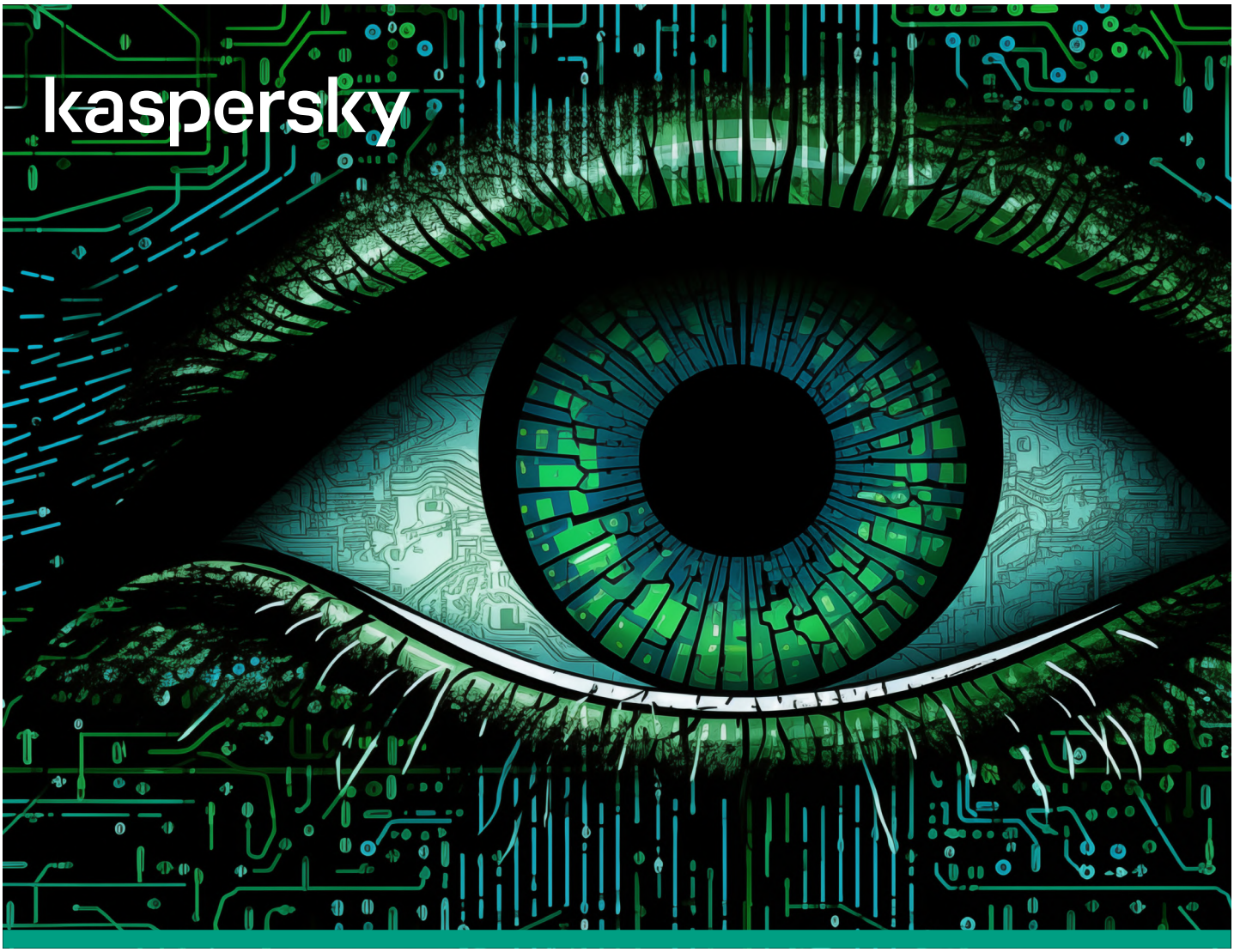
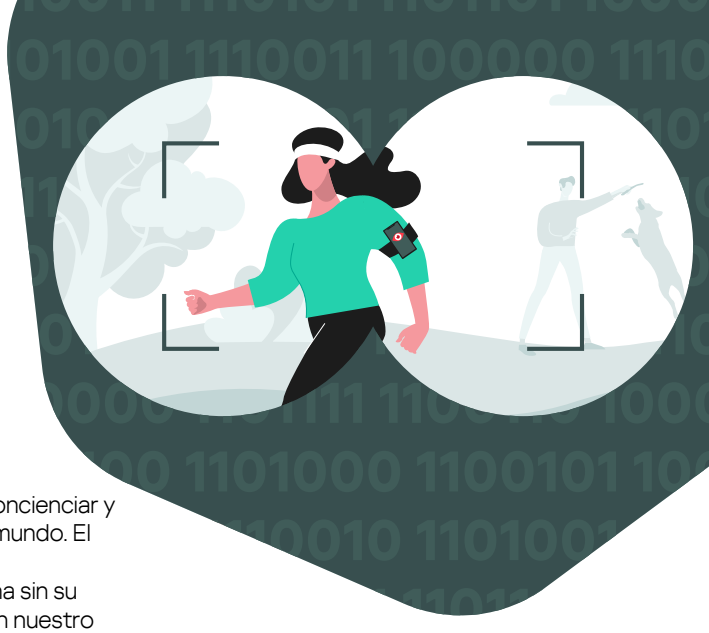


El Estado del **Stalkerware** en 2023

Kaspersky
Febrero 2024

Contents



Principales conclusiones de 2023

El informe anual Kaspersky '**El Estado del Stalkerware**' tiene como objetivo concienciar y contribuir a una mejor comprensión de los efectos del ciberacoso en todo el mundo. El stalkerware es un software comercial que puede instalarse discretamente en smartphones, permitiendo a los agresores vigilar la vida privada de una persona sin su conocimiento. El stalkerware necesita de acceso físico para instalarse, pero en nuestro informe también señalamos tecnologías en remoto que pueden utilizarse con fines maliciosos.

Fácilmente descargable e instalable por cualquier persona con conexión a Internet, el stalkerware hace posible el acceso a un smartphone desde cualquier lugar. Un delincuente no sólo puede violar la intimidad de su víctima vigilando sus actividades, sino que también puede utilizar el software para acceder a grandes volúmenes de datos personales. Dependiendo del software utilizado, se puede controlar todo, desde la ubicación del dispositivo, mensajes de texto, chats en redes sociales, fotos, historial de navegación y mucho más. Dado que el stalkerware funciona en segundo plano y sin ser visto, la mayoría de las víctimas desconocen por completo que se están controlando todos sus movimientos.

En la mayoría de los países, el uso de este software no está prohibido, pero instalar una aplicación de este tipo en el smartphone de otra persona sin su consentimiento es ilegal y está penado. Sin embargo, el responsable será el autor, no el desarrollador de la aplicación.

El stalkerware, junto con otras tecnologías, es una herramienta utilizada con frecuencia en relaciones abusivas, facilitando la ejecución de esa violencia. Dado que este fenómeno digital forma parte de un problema más amplio en el mundo real, Kaspersky está colaborando con expertos y organizaciones relevantes en el campo de la violencia de género. Esto incluye servicios de apoyo a las víctimas, programas para agresores, investigación y agencias gubernamentales. El objetivo es compartir conocimientos y brindar apoyo tanto a profesionales como a víctimas.

