ESTUDIO

Hábitos de los usuarios en ciberseguridad en México

2019

ÍNDICE

FICHA METODOLÓGICA

2019

Realización de las mesas: los días 28 y 30, de enero, así como 1° de febrero.

12 horas

Duración total de las mesas.

5,011

Total de asistentes a las mesas de ciberseguridad.

Encuestas

Metodología utilizada en el estudio: Mesas interactivas de ciberseguridad.

★★★★★

±1.4%

Margen de error de la muestra.

★★★★★

95%

Nivel de confianza de la muestra.

★★★★★

0.5

Nivel de precisión.

INTRODUCCIÓN

La penetración y uso de los servicios de telecomunicaciones y radiodifusión, incluyendo la banda ancha e Internet, durante los últimos años permite, como nunca antes, la circulación de ingentes volúmenes de información y el establecimiento de comunicaciones de manera más fácil (Hernández, 2018). Eso, al mismo tiempo, incrementa exponencialmente la cantidad de incidentes que pueden afectar de manera negativa el uso de dicha información. En respuesta a esto, se han realizado diferentes colaboraciones internacionales, como las siguientes:

La Organización de las Naciones Unidas (ONU) reconoce los problemas que enfrentan los países en desarrollo para crear confianza y seguridad en la utilización de los servicios de telecomunicaciones y radiodifusión, incluyendo la banda ancha e Internet, por lo que hace un llamado a que se preste atención a la creación de capacidades, educación e intercambio de conocimiento entre múltiples interesados de todos los niveles y a la sensibilización entre los usuarios de los servicios de telecomunicaciones y radiodifusión, particularmente, entre los más vulnerados de la sociedad (ONU, 2016).

De acuerdo con algunas fuentes, México registra bajos niveles en materia de marcos legales, instituciones encargadas de tratar la ciberseguridad, así como en lo que respecta a programas de capacitación y certificación de organizaciones de carácter público en esta materia (PWC, 2016).

Por otro lado, la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la información en los Hogares (ENDUTIH) 2017 indica que en México hay, al menos, 71.3 millones de usuarios de Internet, que representan el 63.9% de la población de seis años o más. El crecimiento total de usuarios en México, del 2015 al 2016, fue de 4.7% y, del 2016 al 2017, fue de 8.1%. La tendencia creciente en el número de usuarios exige una atención inmediata a los aspectos de ciberseguridad. Si a esto se agrega que entre las principales actividades de los usuarios de Internet en México, de acuerdo con la ENDUTIH, se encuentran la obtención de información (96.9%), entretenimiento (91.4%), comunicación (90.0%), acceso a contenidos audiovisuales (78.1%) y acceso a redes sociales (76.6%) -actividades en las cuales se puede intercambiar información sensible-, la elaboración e implementación de estrategias y planes nacionales que agilicen la transición hacia un ciberespacio seguro reviste gran importancia. Lo anterior, a fin de que sea posible aprovechar al máximo los enormes beneficios que generan estas nuevas tecnologías (PWC, 2016).

La globalización e hiperconectividad exigen soluciones centradas en la colaboración internacional de manera precisa, eficaz y eficiente (SEGOB, 2017). Como plan para mejorar la educación y capacitación de la sociedad civil en aspectos de ciberseguridad, con apoyo de la Organización de los Estados Americanos (OEA) y recursos del Gobierno del Reino Unido, la Subsecretaría de Comunicaciones de la Secretaría de Comunicaciones y Transportes (SCT) realizó este estudio, con el fin de coadyuvar a identificar la situación actual de la ciberseguridad en México con miras a generar estrategias para fortalecer la confianza y la utilización segura de los servicios de telecomunicaciones y radiodifusión, incluyendo la banda ancha e Internet, en el país.

OBJETIVOS Y METODOLOGÍA

Objetivos generales

Realizar mesas de trabajo, a escala nacional, para identificar las experiencias de los usuarios respecto de las principales problemáticas de ciberseguridad que podrían afectarlos en su vida cotidiana.

Objetivos particulares

Concientizar a los usuarios sobre cómo utilizar de manera segura las tecnologías y cómo el uso de éstas puede impactar su vida.

Evaluar y analizar la información recopilada, con la finalidad de identificar áreas de oportunidad para la creación de políticas públicas en materia de ciberseguridad en México.

Metodología

Mesas de trabajo:

Se realizaron mesas de trabajo a lo largo de tres días (28 y 30 de enero, así como 1° de febrero de 2019), en los Centros de Inclusión Digital (CID) de la SCT. Los CID conforman una red nacional de centros para la capacitación y educación digital, compuesta por 32 ubicaciones, una en cada entidad federativa. Ahí, cualquier persona puede acudir y conectarse con nuevas tecnologías de la información, aprender a utilizarlas y emprender proyectos innovadores.

Durante el desarrollo de cada mesa se impartieron conferencias de concientización sobre ciberseguridad. Se realizaron dos sesiones por día: una enfocada a adultos, en horario matutino, y la segunda, a menores de edad, en horario vespertino. Cada participante fue requerido para asistir a una sola sesión. Cada sesión tuvo una duración de dos horas, por lo que, en su totalidad, este ejercicio tuvo una extensión de 12 horas.

La interacción con los participantes fue lograda por medio de tabletas, computadoras y equipo de telepresencia, recursos que fueron facilitados por los CID.

Las conferencias se impartieron en todos los estados de la República Mexicana. A lo largo de cada sesión, se formuló un total de 25 preguntas (Anexo A), mismas que la audiencia, durante el desarrollo de las conferencias, respondió por medio de una aplicación en línea diseñada especialmente para el evento; en ella se mostraban las preguntas correspondientes a cada tema. En algunos casos, de manera complementaria, se utilizaron cuestionarios en papel con las mismas preguntas.

Se pidió a los participantes, al momento de su registro, datos básicos (edad, género, estado de residencia y escolaridad) e información sobre si contaban con Internet en sus viviendas, datos móviles en sus dispositivos celulares y si habían participado anteriormente en alguna conferencia de ciberseguridad. Además, y de manera opcional, se les pidió información sobre sus redes sociales. Cabe señalar que, por cuestiones de no aplicabilidad en el caso de los menores de edad, no se les pidió responder las preguntas 7, 19, 20, 21, 22, 23 y 24 del cuestionario.

Análisis de datos:

Las respuestas brindadas por los participantes se vaciaron en hojas de cálculo para conformar una base de datos. Con dicha información se realizó el análisis estadístico de las respuestas.

A fin de confirmar la representatividad de la muestra, se utilizó la siguiente fórmula:

$$n = \frac{N \times Z_a^{\,2} \times p \times q}{d^2 \times (N-1) + Z_a^{\,2} \times p \times q}$$

Donde:
N= es el tamaño de la población.
Z= el nivel de confianza.
p= probabilidad de éxito.
q= probabilidad de fracaso.
d= precisión o error muestral.

ESTADOS	PARTICIPANTES
AGUASCALIENTES	150
BAJA CALIFORNIA	70
BAJA CALIFORNIA SUR	54
CAMPECHE	117
CHIAPAS	144
CHIHUAHUA	103
COAHUILA	57
COLIMA	65
CDMX	202
DURANGO	178
GUANAJUATO	198
GUERRERO	74
HIDALGO	214
JALISCO	159
MICHOACAN	137
MORELOS	178
EDOMEX	230
NAYARIT	107
NUEVO LEON	81
OAXACA	78
PUEBLA	184
QUERETARO	163
QUINTANA ROO	75
SAN LUIS POTOSI	198
SINALOA	78
SONORA	232
TABASCO	115
TAMAULIPAS	145
TLAXCALA	212
VERACRUZ	195
YUCATAN	86
ZACATECAS	165
NO INDICARON LUGAR DE RESIDENCIA	567
TOTAL	5,011

Tabla 1: Participación por entidad federativa

La convocatoria para participar en estas mesas de ciberseguridad se distribuyó a través de los CID, logrando una asistencia total de 5,011 personas entre adultos y menores de edad. De esa cifra, 4,444 participantes indicaron su lugar de residencia, mientras que 567 participantes no compartieron dicha información.

En la Tabla 1 se observa la participación total por estado, misma que se plasma en el mapa de la República Mexicana (Figura 1).

El estado con más participantes fue Sonora, mientras que el que contó con el menor número fue Baja California Sur.

