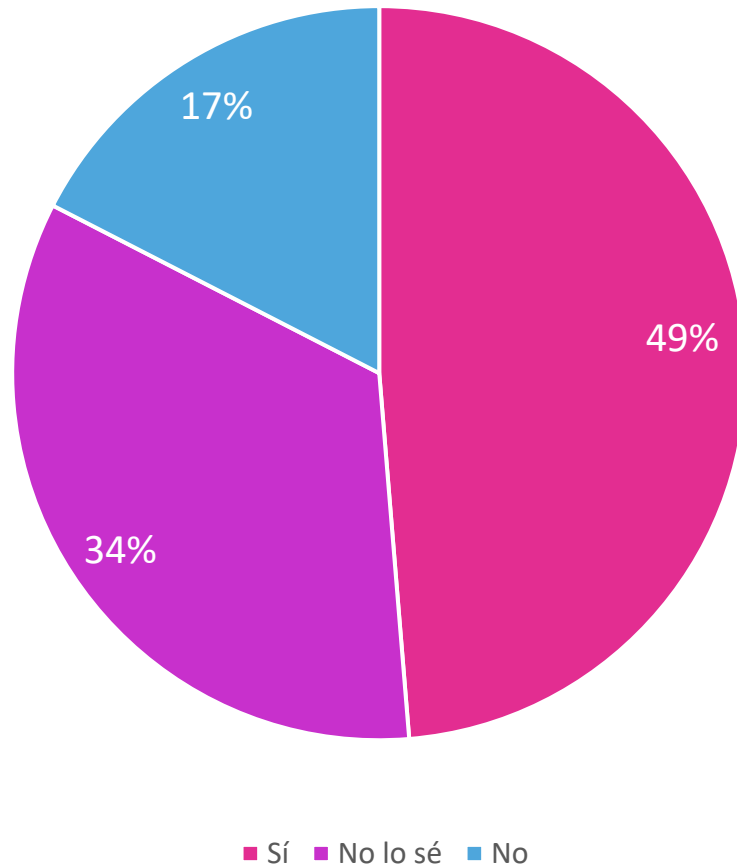
- De vez en cuando, cuando lo recuerdo
- Se hace automáticamente
- La suscripción se agotó
- Nunca
- Al menos una vez al mes
- Al menos una vez por semana
- Al menos dos veces a la semana

Responsabilidad de Seguridad en Computadoras



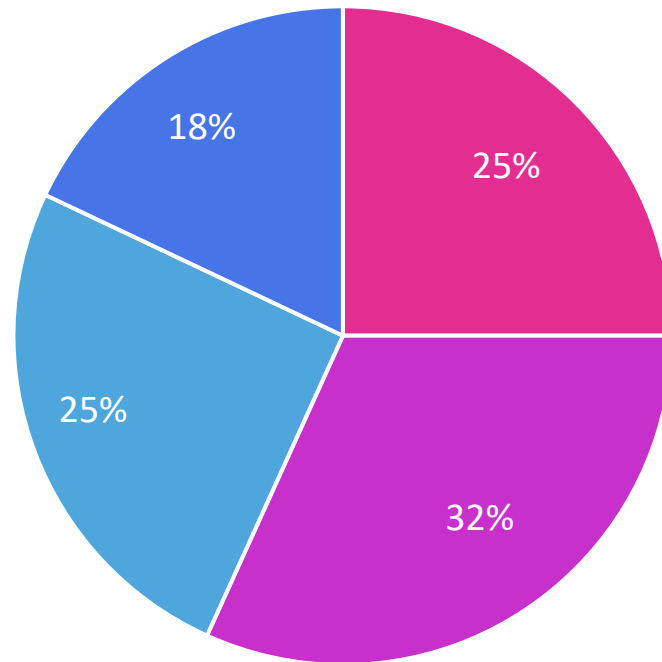
- **Contar con una persona que pueda evaluar y mantener nuestros sistemas y dispositivos es una buena práctica**
 - 47% de los usuarios son los responsables de la seguridad en su computadora

Uso de Firewall en Computadoras



- Más del 83% de los usuarios no utiliza o no sabe si su computadora cuenta con un software que permita controlar el tráfico de sus dispositivos