Datos destacados de 2023

▸ En 2023, un total de 31.031 usuarios se vieron afectados por el stalkerware, cifra superior en comparación con 2022 (29.312).

▸ Kaspersky Security Network revela que el stalkerware se utiliza con mayor frecuencia en Rusia, Brasil e India, y sigue siendo un problema global, con el mayor número de usuarios afectados en los siguientes países:

- Alemania, Francia y Reino Unido (Europa);
- Irán, Turquía y Yemen (Oriente Medio y África);
- India, Indonesia y Filipinas (Asia-Pacífico);
- Brasil, México y Colombia (América Latina);
- Estados Unidos (Norteamérica);
- Federación Rusa, Bielorrusia y Kazajistán (Europa del Este - excluidos los países de la Unión Europea-, Rusia y Asia Central).

▸ En todo el mundo, la app de stalkerware más utilizada es TrackView, con 4.049 usuarios afectados.

▸ El 23% de las personas de todo el mundo revelan haber sufrido algún tipo de acoso online por parte de alguien con quien salían recientemente.

▸ El 40% declaró haber sufrido acoso o sospechar que lo estaban sufriendo.

Stalkerware:

Software comercial utilizado para espiar. El stalkerware permite a una persona vigilar a distancia las actividades del dispositivo de otro usuario sin su consentimiento y sin notificárselo de forma explícita.

Stalking:

Un patrón de comportamiento hacia una persona en concreto que le haría dudar sobre su seguridad o la de los demás; o sufrir una gran angustia emocional. Los agresores utilizan una serie de tácticas, que incluyen (pero no se limitan a): contacto no deseado, incluyendo llamadas telefónicas, mensajes de texto y comunicación a través de las redes sociales, regalos no deseados, presentación/acercamiento a una persona o a su familia/amigos, seguimiento, vigilancia, daños a la propiedad y amenazas.

Tendencias observadas por Kaspersky en 2023

Metodología

Los datos de este informe se han extraído de estadísticas sobre amenazas obtenidas de Kaspersky Security Network, dedicada a analizar datos relacionados con la ciberseguridad procedentes de millones de participantes voluntarios y anónimos de todo el mundo. Para calcular las cifras, se ha revisado el número de las soluciones de seguridad móvil de Kaspersky de acuerdo con los criterios de detección de stalkerware de la **Coalición contra el Stalkerware**. Esto significa que el número de usuarios afectados ha sido atacado únicamente por stalkerware. Otro tipo de aplicaciones de vigilancia o espionaje que quedan fuera del alcance de la Coalición no se incluyen en las estadísticas del informe.

Las estadísticas reflejan los usuarios de móviles afectados por stalkerware, que es diferente del número total de detecciones. El número de detecciones puede ser mayor, ya que el stalkerware puede haber sido detectado varias veces en el mismo dispositivo del mismo usuario si éste no eliminó la aplicación al recibir una notificación. A menudo, las organizaciones de apoyo aconsejan a los afectados que no eliminen el stalkerware para no alertar al agresor de que ha sido descubierto.

Por último, las estadísticas reflejan únicamente los usuarios móviles que utilizan las soluciones de seguridad informática de Kaspersky. Algunos pueden utilizar otra solución de ciberseguridad en sus dispositivos o no utilizar ninguna.

> En 2023, un total de **31.031** usuarios únicos se vieron afectados por stalkerware

Cifras globales de detección: usuarios afectados

Utilizando estadísticas globales y regionales, Kaspersky ha podido comparar los datos recopilados en 2023 y en los cuatro años anteriores. En 2023, un total de 31.031 usuarios se vieron afectados por el stalkerware, un aumento en comparación con 2022 (29.312 usuarios únicos). El gráfico 1, a continuación, muestra cómo ha variado esta cifra año tras año desde 2018.

Año	Usuarios Afectados
2018	40.173
2019	66.927
2020	53.870
2021	32.694
2022	29.312
2023	31.031

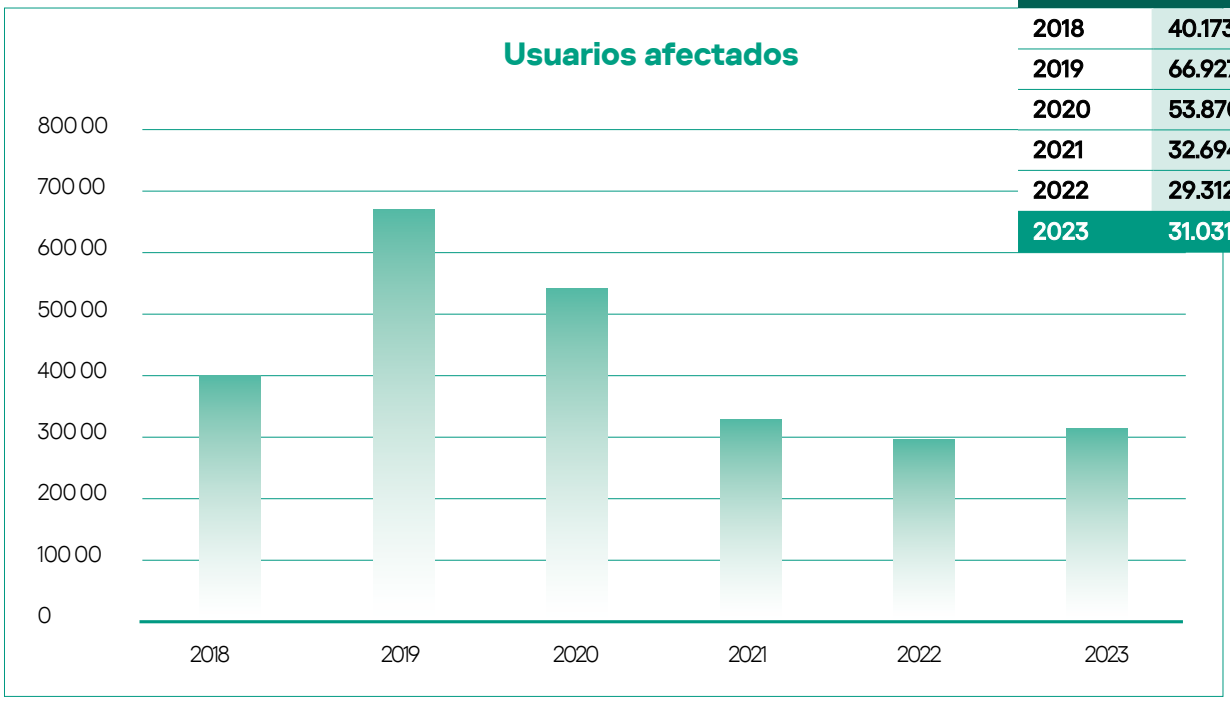


Gráfico 1: **Evolución de los usuarios afectados desde 2018**

Cifras de detección mundiales y regionales: geografía de los usuarios afectados

> En 2023, Kaspersky detectó usuarios afectados en 175 países

El stalkerware sigue siendo un problema global. En 2023, Kaspersky detectó usuarios afectados en 175 países.