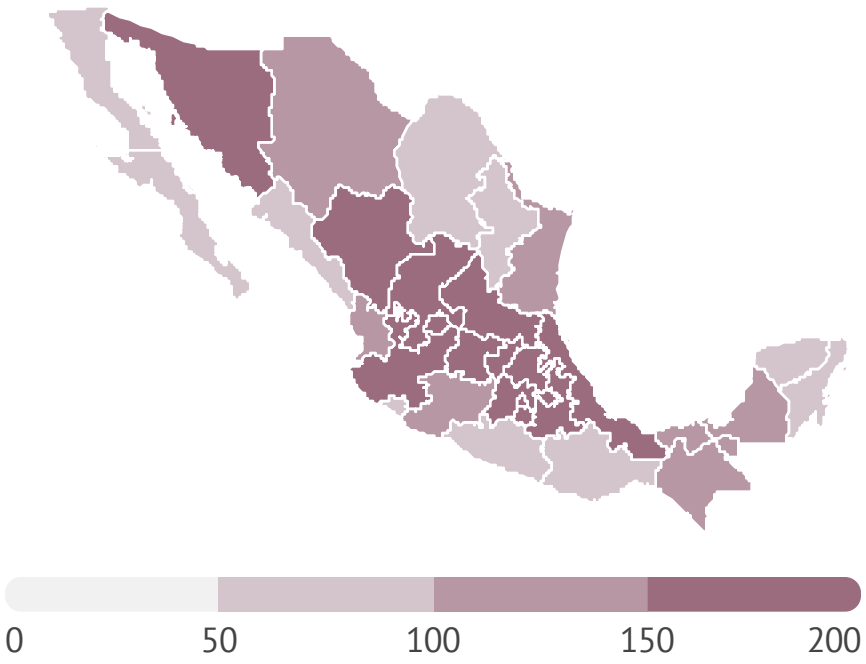

Fig. 1: Participación por entidad federativa

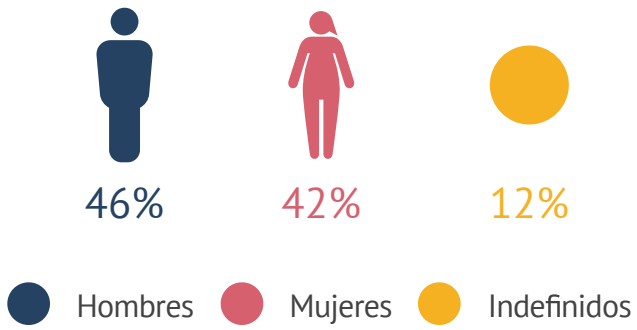

Fig. 2: Distribución por sexo

De acuerdo con los datos reportados por la ENDUTIH 2017, la distribución de personas en el ciberespacio corresponde a un 49.2% de hombres y un 50.8% de mujeres. No obstante, en el estudio realizado se tuvo una mayor participación de hombres (Figura 2).

En la Figura 3 se observan los porcentajes de hombres y mujeres por estado de la República Mexicana, así como aquellos participantes que se identificaron con un sexo indefinido o prefirieron no contestar la pregunta.

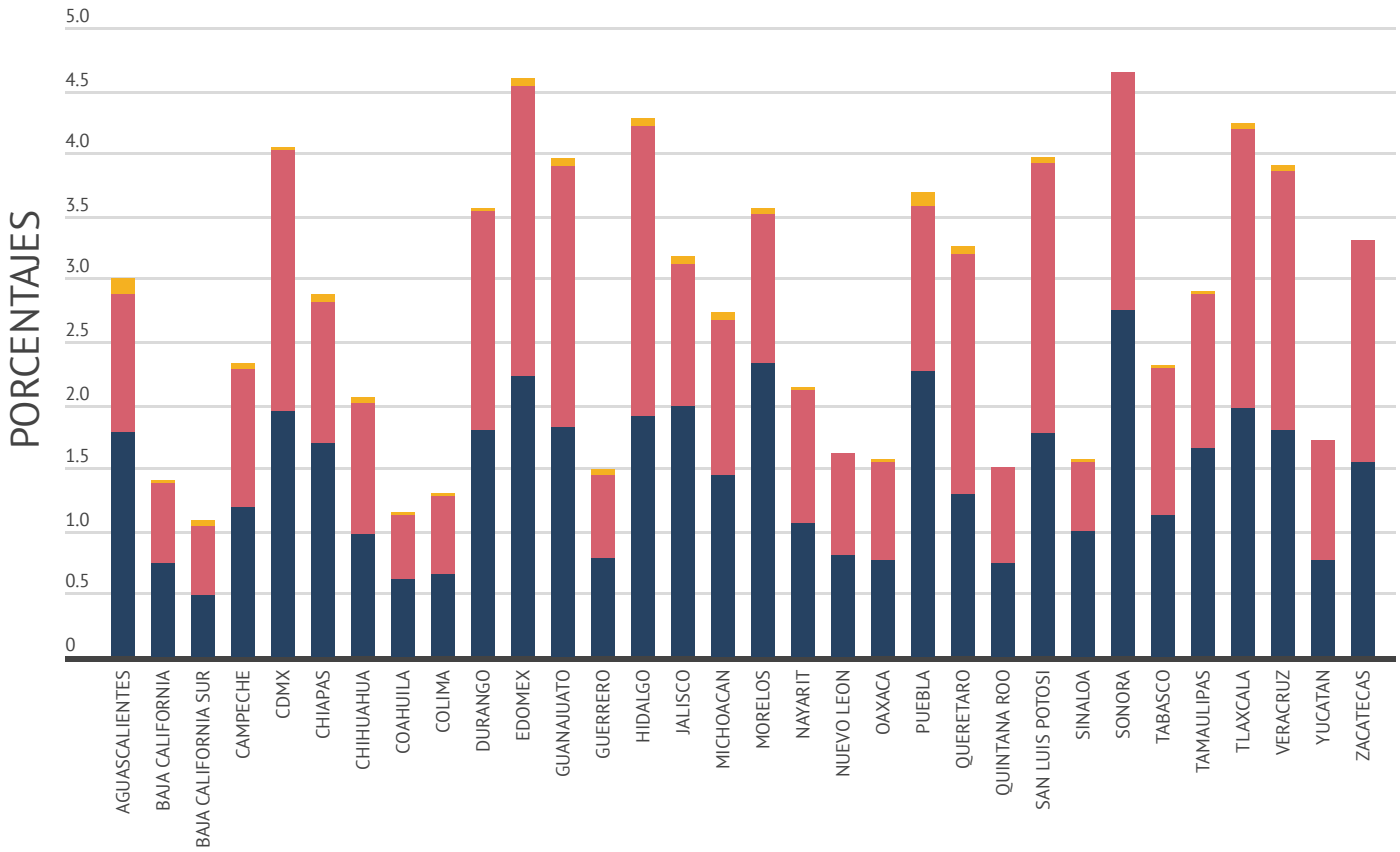

Fig. 3: Distribución por sexo y por entidad federativa

PARTICIPANTES
EDAD

En las mesas de ciberseguridad se registró una participación mayoritaria de menores de edad (54.3%), (Figura 4).

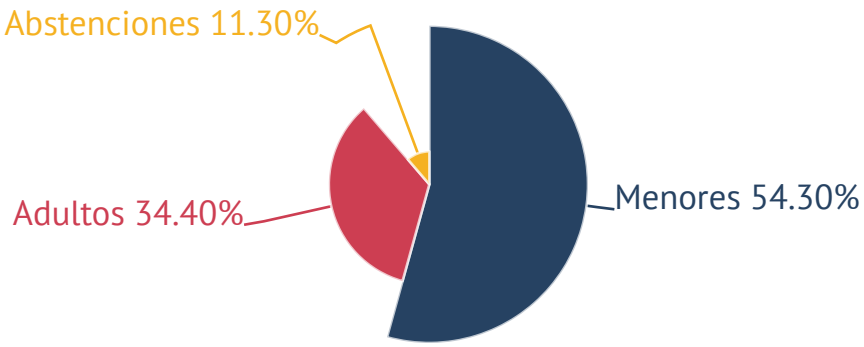

Fig. 4: Adultos y menores

En la Figura 5 se observa que, para este estudio, se tuvo una mayor participación de individuos de 7 a 13 años de edad[1]. Cabe destacar que es en este rango de edad en el cual se comienza a desarrollar el pensamiento lógico y moral, lo que les permite pensar antes de actuar y permanecer conscientes de las transformaciones de la realidad (Piaget,1991). Eso explica que en diversas fuentes, así como en las políticas de privacidad de algunas redes sociales, se considera ilegal o no recomendable que un usuario menor de 14 años tenga acceso libre.