Monitoreo de Computadora por parte del Departamento de Tecnología



■ No ■ No lo sé ■ Sí ■ No aplica

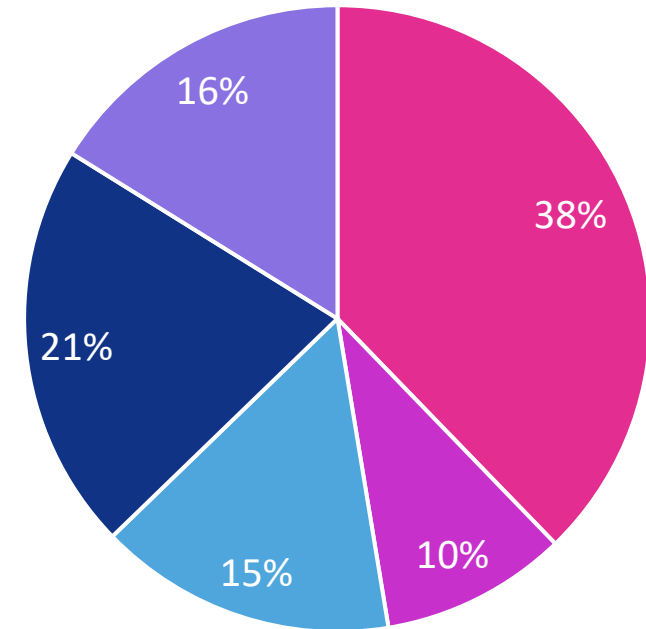
Las organizaciones que tienen implementado BYOD monitorean los equipos personales y tienen posibilidad de administrarlos de forma remota

- Esta administración debe hacerse en consideración de la protección de datos y privacidad de los usuarios

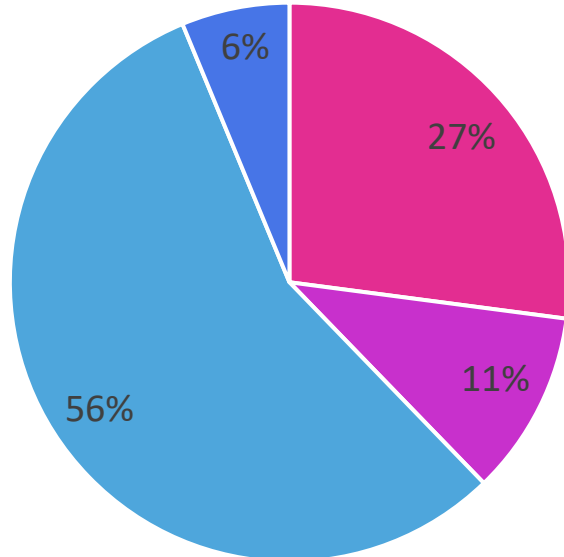
Frecuencia en el Respaldo de Información

- 10% de los usuarios nunca realiza un respaldo de su información mientras que 38% declara hacerlo cada vez que se acuerda

Los respaldos de información son una de las mejores medidas para estar preparado ante ataques como los de ransomware, fallas, pérdida o robo de los dispositivos



- De vez en cuando, cuando recuerdo
- Nunca
- Al menos dos veces a la semana
- Al menos una vez al mes
- Al menos una vez por semana



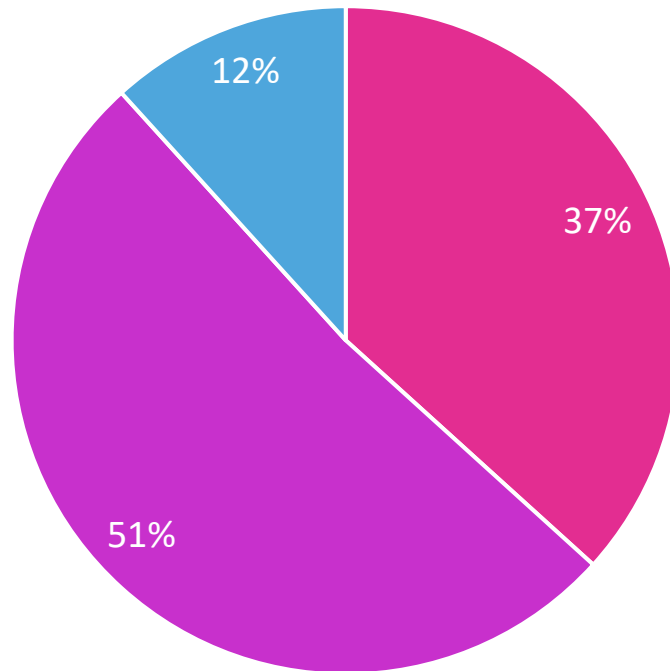
- En la nube
- La misma computadora
- Medios removibles externos como cinta, discos duros o unidades USB.
- No hago respaldos