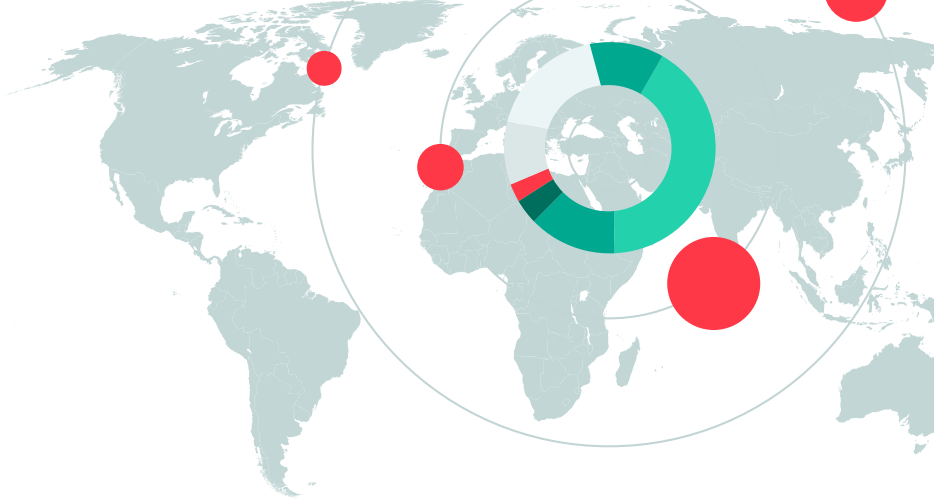
En 2023, Rusia (9.890), Brasil (4.186) e India (2.492) fueron los tres primeros países con más afectados. Según las estadísticas de Kaspersky, esos tres países han mantenido las posiciones de liderazgo desde 2019, todos con un aumento de las infecciones de stalkerware detectadas. Irán entró en el top cinco de los más afectados el año pasado y se mantiene en la misma posición.

Cuando se compara con 2021, hay ligeros cambios en los 10 países más afectados, con la mayoría de ellos manteniéndose en la misma posición. Mientras que Alemania descendió del puesto siete al diez, Arabia Saudí (que ocupaba el octavo lugar en 2022) no figura este año en la lista de países más afectados.

	País	Usuarios afectados
1	Federación Rusa	9.890
2	Brasil	4.186
3	India	2.492
4	Irán	1.578
5	Turquía	1.063
6	Indonesia	871
7	Estados Unidos de América	799
8	Yemen	624
9	México	592
10	Alemania	577

Tabla 1: **Top 10 de los países más afectados por el stalkerware en 2023**

En Oriente Medio y África, el número de usuarios afectados fue de **6.561**



	País	Usuarios afectados
1	Alemania	577
2	Francia	332
3	Reino Unido	271
4	España	257
5	Italia	252
6	Polonia	179
7	Países Bajos	177
8	Suiza	116
9	Austria	70
10	Portugal	63

Tabla 2 - **Top 10 de los países más afectados en Europa en 2023**

El número total de usuarios únicos afectados en Europa en 2023 fue de 2.645, lo que supone un descenso significativo en comparación con 2022 (3.158). Los tres países más afectados en Europa fueron Alemania (577), Francia (332) y el Reino Unido (271). España se situó en la cuarta posición. En comparación con 2021, los países de la lista siguieron figurando como los más afectados de Europa, con la excepción de Grecia, que abandonó la lista. Desafortunadamente, Portugal entró en la lista en décimo lugar.

	País	Usuarios afectados
1	Federación Rusa	9.890
2	Bielorrusia	307
3	Kazajistán	270
4	Ucrania	268
5	Azerbaiyán	243
6	Uzbekistán	100
7	Kirguistán	52
8	Moldavia	49
9	Armenia	43
10	Tayikistán	30

Tabla 3 - **Top 10 de los países más afectados en Europa del Este (excluidos los países de la UE), Rusia y Asia Central en 2023.**

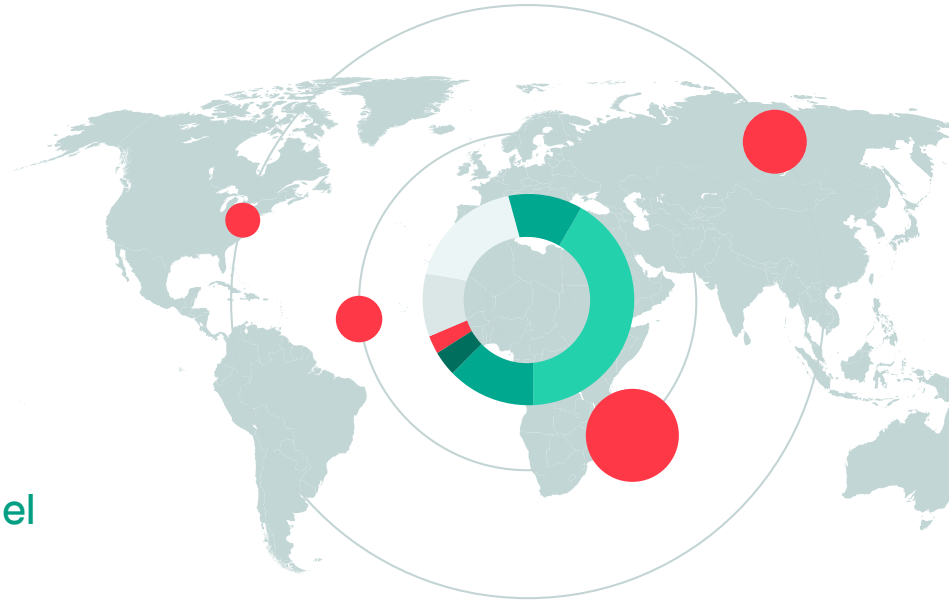
En Europa del Este (excluidos los países de la Unión Europea), la Federación Rusa y Asia Central, el número total de usuarios afectados en 2023 fue de 11.210, más que el año anterior (9.406). Los tres primeros países fueron Rusia, Kazajistán y Bielorrusia.

	País	Usuarios afectados
1	Irán	1.578
2	Turquía	1.063
3	Yemen	624
4	Egipto	569
5	Arabia Saudí	511
6	Algeria	495
7	Marruecos	215
8	Emiratos Árabes Unidos	184
9	Iraq	127
10	Sudáfrica	126

Table 4 - **Top 10 de los países más afectados en Oriente Medio y África en 2023.**

Si nos fijamos en la región de Oriente Medio y África, el número total de usuarios afectados fue de 6.561, ligeramente superior al de 2022 (6.330), pero hay un pequeño cambio en los tres países más afectados este año. Mientras que en 2022 Irán, Turquía y Arabia Saudí fueron los países más afectados, en 2023 fueron Irán, Turquía y Yemen.