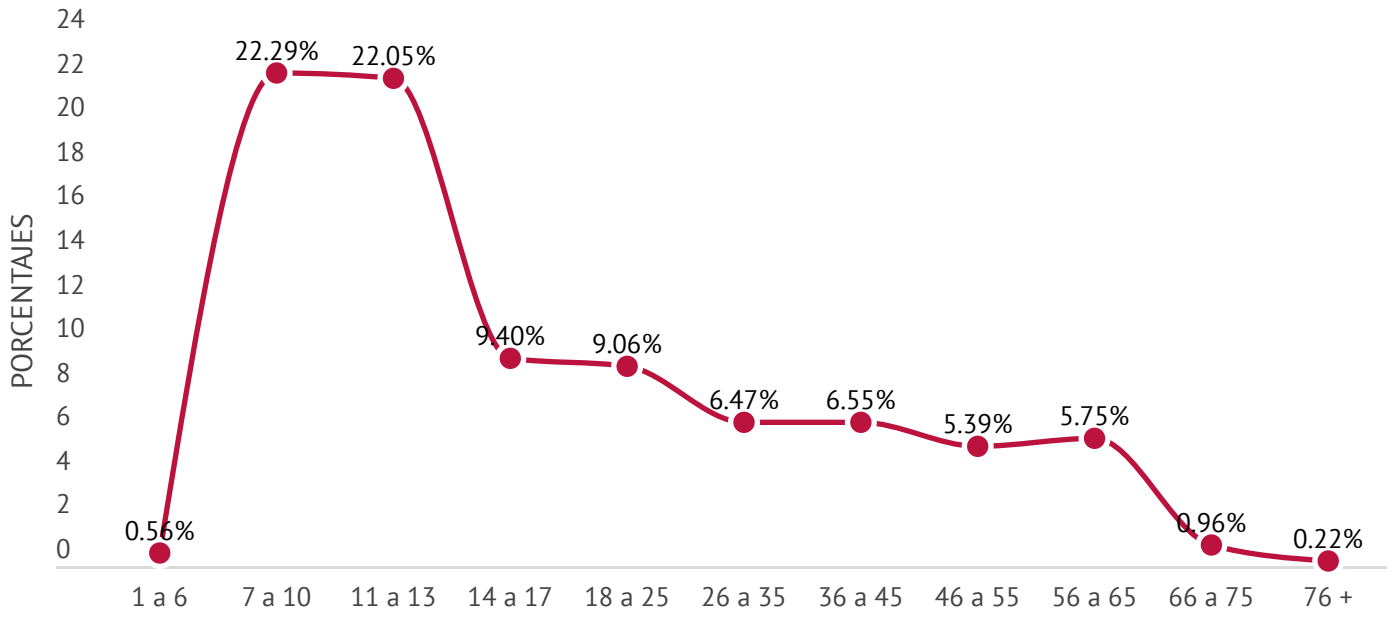

Fig. 5: Rangos de edades declaradas por los participantes

[1] Para la participación de los menores de edad, se solicitó y obtuvo autorización expresa por escrito de uno de los padres o tutores en cada caso.

PARTICIPANTES
ESCOLARIDAD

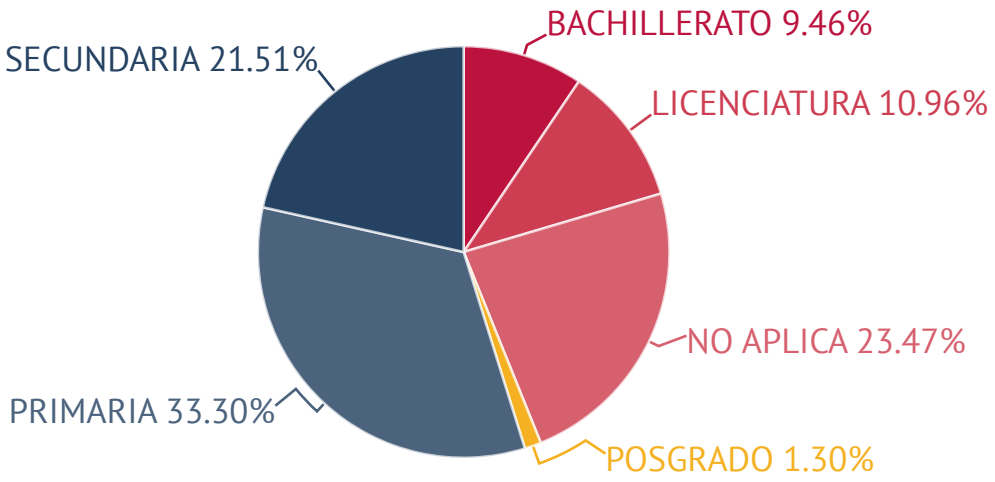

Fig. 6: Totales de escolaridad

En cuanto al nivel de escolaridad, en la Figura 6 se muestra que la mayoría concluyó estudios de primaria, lo que confirma que la mayor parte de los participantes tiene capacidad de lectura y escritura, lo que facilita el uso de la tecnología. Por otro lado, el 23.47% de los participantes no contaba con ninguno de los grados mostrados o prefirió no compartir su nivel máximo de escolaridad.

Adicionalmente, poco más de la mitad de los participantes indicó tener acceso a Internet en casa (Figura 7), mientras que menos de la mitad tiene acceso a Internet por medio de datos móviles (Figura 8).

Fig. 7: Total de participantes con internet en casa

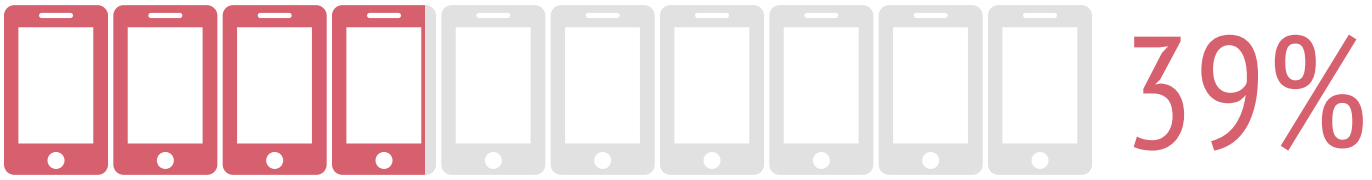

Fig. 8: Total de participantes con datos móviles

CONEXIONES A REDES PÚBLICAS

De acuerdo con el análisis de la información recolectada, en la Figura 9 se muestra el porcentaje de los participantes, por sexo y edad, que respondieron que sí se conectan a una red pública[2] de forma habitual. En la Figura 10 se puede observar que el 6% de los participantes se conecta de forma ocasional; esta cifra, sumada con quienes respondieron que sí se conectan a redes públicas, representa más de un tercio de los participantes. Con esta información, se puede inferir que existe un exceso de confianza por parte de los usuarios al conectarse a cualquier red pública, sin considerar que a través de dicha red su información podría ser robada, ingresar sin autorización al equipo móvil o realizar alguna actividad ilícita.

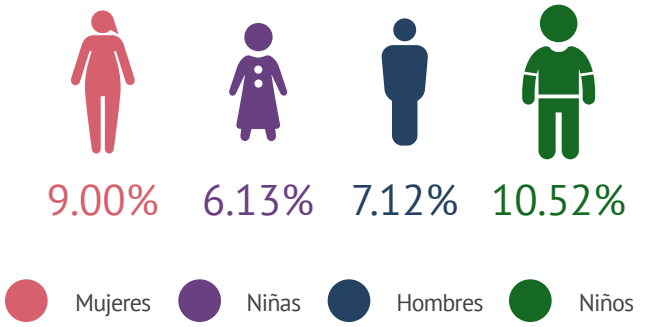

Fig. 9: Participantes que se conectan a redes públicas

En la Figura 10 se muestra también que, a nivel nacional, los niños son los que con mayor frecuencia se conectan a redes públicas, seguidos de las mujeres adultas. Esta situación se repite en la mayoría de las entidades federativas y pone en evidencia la necesidad de concientizar a la población acerca del cuidado que deben tener al conectarse a redes públicas; especialmente, orientar a los menores sobre el uso seguro de las redes.