- **96% de los usuarios realiza respaldos de su información**

- 27% lo hace en la nube
- 67% lo hace en medios físicos

Los respaldos realizados en sistemas en la nube presentan nuevos retos, por ejemplo:

- No dejar abierta la sesión en equipo compartidos
- Reforzar la seguridad del inicio de sesión
- Si se realiza algún cambio, al estar sincronizado, no podrá usarse el respaldo para regresar a una versión anterior

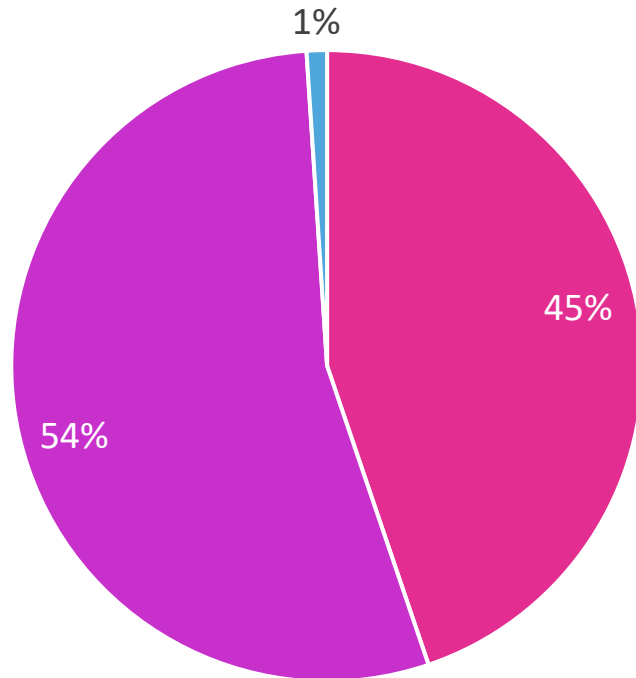


■ No ■ Sí ■ No aplica

- 37% de los usuarios no realiza una verificación de sus respaldos para supervisar que se hayan hecho de manera correcta

Muchos de los respaldos que los usuarios realizan, resultan estar incompletos y solo se advierte esta situación después de un incidente que provoca pérdida de información