Con **2.492** usuarios afectados, India sigue muy por delante de los demás países de la zona



Con **4.186** usuarios afectados, Brasil lidera la región de América Latina y el Caribe

	País	Usuarios afectados
1	India	2,492
2	Indonesia	871
3	Filipinas	323
4	Australia	168
5	Vietnam	97
6	Malasia	88
7	Japón	85
8	Bangladesh	66
9	Hong Kong	51
10	Sri Lanka	51

Table 5 - **Top 10 de los países más afectados en la región de Asia-Pacífico en 2023.**

La región de Asia-Pacífico registró un aumento del uso de programas espía en comparación con el año pasado, con un total de 4.575 usuarios afectados, frente a los 3.187 de 2022. India se mantiene muy por delante de otros países de la región, con 2.492 afectados. Indonesia ocupa el segundo lugar con 871; Filipinas es tercero con 323 y Australia cuarto.

	País	Usuarios afectados
1	Brasil	4,186
2	México	592
3	Colombia	149
4	Perú	138
5	Argentina	95
6	Ecuador	88
7	Chile	63
8	Venezuela	19
9	Bolivia	18
10	Paraguay	17

Tabla 6 - **Top 10 de países afectados en América Latina en 2023.**

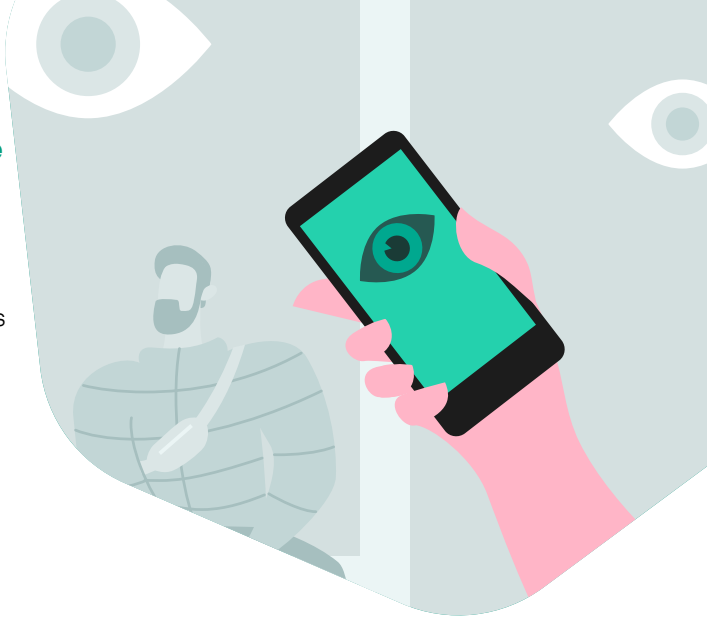
Brasil domina la región de América Latina y el Caribe con 4.186 usuarios afectados, lo que representa aproximadamente el 76% del número total. Le siguen en la lista México y Colombia. Se registraron un total de 5.478 usuarios afectados, lo que supone un pequeño descenso en comparación con 2022 (6.170).

	País	Usuarios afectados
1	Estados Unidos de América	799
2	Canadá	250

Tabla 7 - **Usuarios afectados en Norteamérica en 2023.**

Por último, en Norteamérica, el 77% de todos los usuarios afectados se encontraban en Estados Unidos. Esto era de esperar dado el tamaño relativo de la población en comparación con Canadá. En toda la región norteamericana, 1.049 usuarios se vieron afectados en total.

Cifras globales de detección - aplicaciones de Stalkerware



Este año, Kaspersky detectó **195 aplicaciones de stalkerware diferentes**. La aplicación de stalkerware más utilizada para controlar smartphones en todo el mundo en 2023 fue TrackView, que afectó a 4.049 usuarios.

Los programas de Stalkerware suelen hacerse pasar por aplicaciones legítimas antirrobo o de control parental en smartphones, tabletas y ordenadores, pero en realidad son muy diferentes. Al instalarse, sin consentimiento y conocimiento de la persona rastreada, proporcionan al agresor los medios para controlar la vida de la víctima. Por lo general, este tipo de aplicaciones no se muestran en la lista de aplicaciones instaladas en la configuración del teléfono, lo que dificulta su detección.

	Nombre de la aplicación	Usuarios afectados
1	**TrackView**	**4.049**
2	**Reptilic**	**3.089**
3	**SpyPhone**	**2.126**
4	**MobileTracker**	**2.099**
5	**Cerberus**	**1.816**
6	**Wspy**	**1.254**
7	**Unisafe**	**981**
8	**Mspy**	**899**
9	**MonitorMinor**	**863**
10	**KeyLog**	**852**

Tabla 8: **Top 10 de las aplicaciones de stalkerware en 2023.**

> Los programas de vigilancia suelen hacerse pasar por aplicaciones legítimas antirrobo o de control parental

A continuación, se enumeran algunas de las funciones más comunes presentes en las aplicaciones de stalkerware:

- Icono de la app oculto
- Leer SMS, MMS y registros de llamadas
- Acceso a la lista de contactos
- Seguimiento de la ubicación GPS
- Seguimiento de eventos del calendario
- Leer mensajes de servicios de mensajería y redes sociales somo Facebook, WhatsApp, Signal, Telegram, Viber, Instagram, Skype, Hangouts, Line, Kik, WeChat, Tinder, IMO, Gmail, Tango, SnapChat, Hike, TikTok, Kwai, Badoo, BBM, TextMe, Tumblr, Weico, Reddit etc.
- Ver fotos e imágenes de las galerías del teléfono
- Hacer capturas de pantalla
- Hacer fotos con la cámara frontal (modo selfie)

¿Afectan por igual el stalkerware a los dispositivos iOS y Android?

Las aplicaciones de stalkerware son mucho menos frecuentes en iPhones que en dispositivos Android, porque iOS es un sistema cerrado. Además, aunque los ciberdelincuentes pueden eludir las restricciones de los iPhones con software libre, siguen necesitando acceso físico directo al teléfono para instalar el programa de vigilancia. No obstante, los usuarios de iPhone que teman ser vigilados deben mantener siempre controlado su dispositivo.

Otra posibilidad es que el agresor ofrezca a su víctima un iPhone -o cualquier otro dispositivo- con el stalkerware preinstalado. Hay muchas empresas que ofrecen estos servicios en Internet, lo que permite a los agresores instalar estas herramientas en teléfonos nuevos y entregarlos en un embalaje de fábrica bajo la apariencia de un regalo a la víctima.

Acoso digital, confianza y citas

El stalkerware y el acoso digital están relacionados, pero no son excluyentes. En los últimos años se ha observado un aumento del uso de tecnologías y aplicaciones legítimas con fines ilegítimos o maliciosos para rastrear y vigilar a otras personas. Para profundizar en el tema del ciberacoso, Kaspersky encargó a Arlington Research la realización de 21.000 entrevistas online para obtener información sobre el stalking digital y el stalkerware en todo el mundo. Se interrogó a 1.000 personas en cada uno de los siguientes países: Reino Unido, Alemania, España, Serbia, Portugal, Países Bajos, Italia, Francia y Grecia, Estados Unidos, Brasil, Argentina, Chile, Perú, Colombia, México, China, Singapur, Rusia, India y Malasia. Los encuestados tenían 16 años o más y mantenían una relación duradera (62%), salían con alguien (16%) o no salían actualmente ni mantenían una relación, pero lo habían hecho recientemente (21%). Las entrevistas tuvieron lugar entre el 3 y el 17 de enero de 2024.