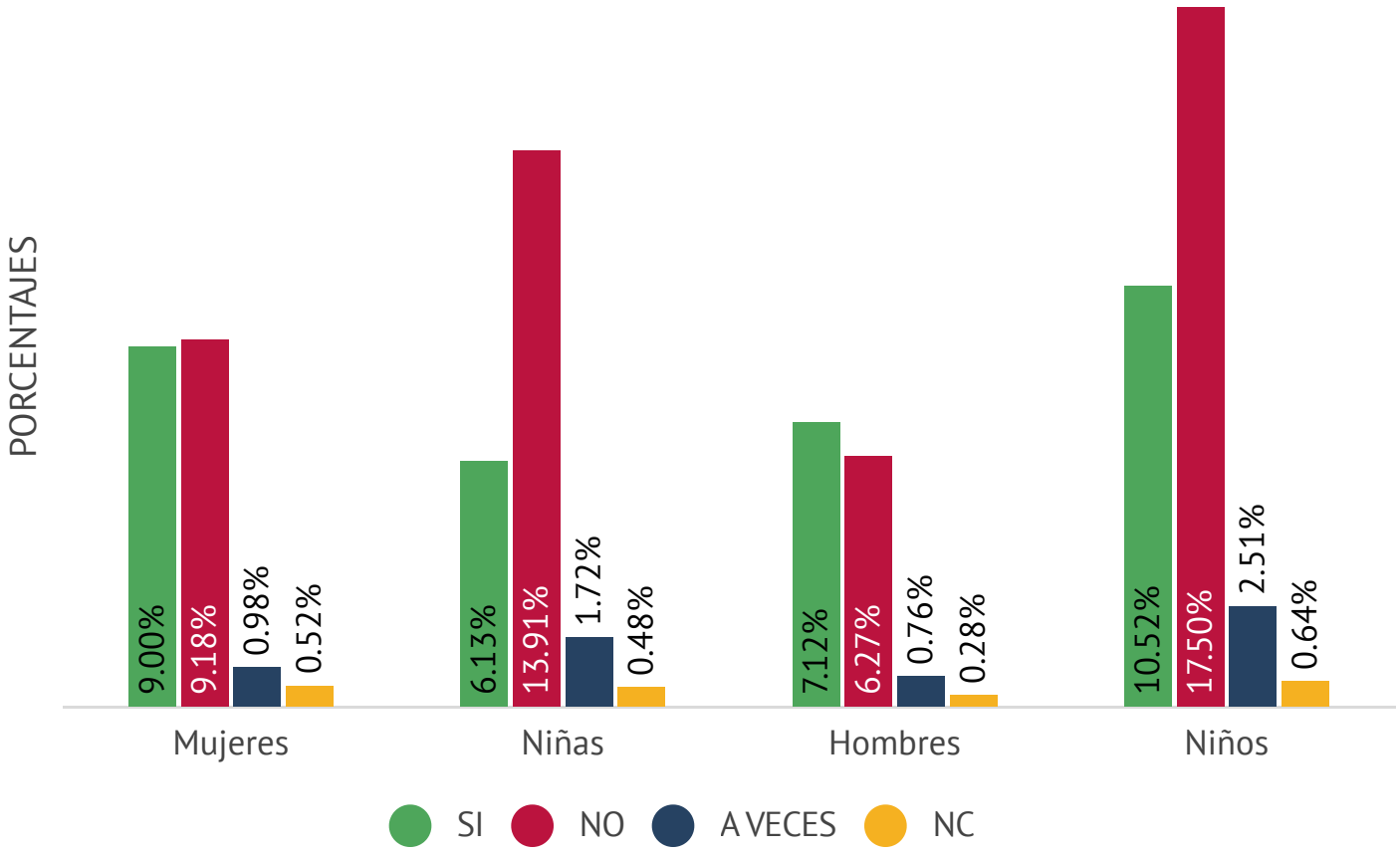

Fig. 10: Datos de conexiones a redes públicas

[2] "Red pública" se refiere a redes WiFi abiertas y accesibles en lugares públicos.

CONEXIONES A REDES PÚBLICAS
CONTINUACIÓN

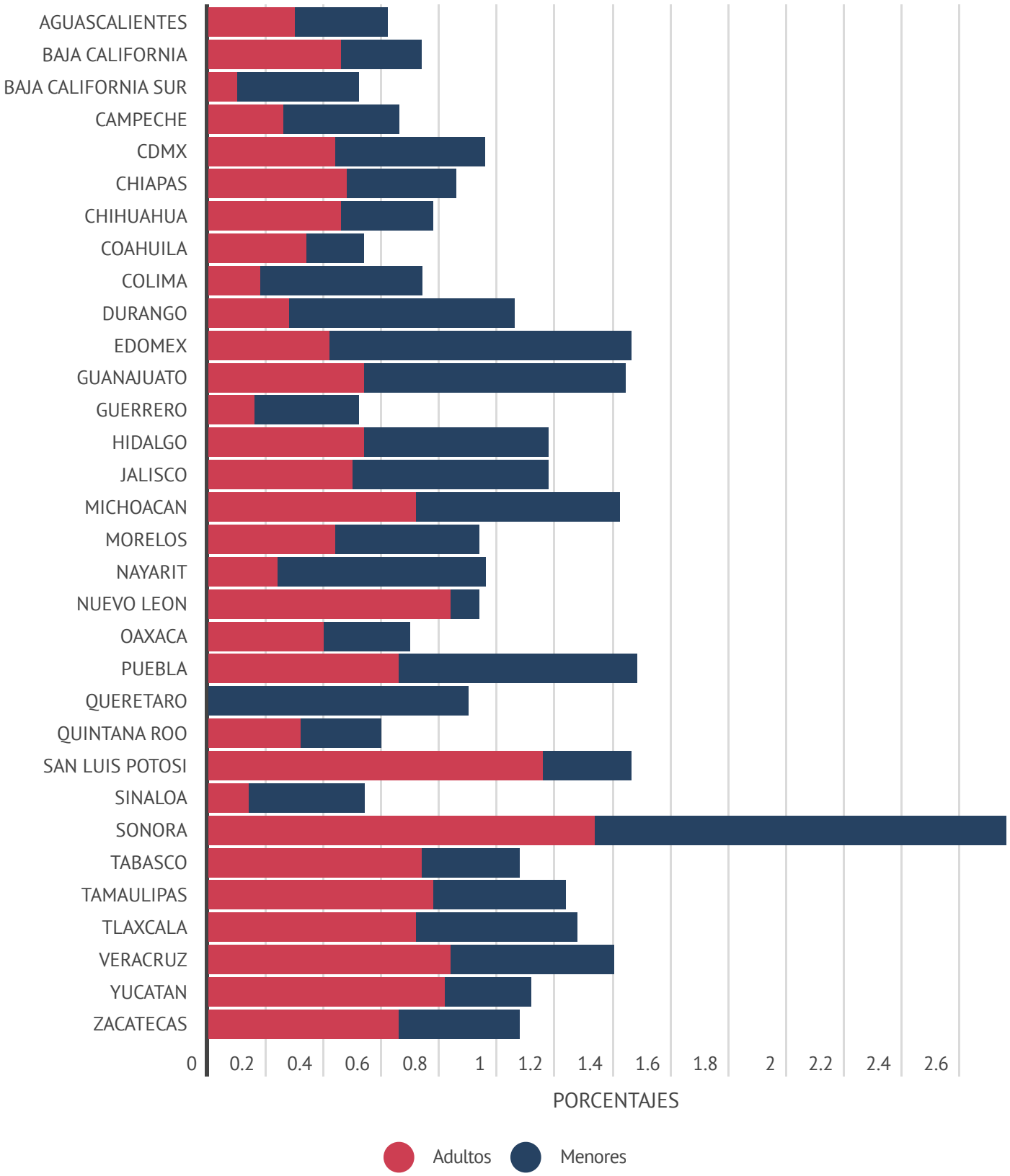

Fig. 11:Participantes que se conectan a redes públicas, por entidad federativa y edad

CORREO ELECTRÓNICO

Fig. 12: Participantes que cuentan con correo electrónico.

Fig. 13: Participantes que han abierto un correo electrónico de un remitente desconocido.

Fig. 14: Participantes que han dado clic en un hipervínculo de correo electrónico.

En la Figura 12 se muestra que sólo 37% de los participantes cuenta con correo electrónico y lo utilizan con frecuencia. Adicionalmente, un 10% de los participantes indicó que, pese a contar con correo electrónico, no lo utilizaban con frecuencia. El menor uso entre quienes contaban con correo electrónico se observó, principalmente, en el caso de los menores de edad; dicho comportamiento puede explicarse con el hecho de que el uso y acceso a diferentes aplicaciones requiere dar de alta un correo electrónico, que los menores crean sin la intención de utilizarlo como medio de comunicación.

Una de las problemáticas asociadas a los servicios de correo electrónico en México es el correo no solicitado (spam), que representa el 58.1% del correo recibido, de acuerdo con algunas fuentes (Symantec, 2019).

Un punto a resaltar es que poco menos de la cuarta parte de los participantes declaró haber abierto alguna vez un correo de tipo spam (Figura 13). Muchas veces, estos correos se utilizan para mandar códigos maliciosos o solicitar que se ingrese a algún sitio en línea donde se pide información sensible a la víctima, la cual puede ser utilizada para cometer algún delito. Otro dato importante es que casi un tercio de los participantes que declaró haber abierto un correo tipo spam, ha dado clic a un hipervínculo contenido en este tipo de correos (Figura 14).