Uso de la Misma Contraseñas en distintos Sitios

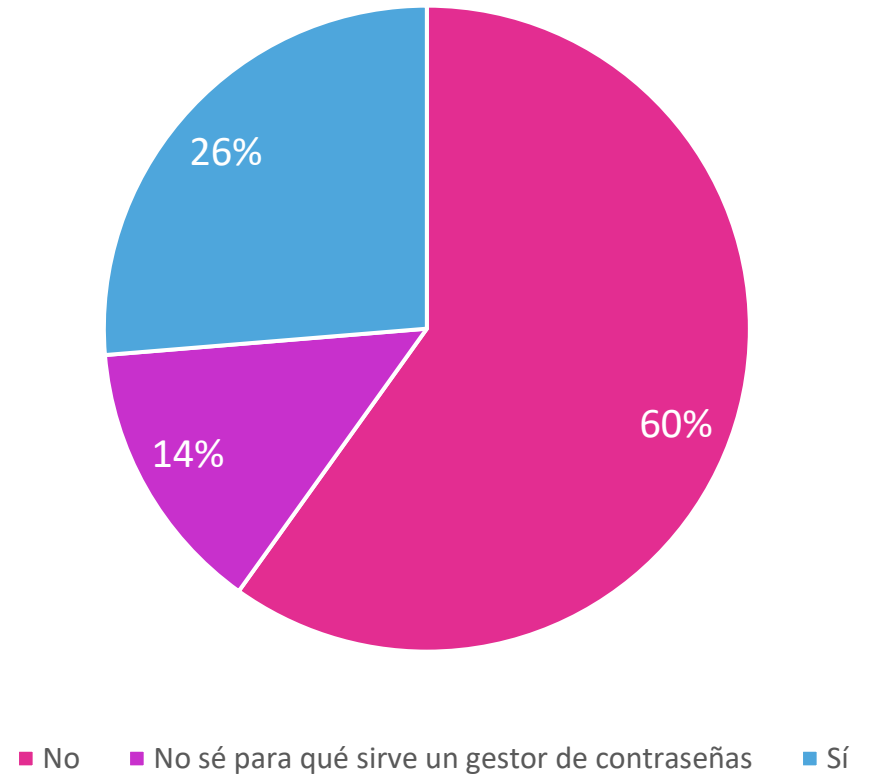


■ Sí ■ No ■ No sé cómo identificarlo

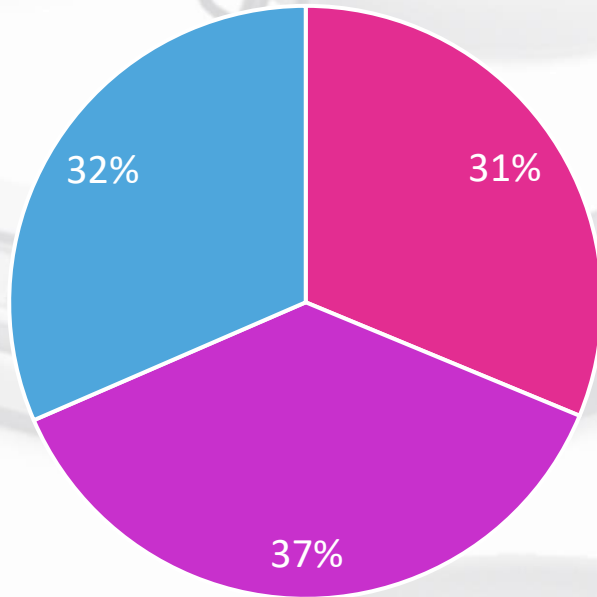
- **51%** de las personas utilizan las mismas contraseñas tanto para el trabajo como para las cuentas personales.
- 71% de las cuentas están protegidas por contraseñas que se utilizan en varios sitios web.
- 45% de los usuarios utilizan la misma contraseña para más de un servicio

El 60% de las personas confían en su memoria para administrar las contraseñas.

- Esto hace difícil de manejarlas, **aumenta la incidencia de repetir la misma contraseña en más de un sitio** y que los usuarios las apunten en lugares inseguros
- 26% de los usuarios utiliza un gestor de contraseñas



Autenticación Multi-factor (MFA) para Acceder a Cuentas

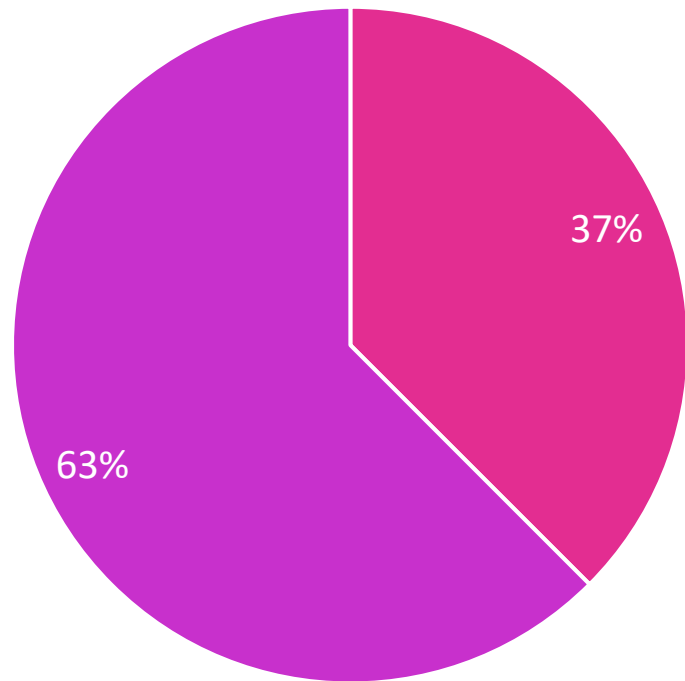


■ No sé que es la autenticación multi-factor ■ Sí ■ No

- **68% de los usuarios, no usa un segundo factor de autenticación**
 - Casi la mitad de ellos (31%) desconoce lo que es un segundo factor de autenticación