Al **7%** se le ha instalado stalkerware en sus dispositivos sin su consentimiento

Perspectiva general sobre el acoso y ser acosado

Xy ww, qr y|¡ r{p£r¡¢nq|¡ r¤ryn |{unor ¡£s vq| nytŹ{ ¢v}|qr np|¡| |{w{r}| }n ¢r qr £{n }r ¡|{np|{yn ~£r unoln{ ¡nwq| rpvr{¢r z r{¢r# X¡ }|¡voyr ~£r r¡¢n¡ }r ¡|{n¡ p|{yn¡ ~£r ¡nyr |{un§n{ £¢ww¨nq|yn v{s| znpvŠ{ qv¡}|{voyr }Źowpn z r{¢r r{yn¡ n}wpnpv|{r¡ qr pv¢n¡ }n n np|¡n # Xy non{vp| qr nt r¡v|{r¡ r¡ ¤n vnq|¼ zĝ¡ qr £{ ¢r pv| ?¤r, @qr y|¡ r{p£r¡¢nq|¡ qrpyn n |{unor ¡£s vq| ¤y|yr{pvn | zny|¡¢ n¢|¡}| }n ¢r qr ¡£ }n rwn np¢£ny | n{¢r v| # X{ }n ¢vp£yn % ryłh, un rpvovq|p| r|¡ ryrp¢ Š{vp|¡| zr{¡nwr¡ {| qr¡rnq|¡§¼y| ~£r r¡ zĝ¡ v{~£vr¢n{¢r% ryłq, un¡vq| t nonq| | s|¢| t nsvnq| ¡v{ ¡£p|{¡r{¢vzvr{¢|# Tqr zĝ¡% ryłls, rp|{|pvŠ ~£r ¡r unoln n¡¢ rnq| ¡£ £ovpnpvŠ{% ryłls, un r¦}r vzr{¢nq| nppr¡| {| n£¢| v¨nq| n¡£¡ p£r{¢n¡ qr rqr¡ ¡|pwnyr¡ | p| r|¡ ryrp¢ Š{vp|¡§¼y| ~£r r¡ nyn zn{¢r% nyh, ¡r yr un v{¡¢nynq| £{ } |t nzn qr np|¡| ?¡¢nyxr ¥n r@r{ ¡£¡ qv¡}|¡v¢v¤|¡ ¡v{ ¡£p|{|pvzvr{¢|

_n qr¡vt£nyqnq qr t¡{r | r{ r¡¢n¡ ¡v¢£npv|{r¡ r¡ r¤vqr{¢r%§n ~£r £{ zn§| }| pr{¢nwr qr z£wr r¡ r{p£r¡¢nqn¡ ?yw, @nsv zn{unor ¡£s vq| ¤v|yr{pvn | no£¡| r{ p|z}n npvŠ{p|{y|¡u|zo r¡ ?¤h, @# Aquellos que tienen relaciones más esporádicas declaran haber experimentado más casos de violencia o abuso que los que tienen relaciones a largo plazo (48% frente a 37%).

h{ ¡vt{vsvpn¢v¤|¤y, qr y|¡ r{p£r¡¢nq|¡ z£r¡¢ n{ } r|p£}npvŠ{ }| ry np|¡| |{w{r% ¡vr{q|yw tr nzr{¢r zĝ¡ ny¢nyn } r|p£}npvŠ{ r{¢ r z£wr r¡ ?¤h, @~£r r{¢ r u|zo r¡ ?¤ł, @# X¡¢n ¡v¢£npvŠ{ ¡r r¦¢vr{qr n {v¤ry ty|onv% p|{£{ zn§| {Źzr | qr pn¡|¡qr np|¡| |{w{r r{ }n ¢r¡qr f£qnz¡ vpn% Vr{¢ |nz¡ vpn§T¡vn# c| rwrz}y|% ry yq w, qr y|¡ r{p£r¡¢nq|¡r{\{qvn% ry¤j, r{ `¡¦vp|§ ry¤h, r{T tr{¢v{n nqzv¢r{unor r¦}r vzr{¢nq| nytŹ{¢v}|qr np|¡| |{w{r#

Tqr zĝ¡% ry yls, qrpyn Š~£r unoln ¡£s vq| np|¡| |¡|¡}rpunon~£r y| r¡¢non ¡£s vr{q|% §|¢ | łq, qw| ~£r {| rp| qnon | {| r¡¢non ¡rt£ | qr ~£r ¡r u£ovr n{} |q£pvq| ¢nyr¡ v{pvqr{¢r¡# `r{|¡qr yn z v¢nq ?y h, @qrpyn n |{~£r {£{pn unoln{¡£s vq| np|¡| {v ¡|¡}rpunon{~£r r¡¢| yr¡u£ovr n |p£ vq|# X{p|z}n npvŠ{p|{ wlswł £{ {Źzr |

menor de encuestados confirmaron haber sufrido acoso a través de la tecnología (24%); mientras que en 2024 un 14% aseguraba no ser capaz de recordar/decir si había sido víctima de este tipo de acoso. Las variaciones regionales muestran mayores incidentes/sospechas en Singapur (69%), India (63%), Malasia (54%), México (53%), Perú (52%) y China (50%); mientras que Portugal (21%), Reino Unido, España e Italia (27%) informaron de tasas más bajas.

Entre los que declararon haber sufrido incidentes/sospechas, el acoso a través de una aplicación de teléfono fue el más frecuente (20%), seguido de una aplicación de ordenador portátil (10%) y el acceso a través de la webcam (10%). Mientras que la mayoría (78%) nunca se había visto presionada por su pareja para instalar aplicaciones de vigilancia o establecer parámetros en sus teléfonos, el 13% declaró que su pareja había instalado o establecido parámetros (similar al 14% en 2021), y el 10% se sintió presionada para instalar una aplicación de vigilancia (15% en 2021). Es significativo que, en la India, el 34 % declaró que su pareja instaló o estableció parámetros y el 29 % se sintió presionado para instalar aplicaciones de control.

Un dato preocupante es que el 12% de los encuestados admitió haber instalado o configurado parámetros en el teléfono de su pareja, mientras que el 9% reconoció haber presionado a su pareja para que instalara aplicaciones de vigilancia. En la India, un tercio lo hizo, y el 26% presionó a su pareja para que instalara aplicaciones de vigilancia.

El conocimiento del stalkerware varía: el 46% no lo conoce, el 17% no está seguro y sólo el 37% está seguro de saber qué es el stalkerware. Entre los que estaban seguros, menos del 10% podía identificar todas sus posibilidades de vigilancia. Ahora, estamos más concienciados ya que en 2021, el 60% no sabía lo que era el stalkerware y el 19% no estaba seguro. En 2024, si los encuestados encontraran stalkerware en sus dispositivos, el 38% intentaría identificar al responsable de la instalación y hablar con él, el 34% intentaría eliminarlo, el 20% dejaría de utilizar el dispositivo y el 24% recurriría a la policía. Esto supone un cambio con respecto a 2021, cuando el 50% intentaría identificar al autor de la infección y el 20% acudiría a la policía.