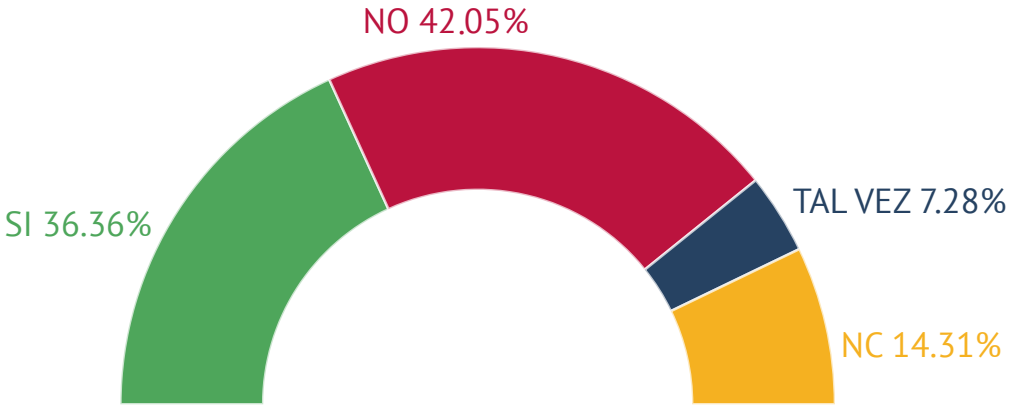

Fig. 15: Participantes que leen los permisos antes de instalar aplicaciones

Durante el uso de tecnología móvil (celulares y tabletas), es muy común instalar aplicaciones adicionales a las que vienen de fábrica. A ese respecto, la Figura 15 muestra que casi la mitad de los participantes (42.05%) indicó que no revisa el contenido de los permisos requeridos; dicho porcentaje está compuesto en su mayoría por menores de edad (Figura 16).

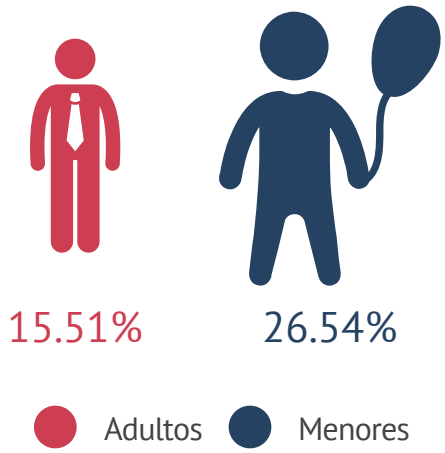

Fig. 16: Participantes que no leen los permisos antes de instalar aplicaciones en dispositivos móviles, por edad.

La no revisión de los permisos requeridos representa un importante hueco de ciberseguridad en el uso de los dispositivos móviles. Lo anterior, debido a que muchas aplicaciones pasan como oficiales o no maliciosas cuando, en realidad, se encargan de robar información o buscar accesos hacia otros dispositivos. La instalación de este tipo de aplicaciones en dispositivos móviles puede afectar incluso a equipos de cómputo de escritorio, por ejemplo, al conectar el dispositivo móvil a la red de la casa o del trabajo.

A pesar de que empresas tienen políticas de seguridad en el uso de estos dispositivos, es interesante ver que en el hogar esto no se replique. Adicionalmente a esto, casi la mitad de los participantes (Figura 17) reportaron no tener antivirus en sus equipos móviles.

Fig. 17: Participantes con antivirus en su celular

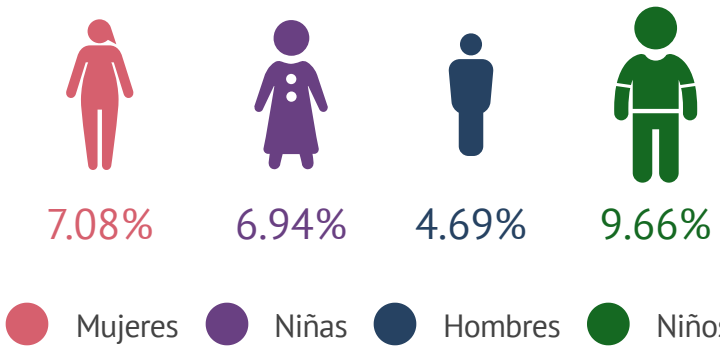

Fig. 18: Participantes que toman fotografías de su vida cotidiana

Las redes sociales son una actividad en la que se involucra el 76.6% de los internautas mexicanos (ENDUTIH, 2017). De acuerdo con la información proporcionada por los participantes de las Mesas, los niños son quienes más utilizan estas plataformas para publicar fotos de su vida cotidiana (Figura 18), seguidos de las mujeres adultas. Aunque, en cada uno de los dos casos antes referidos, el porcentaje no supera el 20%, considerando a quien lo hace esporádicamente, la compartición de fotografías de su vida cotidiana en redes sociales merece atención, para evitar que los usuarios compartan involuntariamente información sensible que pudiera ponerlos en riesgo (Figura 19).

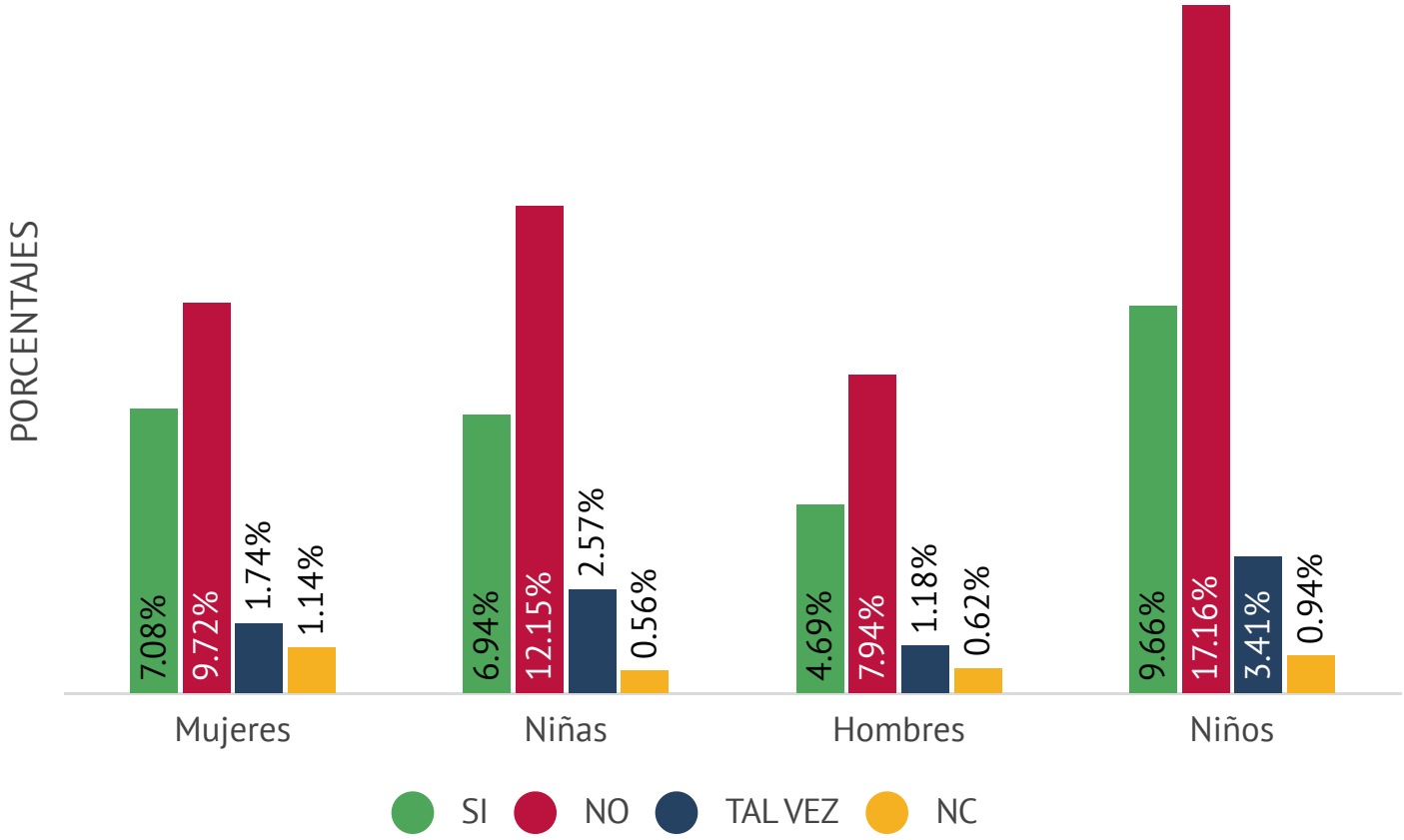

Fig. 19: Datos de participantes que toman fotografías de su vida cotidiana

REDES SOCIALES
CONTINUACIÓN

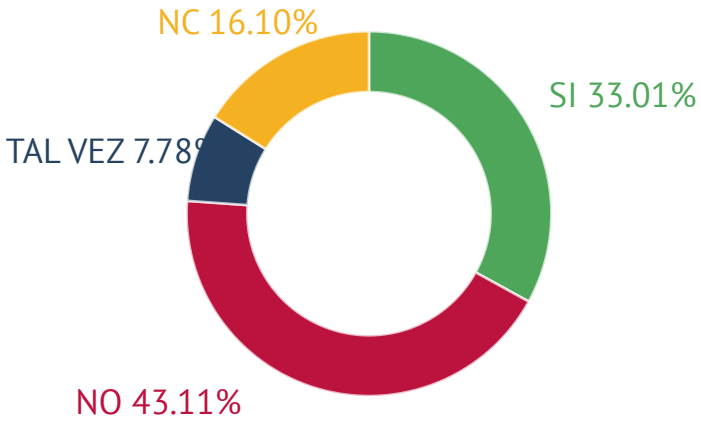

Fig. 20: Participantes que cuidan el contenido de sus fotografías antes de publicarlas.