El uso de un segundo factor de autenticación es la mejor medida para reforzar la seguridad del inicio de sesión de nuestros sistemas, redes y dispositivos

Consentimiento para Salir en Publicaciones de Otras Personas

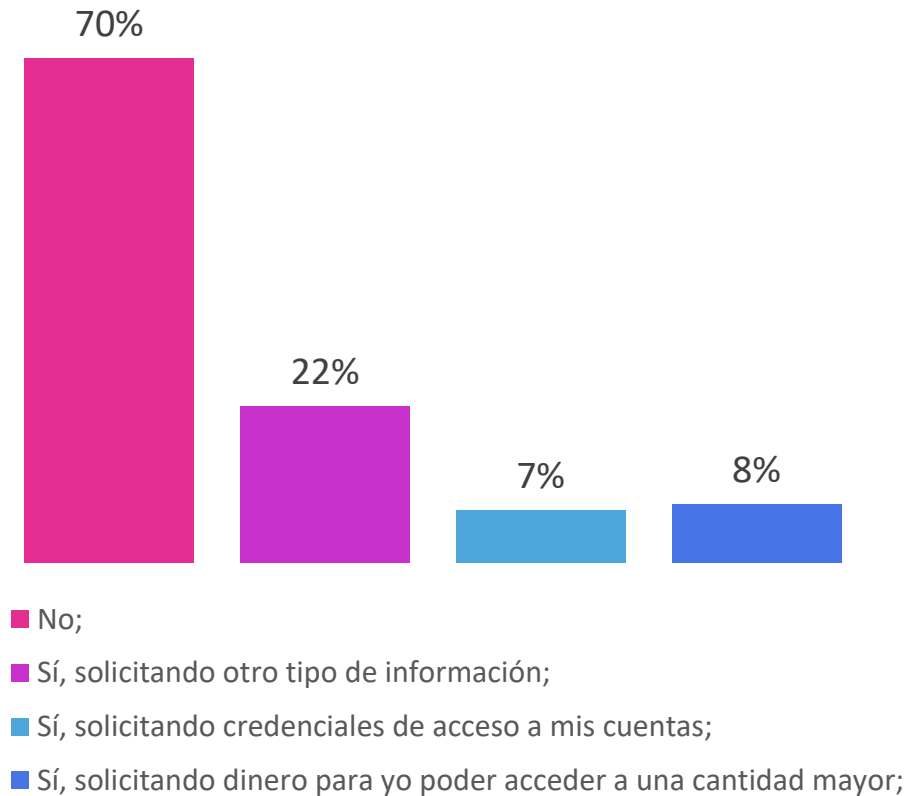


■ Sí ■ No

- 37% de los encuestados reporta haber aparecido en alguna fotografía o video dentro de alguna publicación realizada por otra persona y sin su consentimiento

Respetar la privacidad e intimidad es tarea para cada uno de nosotros, la mayoría de la gente que comparte imágenes de otras personas so sabe que es inapropiado hacerlo sin su autorización