Perspectivas cambiantes sobre el acoso en las relaciones actuales: privacidad, consentimiento y realidad del acoso

La mayoría de las personas (54%) no apoya la idea de vigilar a su pareja sin su conocimiento. En este sentido, cabe destacar que las personas de mayor edad, como la Generación X, los Baby Boomers y la Generación Silenciosa, están más en contra de la vigilancia sin consentimiento que los más jóvenes. En comparación, entre 2021 y 2024, se ha producido un notable descenso en el número de personas que afirman que es inaceptable vigilar a una pareja sin su conocimiento, pasando del 70% al 54%. Curiosamente, los que opinan que es aceptable también disminuyeron, del 13% en 2021 al 8% en 2024. La postura respecto a este tema es clara, ya que en 2024 el 38% considera aceptable la vigilancia sin consentimiento en ciertas circunstancias, lo cual representa un aumento significativo desde el 17% registrado en 2021.

Al examinar las actitudes hacia la supervisión consentida online de la pareja (compartir información con pleno conocimiento y consentimiento para un fin como la seguridad), el 45% de los encuestados creen que no es aceptable, haciendo hincapié en la importancia del derecho a la intimidad. Mientras que un 27% defiende la transparencia total en las relaciones, considerando apropiada la supervisión consentida, y el 12% la considera aceptable sólo cuando es mutua.

Además, el 12% está de acuerdo con este tipo de vigilancia cuando afecta a la seguridad física, mientras que el 4% lo hace a regañadientes debido a la insistencia de su pareja. Mientras que las opiniones de este año respecto a la supervisión consentida coinciden estrechamente con las de 2021, un porcentaje ligeramente superior está abierto a la idea en 2024 (27%, frente al 25% en 2021). Sin embargo, estas acciones siguen siendo inaceptables para la mayoría (45%), lo que refuerza la convicción de la privacidad como un derecho fundamental en las relaciones.

Aunque la mayoría tiene una opinión clara sobre la vigilancia, el acoso es un tema muy importante en el mundo de las citas. Un 34% considera aceptable buscar en Google o revisar las redes sociales de alguien con quien está saliendo, como una forma de precaución. Además, menos de una cuarta parte (23%) ha sufrido algún tipo de acoso online por parte de alguien con quien ha tenido contacto reciente, lo que destaca la relevancia de este problema en el actual mundo de las citas.

Navegando entre la confianza y los límites: análisis de los problemas de privacidad digital

Casi la mitad de los encuestados (47%) expresan preocupaciones sobre que sus parejas violen su privacidad digital, lo que significa un aumento notable desde 2021 cuando se registró un 37%. Este miedo es más pronunciado en Europa, donde el 62% comparte estas preocupaciones, en contraste con un porcentaje más bajo en la región de Asia-Pacífico (37%). En todas las regiones, las fuentes comunes de preocupación incluyen la monitorización de mensajes de texto (20%) y las parejas que buscan tener acceso total a sus teléfonos, tanto física como remotamente (20%). Más encuestados ahora se preocupan por que sus parejas violen su privacidad al eliminar contraseñas de sus dispositivos (13% en 2024 en comparación con el 9% en 2021) o al solicitar constantemente compartir la geolocalización (12% en 2024 en comparación con el 10% en 2021). Sin embargo, un porcentaje ligeramente menor (15% en 2024 en comparación con el 17% en 2021) se preocupa por que sus parejas invadan su privacidad al leer sus correos electrónicos.

En cuanto a la confianza y el acceso a dispositivos personales, el 51% expresa confianza en sus parejas concediéndoles acceso total a sus teléfonos. Otro 19% permite el acceso, pero con aplicaciones protegidas por contraseñas o medidas de seguridad. Una quinta parte, aunque confiando en sus parejas, opta por no proporcionar acceso. El resto están divididos, con un 5% que no dan acceso y un 4% que elige no responder. Las personas en relaciones temporales muestran más reticencias, con un 40% que acepta otorgar acceso total en comparación con el 61% entre aquellos en relaciones a largo plazo.

Por otro lado, un 52% aseguró tener acceso total al teléfono de sus parejas. Un 23% tiene acceso, pero no total, ya que hay aplicaciones que su pareja protege con contraseñas u otras medidas de seguridad. Por su parte, un 18% dijo no haber recibido acceso al teléfono de sus parejas y un 7% prefirió no revelar esta información. Estas dinámicas destacan la compleja relación entre la confianza y los límites digitales dentro de las relaciones románticas.

Perspectivas sobre el complejo panorama del intercambio de información en las relaciones de pareja

Mientras que una mayoría de los encuestados, más del 90%, se muestra dispuesto o considerar la posibilidad de compartir las contraseñas de servicios de streaming como Netflix y sus fotos, se observa un enfoque más prudente cuando se trata de información más sensible. Curiosamente, los encuestados muestran mayor reticencia a compartir las contraseñas de los dispositivos, ya que un 18% sostiene que nunca compartiría el acceso a los mismos

> Es positivo observar un aumento de la prudencia, especialmente respecto a datos sensibles como contraseñas

Más en detalle, los datos revelan muchos matices sobre el tipo de información que se comparte. Así, el 69% está dispuesto a compartir contraseñas de streaming y sólo el 9% afirma que nunca lo haría. Del mismo modo, en el caso de las fotos, el 66% está dispuesto a compartirlas, el 26% podría planteárselo y el 8% se resiste a la idea. En aspectos más personales, como los mensajes de texto, el 52% se declara dispuesto a compartirlos, mientras que el 33 % podría considerarlo, pero el 15 % nunca mostraría estos datos.

Esta tendencia también se observa en el caso de las contraseñas de dispositivos de seguridad, como los videoporteros con Bluetooth. Aquí, el 52% está dispuesto a compartir dichas contraseñas, mientras que el 30% podría planteárselo y el 18% no las revelaría. Cuando se trata de información de pago, el 49% se muestra dispuesto a compartirlas, un 30 % algo dispuesto y un 21 % no la compartiría.

A medida que aumenta la importancia de la información, disminuye la disposición a facilitarla, como demuestran los porcentajes, cada vez menores, de personas dispuestas a revelar contraseñas de determinadas cuentas (47% dispuestas, 29% podrían considerarlo y 24% no están dispuestas) y el historial del navegador (46% dispuestas, 34% podrían considerarlo y 20% no están dispuestas). Este difícil equilibrio entre transparencia y el intercambio de información en la relaciones.

David Emm, experto en seguridad y privacidad . Kaspersky

Estos resultados ponen de manifiesto el delicado equilibrio entre la intimidad y la protección de la información personal. Es positivo notar una mayor prudencia, especialmente en lo que respecta a datos sensibles. La reticencia a compartir este tipo de accesos está en línea con los principios de la ciberseguridad. La disposición a compartir contraseñas de streaming y fotos supone un cambio de mentalidad, aunque las personas deben reconocer los riesgos potenciales incluso en el intercambio de información aparentemente inofensiva. Estas ideas subrayan la importancia de fomentar la comunicación abierta en las relaciones, establecer límites claros y promover la educación digital. Para los profesionales de la seguridad, refuerza la necesidad de una formación continua sobre las mejores prácticas de ciberseguridad y de capacitar a las personas para tomar decisiones con conocimiento de causa a la hora de compartir información personal en las relaciones".