Aunado a lo anterior, es importante destacar que casi la mitad (43.11%) de los participantes que toman fotografías para publicarlas en sus redes sociales no verifica si en dichas imágenes existe información sensible (Figura 20).

Las imágenes compartidas en redes sociales, o la información contenida en ellas, puede ser utilizada para causar afectación en quienes las comparten o en alguien de su círculo social. Por ejemplo, quienes suben fotografías de diplomas o reconocimientos están divulgando, entre otras cosas, el nombre completo de quien recibió dicho reconocimiento, así como el nombre de la institución que lo otorgó (con lo que se puede inferir la ubicación del centro de estudios y nivel socioeconómico de la persona).

Aunado a esto, otra mala práctica de los participantes en redes sociales consiste en publicar su ubicación al llegar a un lugar en específico. Esto puede dar pie a otros delitos como secuestro o robo de casa habitación, ya que los potenciales atacantes tienen acceso a la ubicación en tiempo real de la víctima. A través de esta práctica, incluso es posible detectar los sitios que más frecuentan los usuarios, así como la ubicación específica de los mismos, como escuela, casa, restaurantes o lugares recreativos.

Todos estos problemas se intensifican si el usuario no ha configurado adecuadamente los ajustes de privacidad de sus redes sociales, siendo lo ideal limitar el acceso únicamente a personas que conozca físicamente.

39% Publica su ubicación

en redes sociales

NAVEGACIÓN EN INTERNET

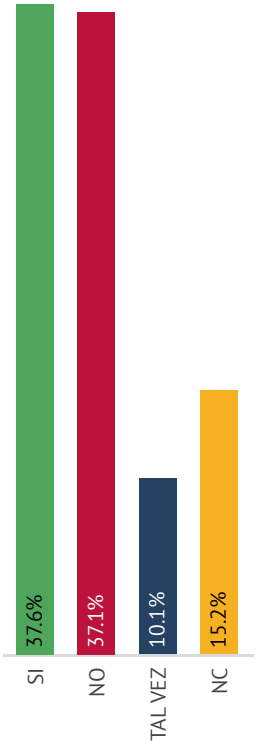

Fig. 21: Participantes que guardan sus contraseñas en papel o habilitan la función "recuérdame"

Si bien el uso del Internet no se limita exclusivamente al correo electrónico o redes sociales, estas actividades tienen algo en común: los mecanismos de autenticación. Es decir, el empleo de un nombre de usuario y contraseña para que el usuario pueda tener acceso a su información. De ahí la importancia de conocer los hábitos que tienen los usuarios al momento de gestionar sus contraseñas.

Al respecto, como parte de este ejercicio se detectó que más de la tercera parte de los participantes (Figura 21) tiene la costumbre de indicarle al navegador que recuerde su contraseña o anotarla en alguna libreta o papel que, en muchos de los casos, pone a un lado de la computadora o sobre el monitor. Estas prácticas, si bien facilitan el uso de contraseñas para el usuario, no son recomendables ya que cualquier persona que tenga acceso a esas notas, o al dispositivo donde se indicó al navegador guardar la contraseña, puede ingresar y secuestrar las cuentas del usuario.

Otra actividad muy popular entre los usuarios de Internet es el entretenimiento, con un 91.4% de los internautas (ENDUTIH, 2017). En esta categoría podemos ubicar a los juegos en línea.

Respecto a este último tema, se detectó que los menores son quienes tienden a jugar más en línea, en comparación con los adultos (Figura 22). Aunque por sí solo jugar no es algo que represente un riesgo para la seguridad del menor, el no conocer personalmente a los otros jugadores con los que interactúa sí representa un riesgo. Por ejemplo, un delincuente podría aprovechar el anonimato que dan estas plataformas para hacerse pasar por alguien más, con la finalidad de relacionarse con el menor y ganarse su confianza; de esa manera, podría obtener acceso a información sobre los hábitos de su hogar, entre otras cosas, comprometiendo su seguridad y la de su familia o amigos.

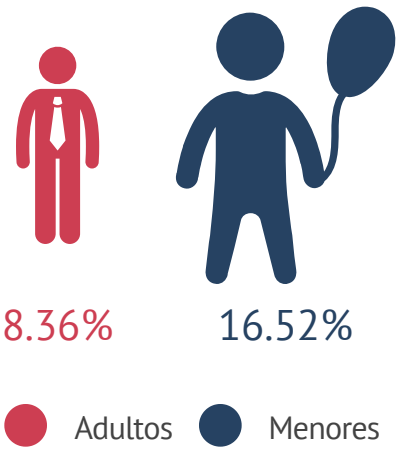

Fig. 22: Adultos y menores que juegan en línea

NAVEGACIÓN EN INTERNET
CONTINUACIÓN

El Internet se ha convertido en una herramienta que permite conocer a varias personas, al mismo tiempo que mantener o terminar relaciones ya establecidas, todo ello sin siquiera salir de casa (Fogaça, 2008). Entre los participantes, el uso de aplicaciones para conocer personas es casi igual entre hombres y mujeres, siendo ligeramente mayor en estas últimas (Figura 23).

Este tipo de interacción en línea podría involucrar un cierto nivel de intimidad entre los participantes, como es a través del envío de fotografías con poca o nula ropa. En el marco de este ejercicio, a nivel nacional, 34% de los participantes dijo haber enviado este tipo de fotografías; las mujeres representan más de la mitad de esa cifra. Sin embargo, es importante resaltar que hay estados de la República Mexicana, como el caso de Puebla, donde las respuestas de los hombres indican que son ellos quienes envían más fotografías con poca o nula ropa. En la Figura 24 se muestran los resultados por entidad federativa.