Solicitud de Información Personal por Parte de Desconocidos

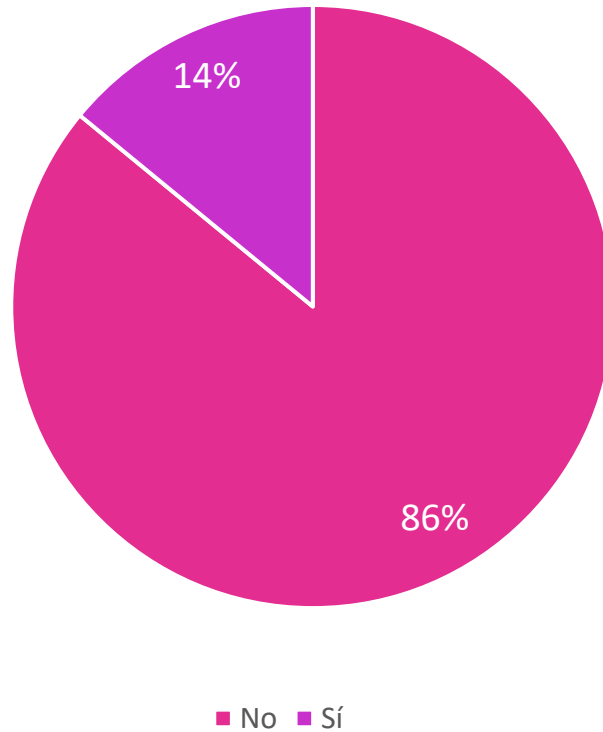


- 7% de los encuestados declara que les han solicitado credenciales de acceso a sus cuentas

El fraude y la suplantación de identidad comienzan la mayoría de las veces por engañar a los usuarios para que compartan su información personal

Solicitud de Fotografías Intimas

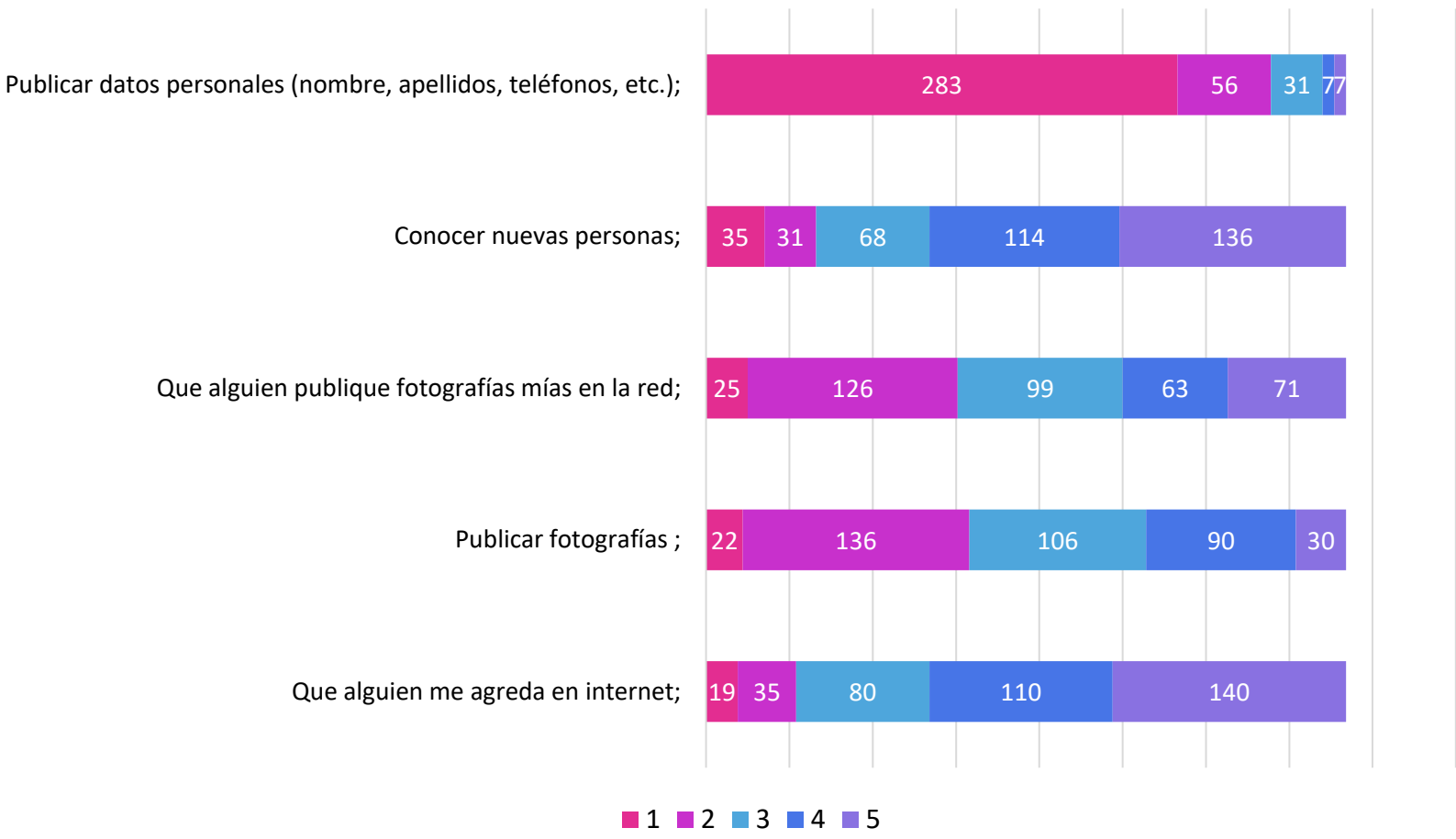
- 14% de los usuarios reportó que alguien le ha solicitado el envío de contenido de carácter íntimo