Emma Pickering, Head of Technology-Facilitated Abuse and Economic Empowerment Team en Refuge

> Lamentablemente, hay que reconocer que muchos supervivientes no han tenido la opción de crear sus contraseñas o de no compartirlas

Los datos de este informe son realmente preocupantes, pero siguen sin sorprendernos. En Refuge estamos observando un aumento alarmante del número de víctimas que denuncian problemas relacionados con stalkerware. Como revelan estas estadísticas, el problema del stalkerware es una preocupación generalizada.

Es probable que esto se deba al aumento de las funcionalidades de stalkerware en las aplicaciones de control parental, que hacen que la posibilidad de acosar sea cada vez más accesible. Mientras estamos buscando activamente stalkerware destinado a vigilar a su expareja, hay muchas otras formas de stalkerware disponibles que están dirigidas a un público que descarga las aplicaciones sin entender todas las características, o para ser utilizadas por otras razones maliciosas.

También es muy importante tener en cuenta que rara vez vemos que una forma de abuso tecnológico se utilice de forma aislada. Además de los programas de vigilancia, los agresores suelen utilizar otras formas de tecnología para hacer daño. Por eso debemos asegurarnos siempre, como organización, de completar una evaluación tecnológica detallada y ayudar a las víctimas a recuperar el acceso a todas las cuentas y dispositivos. Por esta razón es imprescindible que sigamos trabajando junto con la comunidad tecnológica en general, para entender la tecnología que se utiliza, para tratar de evitar que se utilice para hacer daño y para tratar de construir en colaboración la seguridad mediante el diseño.

Lamentablemente, reconocemos que muchos de los afectados no pueden permitirse el lujo de poner contraseñas en los dispositivos o de no compartir el dispositivo o la contraseña. Si alguien está preocupado, le aconsejamos que utilice siempre un dispositivo seguro para ponerse en contacto con una agencia de apoyo y que, en el caso de conversaciones, correos electrónicos o búsquedas delicadas, no las realice en el dispositivo que crea que pueda estar siendo vigilado.

El consentimiento es un acuerdo libre de cualquier tipo de coacción

Erica Olsen, Senior Director, Safety Net Project, National Network to End Domestic Violence (NNEDV)

Este informe pone de manifiesto tanto la frecuencia de las conductas de acoso perpetradas con tecnología como las ideas relacionadas con la privacidad en las relaciones de pareja. El uso de stalkerware o de cualquier herramienta para vigilar a otra persona sin su consentimiento es una violación de la intimidad y una táctica habitual de abuso. Este informe demuestra cómo los agresores utilizan una amplia gama de técnicas de vigilancia, que incluyen tanto stalkerware como otras aplicaciones que facilitan el intercambio de información personal.

El informe también explora las normas y perspectivas sobre la privacidad en las relaciones de pareja. Una parte significativa de los encuestados declaró que compartiría voluntariamente cierta información, ya fuera por razones de seguridad o de otro tipo. Un pequeño porcentaje, el 4%, declaró que accedía a regañadientes a la vigilancia ante la insistencia de su pareja, lo que no es lo mismo que consentimiento. Es importante establecer una distinción clara entre compartir información de forma consentida y vigilar de forma no consentida. El consentimiento es un acuerdo libre de fuerza o coacción.

Combatiendo el stalkerware juntos

El stalkerware no es solo un problema tecnológico, sino la manifestación de un problema social que requiere la intervención de todos los sectores de la sociedad. Kaspersky no solo se compromete activamente a proteger a los usuarios de esta amenaza, sino también a mantener un diálogo multinivel con organizaciones sin ánimo de lucro y organismos de la industria, de investigación y públicos de todo el mundo para trabajar juntos en soluciones que atajen el problema.
En 2019, Kaspersky fue la primera empresa de ciberseguridad del sector en desarrollar una nueva alerta que llama la atención y que notifica a los usuarios si se detecta stalkerware en su dispositivo de forma clara. Mientras que las soluciones de Kaspersky han estado señalando aplicaciones potencialmente dañinas que no son malware -incluido el stalkerware- durante muchos años, la nueva función de notificaciones alerta al usuario del hecho de que se ha encontrado una aplicación en su dispositivo que puede ser capaz de espiarlo.

En 2022, como parte del lanzamiento de sus nuevos productos, Kaspersky amplió los servicios de la Alerta de Privacidad, informando ahora al usuario de la presencia de stalkerware en el dispositivo. También le advierte de que, si se elimina el stalkerware, se notificará a la persona que lo instaló, lo cual podría empeorar la situación. Además, el usuario se arriesga a borrar datos o pruebas importantes que podrían utilizarse en un proceso judicial. La imagen 2 que se presenta a continuación muestra la nueva advertencia en un cuadro azul. La Alerta de Privacidad de Kaspersky está incluida en todas las soluciones de seguridad para usuario final para proteger a los usuarios contra el stalkerware.

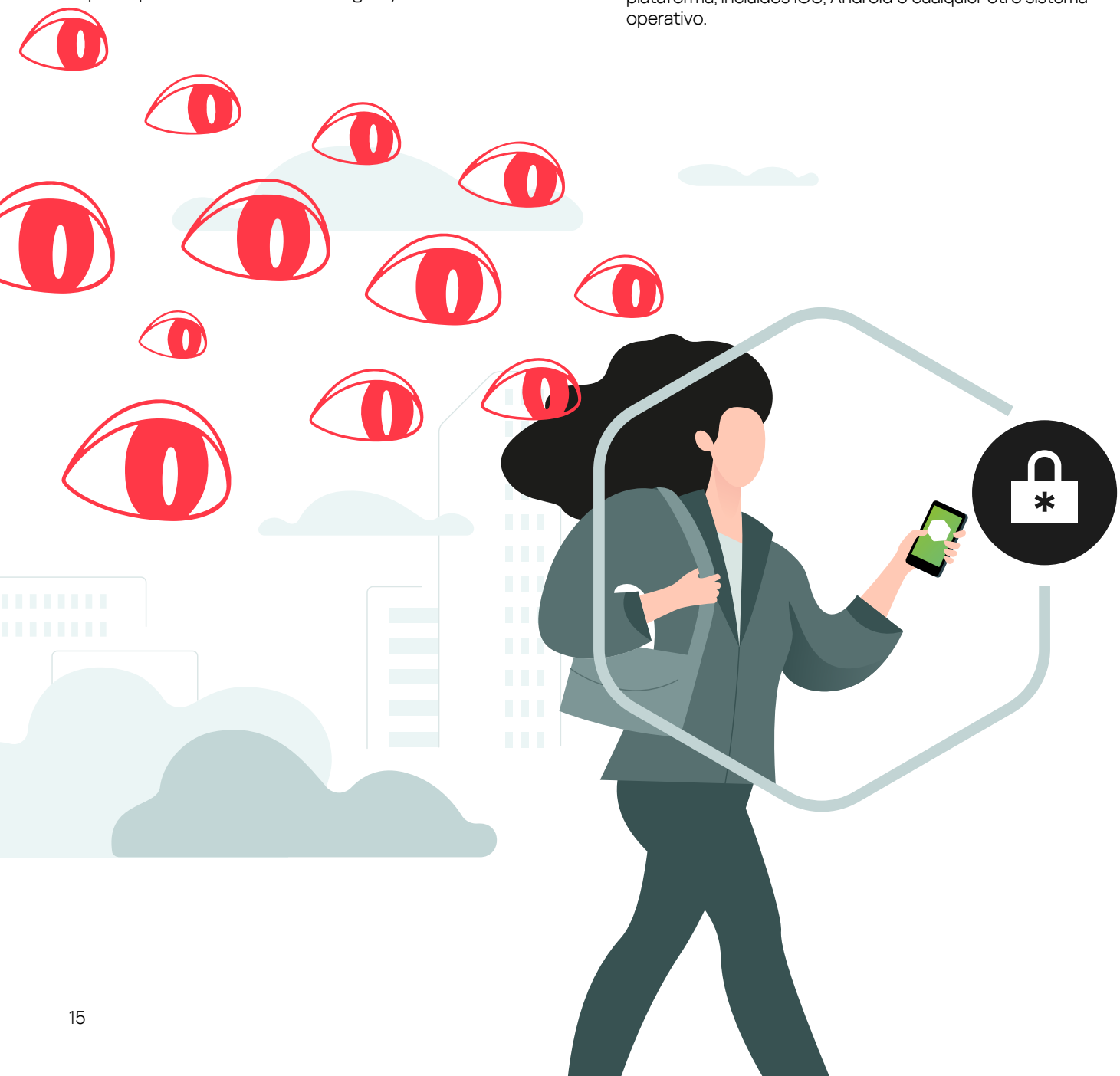
Imagen 2 – Alerta de Privacidad de Kaspersky