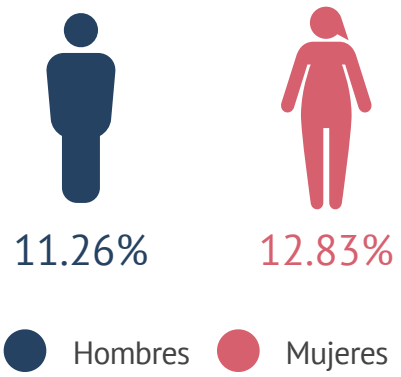

Fig. 23: Adultos que han utilizado aplicaciones para conocer personas

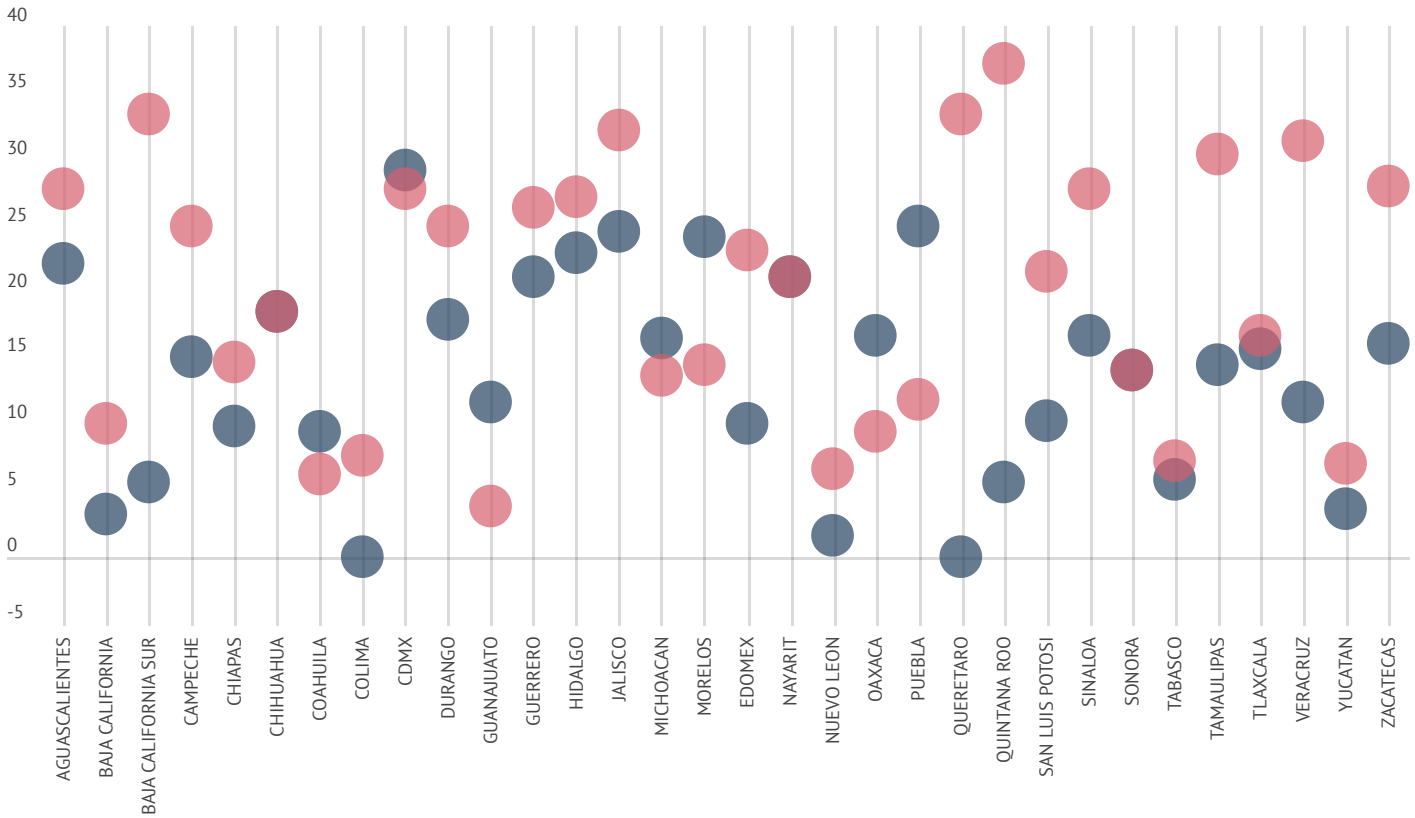

Fig. 24: Participantes que han enviado fotos con poca o nula ropa, por sexo y entidad federativa

En la Figura 25 se muestra la distribución por estado de la República Mexicana respecto a la divulgación de fotografías con poca o nula ropa. La Ciudad de México, Jalisco e Hidalgo son las entidades en donde los participantes dijeron compartir más este tipo de contenido, mientras que Colima, Nuevo León y Yucatán son los que menos lo envían.

Las cifras anteriores son preocupantes, debido a que este tipo de fotografías pueden llegar a manos equivocadas y ser publicadas en Internet, quedando a disposición de cualquier otro internauta. Aunado a esto, los avances tecnológicos han dado lugar a la multiplicación de los usos que se le pueden dar a los datos y de los lugares donde éstos se almacenan (Terwangne, 2011), haciendo casi imposible su eliminación una vez que se encuentran en línea.

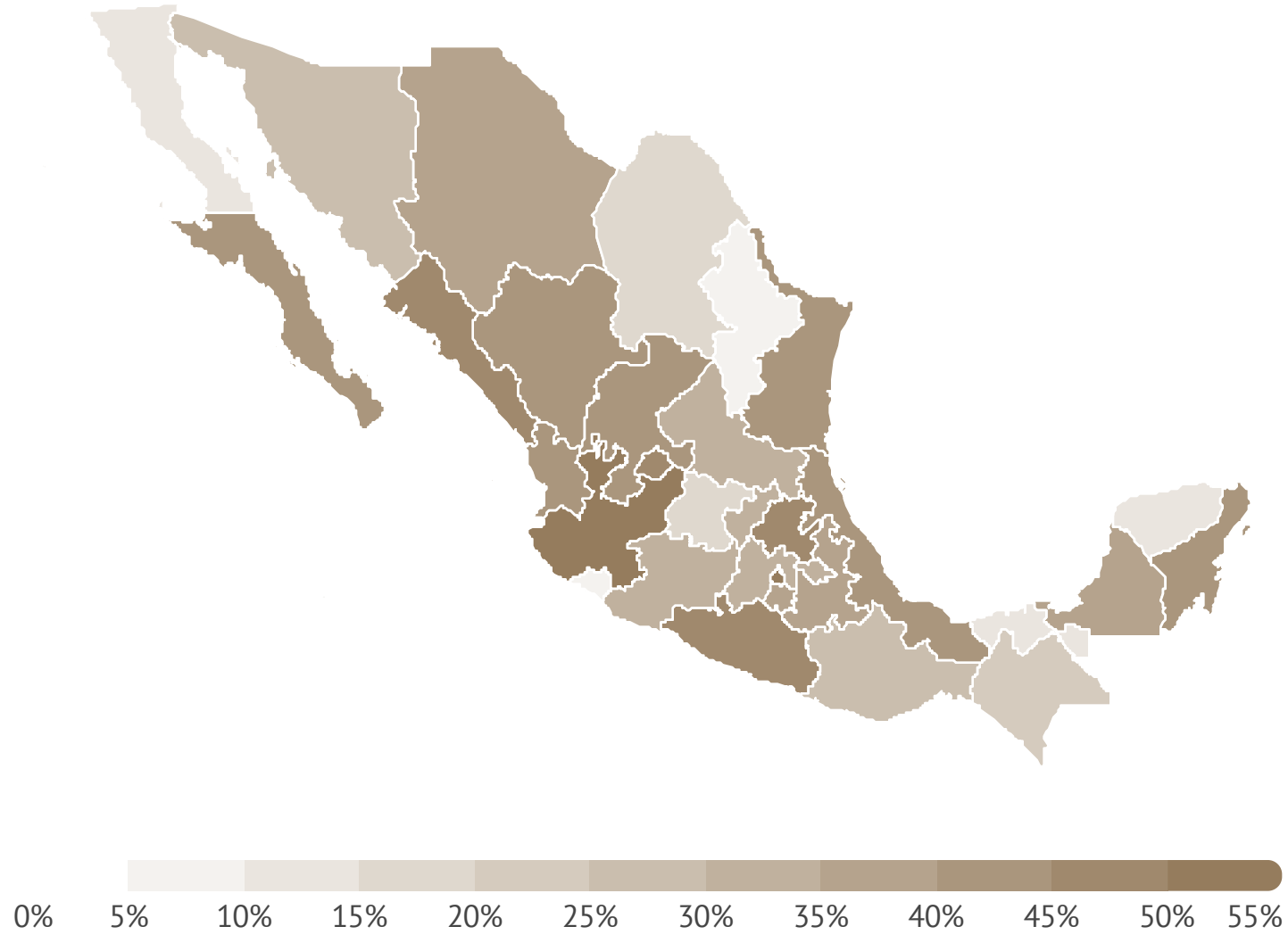

Fig. 25: Participantes por entidad federativa que han enviado fotografías con poca o nula ropa

Fig. 26: Adultos participantes que le dan dispositivos electrónicos a menores de edad para entretene

Los servicios de telecomunicaciones y radiodifusión, incluyendo la banda ancha e Internet, se han convertido en el "territorio natural" de los más jóvenes (de Larra, 2005). Por ello, es cada vez más frecuente que los padres otorguen algún dispositivo electrónico a sus hijos, ya sea para acercarlos a las nuevas tecnologías o simplemente como una ayuda en la crianza y el entretenimiento del menor. En estos casos, podría caerse en un esquema de "niñeras tecnológicas", que permiten a los padres tener más tiempo y libertad para realizar otro tipo de actividades, sin la necesidad de preocuparse por el menor de edad o lo que está haciendo.

Como parte de este ejercicio, el 37% de los padres (Figura 26) dijo otorgar dispositivos electrónicos a sus hijos con la finalidad de mantenerlos entretenidos. No obstante, durante las mesas de trabajo realizadas con menores de edad, éstos comentaron que dicha práctica es más frecuente, o al menos así lo perciben.

Lo anterior, deja entrever una posible problemática respecto a la interacción existente entre padres e hijos convirtiendo el uso de la tecnología en una forma de aislamiento entre ellos; este distanciamiento familiar no sólo conlleva a la adquisición de nuevas pautas de comportamiento posiblemente negativas, sino también el desarrollo de determinadas colectividades subculturales[3] (ABELA, 2003).

Otro de los riesgos que conlleva brindar un dispositivo tecnológico a los menores es que, en muchos de los casos, los padres no cuidan el contenido que visitan los menores de edad. En este ejercicio, sólo el 45% de los participantes (Figura 27) declaró que vigila la navegación de sus hijos en Internet. Al encontrarse que la mayoría de los adultos no realiza esta actividad, es importante señalar que los menores podrían estarse exponiendo a una variedad de riesgos en línea.

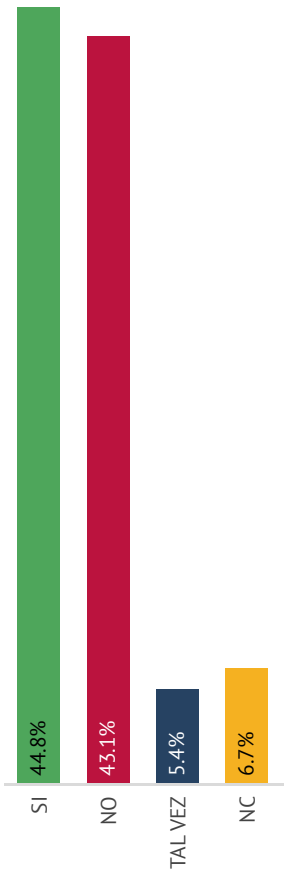

Fig. 27: Adultos que revisan el contenido que visitan los menores de edad

[3] Comunidades de cibernautas, que en el mundo real pertenecen a culturas diferentes, sin embargo, tienen algún punto en común y eso los hace conformar un nuevo colectivo en el ciberespacio.