Lo más recomendable es no compartir contenido íntimo, pero si piensas hacerlo considera:

- Tener plena confianza en el destinatario o destinataria
- Recorta o tapa rasgos que puedan identificarte
- Desactiva la sincronización de fotos con la nube y revisa que no se subieron
- Usa servicios de mensajería segura

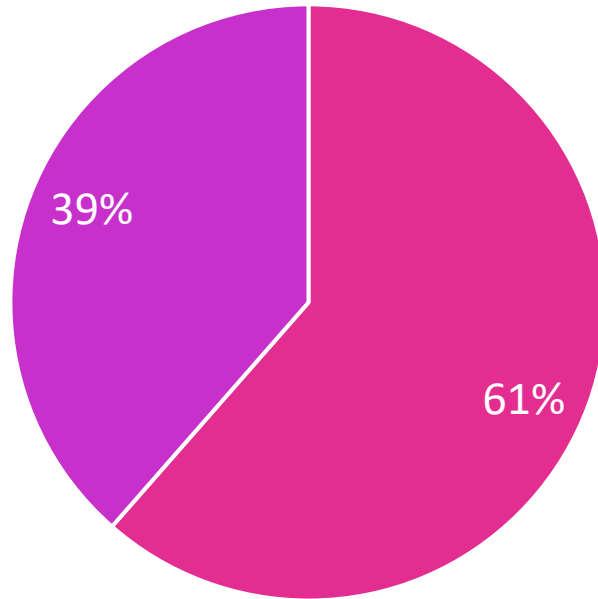
Mayores Peligros de la Interacción por Internet



Los usuarios consideran que la situación que más expone a los usuarios en Internet es compartir o publicar datos personales



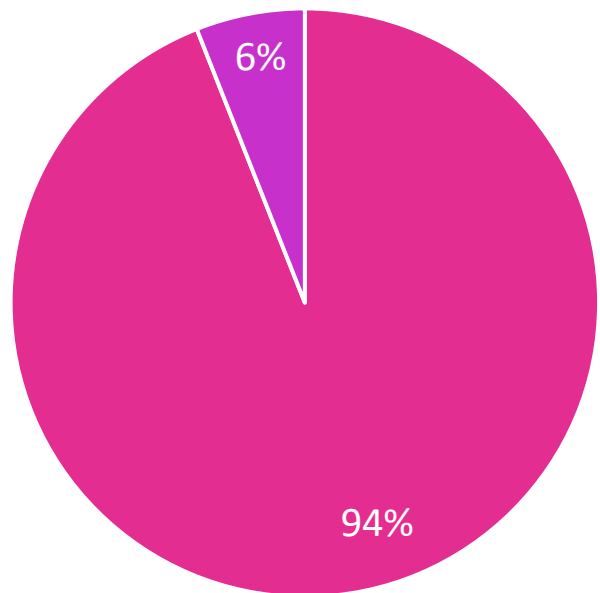
¿Has conocido físicamente a alguien a quien conociste inicialmente por Internet?



■ No ■ Sí

- El 39% de los usuarios ha conocido en persona a alguien que inicialmente contactaron por internet
- Según datos del MOCIBA 2019 el 42.90% de los adolescentes que han sido víctima de algún tipo de ciberacoso fue acosada por un desconocido
- 55% de los acosadores fueron hombres.