En 2019, Kaspersky también cofundó la Coalición contra el Stalkerware, un grupo de trabajo internacional contra el stalkerware y la violencia de género que reúne a empresas privadas de TI, ONGs, instituciones de investigación y agentes de la ley que trabajan para combatir el acoso online y ayudar a las víctimas de abuso. A través de un consorcio de más de 40 organizaciones, las partes interesadas pueden compartir conocimientos y colaborar para resolver el problema de la ciberviolencia. Además, la web de la Coalición, disponible en siete idiomas diferentes, ofrece a las víctimas ayuda y orientación en caso de que sospechen la presencia de programas de acoso en sus dispositivos.

De 2021 a 2023, Kaspersky fue socio del consorcio del proyecto DeStalk de la UE, cofinanciado por el Programa de Derechos, Igualdad y Ciudadanía de la Unión Europea. Los cinco socios del proyecto combinaron la experiencia de la comunidad de seguridad informática, la investigación y las organizaciones de la sociedad civil y las autoridades públicas. Como resultado, el proyecto DeStalk formó a un total de 375 profesionales que trabajan directamente en servicios de apoyo a la mujer y programas para agresores, y a funcionarios de las autoridades públicas sobre cómo abordar eficazmente el stalkerware y otras formas digitales de violencia de género, además de sensibilizar a la opinión pública sobre la violencia digital y el stalkerware.

Como parte del proyecto, Kaspersky desarrolló un curso de aprendizaje online sobre ciberviolencia y stalkerware dentro de su Kaspersky Automated Security Awareness Platform, una microplataforma de formación online gratuita a la que se puede acceder en cinco idiomas diferentes. Hasta la fecha, más de 130 profesionales han completado el curso y otros 80 participan actualmente en él. Aunque el proyecto DeStalk ha finalizado, el curso sigue disponible en la web del proyecto DeStalk: https://www.work-with-perpetrators.eu/destalk.

En junio de 2022, Kaspersky lanzó una web dedicada a TinyCheck para difundir más información sobre la herramienta. TinyCheck es una herramienta gratuita, segura y de código abierto que pueden utilizar organizaciones sin ánimo de lucro y unidades policiales para ayudar a apoyar a las víctimas de acoso digital. En 2020, la herramienta se creó para comprobar los dispositivos en busca de stalkerware y aplicaciones de vigilancia sin que el agresor sea consciente de la comprobación. No requiere instalación en el dispositivo del usuario porque funciona de forma independiente para evitar ser detectada por un agresor. TinyCheck escanea el tráfico saliente de un dispositivo utilizando una conexión Wi-Fi normal e identifica las interacciones con fuentes conocidas, como servidores relacionados con stalkerware. TinyCheck también puede utilizarse para comprobar cualquier dispositivo en cualquier plataforma, incluidos iOS, Android o cualquier otro sistema operativo.



¿Crees que eres víctima de stalkerware? Aquí tienes algunos consejos

Tanto si eres víctima de stalkerware como si no, estos consejos pueden ayudarte a protegerte mejor:

- Protege tu teléfono con una contraseña segura que nunca compartas con tu pareja, amigos o compañeros.
- Cambia las contraseñas de todas tus cuentas periódicamente y no las compartas con nadie.
- Descarga solo aplicaciones de fuentes oficiales, como Google Play o Apple App Store.
- Instala en los dispositivos una solución de seguridad de confianza, como Kaspersky, y examínalos con regularidad. Sin embargo, si el stalkerware ya se ha instalado, la solución solo debe instalarse una vez que se haya evaluado el riesgo para la víctima, ya que el agresor puede darse cuenta del uso de la ciberseguridad.

Las víctimas de stalkerware podrían sufrir un abuso mayor, incluido el físico.

En algunos casos, el agresor recibe una notificación si su víctima realiza un examen del dispositivo o elimina una aplicación de stalkerware. Si esto ocurre, puede llevar a un agravamiento de la situación y a nuevas agresiones. Por eso es importante proceder con cautela si crees que estás en el punto de mira de un stalkerware.

- **Acude a una organización de apoyo:** para encontrar una cerca de ti, consulta la web de la **Coalición contra el Stalkerware**.
- **Presta atención a las siguientes señales de alerta:** pueden ser que la batería se agote rápidamente debido a aplicaciones desconocidas o sospechosas, y aplicaciones recién instaladas con acceso sospechoso para utilizar y rastrear tu ubicación, enviar o recibir mensajes de texto y otras actividades personales. Comprueba también si el ajuste "Orígenes desconocidos" está activado, puede ser una señal de que se ha instalado software no deseado procedente de terceros. Sin embargo, los indicadores anteriores son circunstanciales y no indican la presencia inequívoca de stalkerware en el dispositivo.
- **No intentes borrar el stalkerware, cambiar algún ajuste ni manipular el teléfono antes de tener un plan de seguridad:** esto puede alertar a tu posible agresor y agravar la situación. También corres el riesgo de borrar datos o pruebas importantes que podrían utilizarse en un proceso judicial. Toma medidas para determinar qué línea de actuación tiene más sentido para la situación actual antes de hacer cambios que podrían llevar a una escalada del comportamiento de un potencial agresor.

Para más información acerca de nuestras actividades o cualquier otra consulta:
ExtR@kaspersky.com

kaspersky