PROBLEMÁTICAS IDENTIFICADAS

34% De los participantes ha sufrido algún tipo de acoso (bullying), de los cuales dos terceras partes son menores de edad.

27% De los participantes ha sufrido robo de identidad en medios digitales, de los cuales sólo una tercera parte son adultos.

21% De los adultos participantes ha sufrido fraudes financieros por medios digitales.

17% De los adultos participantes ha sufrido extorsión por el envío de fotografías con poca o nula ropa.

CONCLUSIONES

Durante el desarrollo de las mesas de ciberseguridad se identificaron distintas problemáticas que afectan a los internautas mexicanos que participaron en este estudio.

Respecto a las conexiones a redes públicas, es tanta la necesidad de estar conectados que, en muchas ocasiones, los usuarios no se detienen a pensar sobre los lugares a los que se conectan y las consecuencias que esto puede tener. Ello se refleja en que una tercera parte de los participantes afirmó conectarse a redes públicas, ya sea de forma habitual u ocasional. Si bien, no todas estas redes son maliciosas, existe el riesgo de que los usuarios se conecten a puntos creados con la finalidad de esparcir códigos maliciosos o robar información, por lo que es recomendable utilizar puntos seguros de conexión a Internet y, en general, fomentar la concientización de los usuarios sobre la importancia de buscar conexiones seguras.

En el caso del uso del correo electrónico, muchos participantes mostraron interés en aprender a distinguir las características que tienen los correos malintencionados, especialmente considerando que el 21% de los adultos participantes dijo haber sufrido fraudes financieros por este medio. Si bien la cifra pareciera no ser alta, sería recomendable redoblar esfuerzos con las entidades financieras para seguir concientizando a los usuarios respecto a este tema.

En el caso de los dispositivos móviles, se detectó que la mayoría de los participantes no cuida el tipo de aplicaciones que instala. En muchos casos, son menos cuidadosos con las aplicaciones que instalan en estos dispositivos, frente al cuidado que tienen instalando aplicaciones o programas en dispositivos de cómputo. Considerando que los dispositivos móviles son cada vez más utilizados, y que han remplazado en buena medida el uso de las computadoras, es de vital importancia educar a los usuarios para que aprendan a emplearlos de forma segura.

El estudio también reveló que la mayoría de los participantes no tiene una conciencia clara acerca de la privacidad en el uso de las redes sociales e Internet. Al vivir en una era digital, es cada vez más frecuente encontrar usuarios que publican partes de su día a día en este tipo de sitios (fotografías, sitios que visita y opiniones, entre otras cosas) o utilizan estas plataformas para buscar pareja o relacionarse con otras personas. Todo ello, de no hacerse con el nivel de cuidado adecuado, podría exponerlos a delitos como robo de identidad, secuestro, trata de personas y corrupción de menores. De ahí la importancia de crear conciencia en los ciudadanos sobre el uso de todas estas herramientas tecnológicas.

Por otro lado, el anonimato o falta de confrontación que ofrecen las redes sociales también motiva a los usuarios a compartir información que puede dañar a alguien más, como sucede con el acoso o bullying. Como sociedad, es importante atender estos problemas, ya que no sólo nos afecta como individuos, sino como comunidad. Aunque en México se cuenta con legislación para algunos de los riesgos mencionados, hace falta impulsar programas y leyes relacionados con el robo de identidad y el acoso o bullying.

CONCLUSIONES
CONTINUACIÓN

Entre los problemas más preocupantes que fueron identificados está el acceso libre que tienen los menores de edad a la tecnología. Dicho acceso muchas veces es propiciado por los mismos padres, quienes otorgan dispositivos tecnológicos (como celulares, tabletas y consolas de videojuegos) a los menores de edad, sin reparar en el contenido que visitan o las personas con las que se relacionan. Este problema se intensifica debido a que en Internet es posible encontrar cualquier tipo de contenido dando unos cuantos clics y, en muchos de los casos, los menores pueden verse frente a contenidos no adecuados para su edad, que pueden afectar su crecimiento y relacionamiento social. Aunado a esto, el anonimato que provee el Internet podría, incluso, permitir el contacto de pedófilos con los menores.

Es por esto que resulta de vital importancia vigilar el acceso de los menores de edad a Internet, promoviendo que su uso siempre sea supervisado por un adulto responsable, además de impulsar programas de concientización con los infantes y sus familiares para identificar de forma oportuna estos riesgos.

A través de los hallazgos de este estudio, se puede observar la importancia de continuar los esfuerzos para fomentar las capacidades digitales de los ciudadanos de forma integral, en donde se inculque el uso seguro y responsable de la tecnología, además de la creación de políticas públicas, leyes y programas sociales lo apoyen.

REFERENCIAS

Hernández, J. C. (2018). Estrategias Nacionales de Ciberseguridad en América Latina. Análisis GESI, (8), 1.

ONU (2016) 70/125. Documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información, A/RES/70/125: Asamblea General de las Naciones Unidas.

PwC (2016) Ciberseguridad y privacidad: De la percepción a la realidad, México: PricewaterhouseCoopers, S.C.

Secretaría de Gobernación (2017) Estrategia Nacional de Ciberseguridad, México: Gobierno de México.

Cécile de Terwangne (2012) 'Privacidad en Internet y el derecho a ser olvidado/derecho al olvido', IDP, Revista de Internet, Derecho y Política., Vol. 13, pp. 53-66 [En línea]. Disponible en: https://www.redalyc.org/pdf/788/78824460006.pdf (Accedido: 21/02/2019).

Cibele Izidorio Fogaça Vieira (2008) 'Amor Contemporâneo e Relações na Internet Ausência do Corpo nas Relações ', Artigo, RBSE 7(19), pp. 72-117 [En línea]. Disponible en: http://paginas.cchla.ufpb.br/rbse/VieiraArt.pdf (Accedido: 21/02/2019).

Jaime Andréu Abela (2003) 'INFANCIA SOCIALIZACIÓN FAMILIAR Y NUEVAS TECNOLOGÍAS DE LA COMUNICACIÓN', Portularia, 3, pp. 243-261 [En línea]. Disponible en: http://rabida.uhu.es/dspace/bitstream/handle/10272/156/b15148312.pdf?sequence=1 (Accedido: 21/02/2019).

Jean Piaget (1991) Seis estudios de psicología, 1a edn., España: Labor S.A.

Rocío Miranda de Larra (2005) Los menores en la Red: comportamiento y navegación segura. Fundación Auna [En línea]. Disponible en: http://jakintza.net/wp-content/uploads/Los_menores_red_Miranda.pdf (Accedido: 21/02/2019).

Symantec (2019) ISTR: Internet Security Threat Report https://img03.en25.com/Web/Symantec/%7B1a7cfc98-319b-4b97-88a7-1306a3539445%7D_ISTR_24_2019_en.pdf: Symantec.

ANEXO A

Pregunta
¿Tienes dudas sobre las instrucciones?
¿Utilizas la tecnología de forma responsable?
¿Te has conectado a una red pública abierta?
¿Cuentas con correo electrónico?
¿Has abierto alguna vez algún correo de algún desconocido?
¿Has dado clic en la liga que viene en los correos?
¿Has sufrido de algún problema financiero debido a un correo electrónico?
¿Has descargado aplicaciones de sitios no oficiales?
¿Revisas con detenimiento los permisos que requiere la aplicación antes de instalarla?
¿Tienes antivirus en tu celular?
¿Tomas fotos de tu vida cotidiana?
¿Cuidas el tipo de contenido (datos personales) que pones/subes en tus fotos?
¿Has sufrido bullying o acoso en medios digitales?
¿Has sufrido de robo de identidad?
¿Realizas check-ins o publicas la ubicación de los lugares que visitas?
¿Has compartido memes?
¿Guardas tu usuario y/o contraseña en algún papel, block de notas o habilitas el “recordarme”?
¿Has jugado con juegos en línea?
¿Has utilizado aplicaciones para conocer gente?
¿Has enviado fotos con poca o nula ropa a otra persona?
¿Has sufrido extorsión por enviar este tipo de fotos?
¿Le has dado una tableta o dispositivo a un menor de edad para que se entretenga?
¿Cuidas el contenido y los sitios que visitan los menores de edad?
¿Has recibido llamadas de instituciones financieras ofreciendo algún tipo de servicio?
Entonces... ¿Utilizas la tecnología de forma responsable?

SCT

SECRETARÍA DE COMUNICACIONES
Y TRANSPORTE

OEA
Más derechos
para más gente

Foreign &
Commonwealth
Office

KALANT'AAN
EXPERTOS EN CIBERSEGURIDAD