Las interacciones a través de medios electrónicos no permiten saber fácilmente si la persona del otro lado del teclado es quien dice ser



■ No ■ Sí

- **6% de los usuarios se han sentido amenazados o preocupados por comentarios que alguien más ha hecho a través de internet**
- En el periodo comprendido del 01 de enero al 14 de septiembre de 2020, la Guardia Nacional reporta haber recibido 2,898 denuncias de comentarios de amenaza en la red

Conclusiones

- **60% de los usuarios considera que su equipo no está protegido** ente las amenazas que presenta el uso de internet
- **La medida más importante para el uso de internet de forma segura es estar conectado a una red segura**
- La preocupación más grande de los usuarios de internet en la suplantación de identidad, seguida por el fraude y pérdidas financieras
- **53% de los usuarios fue víctima de alguna vulneración** en los últimos 12 meses, principalmente de pérdida de información, fraudes y pérdidas financieras
- Utilizar **contraseñas robustas fue considerada como la medida de seguridad más importante**
- **32% de las personas encuestadas utiliza su equipo personal para actividades de la empresa**
- **10% de la gente no actualiza nunca su software antimalware**
- Solo el **26%** de los usuarios utiliza un gestor de contraseñas
- **69%** de los usuarios, no sabe qué es o **no utiliza un segundo factor de autenticación**
- **14%** de los usuarios reportó que **alguien le ha solicitado el envío de contenido de carácter íntimo**
- Los usuarios consideran que la **situación que más expone** a los usuarios en Internet es **compartir o publicar datos personales**
- **39%** de los usuarios ha **conocido en persona** a alguien que inicialmente contactaron por internet
- **6% de los usuarios se han sentido amenazados o preocupados** por comentarios que alguien más ha hecho a través de internet

Estructura del estudio sobre políticas públicas y regulación en materia de ciberseguridad

MAPA DE ACTORES

Identificación de las o los hacedores de políticas públicas o de normatividades

MAPA DE INICIATIVAS LEGISLATIVAS

Régimen jurídico para determinar el grado de correspondencia con las necesidades de la sociedad

EJES DE LA CIBERSEGURIDAD

Impulsar acciones desde la AIMX para promover la cultura de la seguridad de las niñas, niños y adolescentes en México en el entorno digital, encaminadas a generar información útil para los pequeños internautas y medidas de prevención de conductas antisociales en su perjuicio

MAPA DE POLÍTICAS PÚBLICAS

Integrar y evaluar los esfuerzos por proteger a la infancia de los riesgos en su calidad de internautas

COMPENDIO ESTADÍSTICO

Revisión de datos relacionados con población objetivo (menores de edad), victimización, denuncias, concentración de casos

Fuente: Estado de las políticas y regulación sobre la ciberseguridad en México 2020 – AIMX, GEV

Conclusiones Generales

La ciberseguridad es una de las preocupaciones que mayor interés ha tenido recientemente, esto es confirmado por el reporte de riesgos globales del Foro Económico mundial de 2018, que menciona que los ataques de ciberseguridad son el tercer riesgo mayor a nivel mundial, detrás de los cambios climáticos y los desastres naturales

Las organizaciones que han adoptado esquemas de atención y gestión de riesgos formales han tenido una incidencia menor de vulneraciones de seguridad. En particular:

- *La concientización de los usuarios sobre las amenazas y la identificación de actividades y comunicación maliciosa,*
- *El reforzamiento de medidas de seguridad evitando usar las configuraciones por defecto de los sistemas, la autenticación de usuarios y autorización de cada acción realizada,*
- *La actualización de los sistemas y aplicaciones son las medidas de seguridad que mejor resultado han tenido.*

La adopción de una estrategia integral de seguridad que no dependa únicamente de una sola herramienta, sistema o persona. Es importante para que las organizaciones refuercen sus capacidades de Identificación, protección, detección, respuesta y recuperación antes incidentes de ciberseguridad.

[The Global Risks Report 2018 | World Economic Forum \(weforum.org\)](https://www.weforum.org/reports/global-risks-report-2018)

ESTUDIO SOBRE CIBERSEGURIDAD EN EMPRESAS, USUARIOS DE INTERNET Y PADRES DE FAMILIA EN MÉXICO 2021

