

DIÁLOGOS



PRIMER INFORME

Prueba piloto del 11 al 22 de febrero de 2026

Elaborado por Equipo Ciberadar

ciberadar
Juventudes por espacios digitales seguros

Autor

Equipo de Ciberadar

Equipo de Diálogos

Walter Corzo, Director Ejecutivo

Daniel Núñez, Director Académico

Gabriela Ayerdi, Coordinadora de Gestión

Mayarí Prado, Coordinadora de Comunicación

Diseño: **Pedro Pablo Sánchez**

Edición: **Consejo Editorial Diálogos**






Dirección: 0 calle 16-26 zona 15 colonia El Maestro

Ciudad de Guatemala

Tel: 2369-6418

Correo: info@dialogos.org.gt

www.dialogos.org.gt

     @DialogosGuate

Este documento ha sido elaborado por Diálogos. El análisis y las opiniones contenidas en este documento pertenecen exclusivamente a Diálogos. Cualquier parte de esta publicación puede reproducirse total o parcialmente, sin permiso expreso de Diálogos, siempre y cuando se reconozca el crédito y las copias se distribuyan gratuitamente. Cualquier reproducción comercial requiere previo permiso escrito de Diálogos para ello puede solicitarlo al correo comunicacion@dialogos.org.gt.

Si tienes algún comentario u observación sobre esta publicación puedes enviarla al correo electrónico: info@dialogos.org.gt

Equipo de Ciberadar, Informe de prueba piloto (Ciudad Guatemala: Asociación Civil Diálogos, Observatorio Ciberadar, 2026).

Resumen ejecutivo

Este informe presenta los principales hallazgos de la prueba piloto del Ciberadar, realizada entre el 11 y el 22 de febrero de 2026, durante la cual el equipo de observación documentó 38 casos de ciberviolencia en distintas plataformas digitales. El objetivo de esta fase inicial exploratoria fue identificar patrones, tipos de agresión y dinámicas de interacción entre víctimas y victimarios en entornos digitales, con el fin de orientar futuras observaciones y mejorar las herramientas de monitoreo.

El tipo de ciberviolencia más frecuente fue el de ataques verbales y discursos de odio, que representaron 17 casos (45%) del total registrado. A estos se suman 14 casos adicionales (37%) en los que este tipo de agresión apareció combinado con otras formas de ciberviolencia, como amenazas, difusión no consentida de contenido, manipulación o acceso no autorizado a información. En conjunto, esto indica que gran parte de los episodios documentados corresponden a un discurso agresivo y hostigamiento público, muchas veces acompañado de otras prácticas digitales dañinas.

Un primer patrón relevante es que algunos casos de ciberviolencia están directamente vinculados con el contexto político nacional. Se documentaron ataques y campañas de desinformación que hacen referencia a procesos políticos en curso, como la elección de magistrados de cortes o procesos universitarios internos, que buscan engañar y desincentivar la participación política de las juventudes universitarias. En estos casos, actores digitales difundieron información falsa o promovieron campañas de desprestigio contra figuras públicas o actores políticos. Estos hallazgos sugieren que, además de responder a dinámicas propias de las redes sociales, ciertas manifestaciones de ciberviolencia—particularmente aquellas dirigidas contra actores políticos, que emplean marcos discursivos ideológicos o que se intensifican en contextos electorales—pueden funcionar como instrumentos de confrontación política o violencia política digital.

Otro hallazgo importante es que algunos casos de ciberviolencia están atravesados por estructuras más amplias de desigualdad social, especialmente aquellas relacionadas con sexo/género, etnia/raza y clase/posición socioeconómica. Ejemplos ilustrativos documentados incluyen ataques contra mujeres en páginas de “funas”, campañas de humillación pública sobre la apariencia física y casos de difusión no consentida de contenido íntimo. En varios de estos episodios, la violencia digital reproduce patrones de discriminación y misoginia presentes en la sociedad fuera de línea.

En relación con los actores involucrados, el análisis muestra que la mayoría de las víctimas fueron personas individuales (60%), mientras que la mayoría de los victimarios corresponden a grupos de individuos (58%). Esto indica que una proporción significativa de la ciberviolencia documentada adopta la forma de violencia colectiva, en la que múltiples usuarios participan en ataques coordinados o acumulativos contra una persona o grupo. Este fenómeno se ve facilitado por el anonimato y la dinámica de interacción propia de las redes sociales. Los patrones más frecuentes observados corresponden a grupos de usuarios atacando a individuos o a otros grupos de usuarios.

Asimismo, el análisis de los casos que involucran individuos muestra una clara sobrerrepresentación de perfiles femeninos entre las víctimas. En 14 de los 23 casos individuales (61%), las víctimas fueron personas femeninas, mientras que en siete casos (30%) fueron perfiles masculinos y en uno (4%) se trató de una persona trans. En el caso restante se desconoce el género de la persona. En contraste, en la mayoría de los casos no fue posible inferir el género de los victimarios, debido al uso de cuentas anónimas o páginas colectivas.

En cuanto a las plataformas utilizadas, Facebook concentró la mayoría de los casos registrados (58%), seguido por TikTok (21%), Instagram (10%) y X/Twitter (8%). En un caso (3%) se desconoce la plataforma utilizada. Aunque no se identificó una relación clara entre plataformas y tipos específicos de ciberviolencia, Facebook fue el principal espacio de interacción digital donde se observaron este tipo de agresiones.

El análisis también permitió clasificar los casos según su duración, finalidad y grado de intrusión. La mayoría de los episodios fueron ataques dirigidos a dañar a una persona o grupo en espacios públicos digitales, y ocurrieron de manera prolongada o reiterada. Sin embargo, también se registró un número significativo de casos efímeros, así como situaciones en las que no fue posible determinar con precisión estas dimensiones debido a limitaciones de información.

Finalmente, es importante subrayar que los patrones identificados deben interpretarse con cautela. Los resultados están condicionados por sesgos y limitaciones de observación inherentes al proceso de monitoreo, ya que los casos dependen del contenido público de las redes, páginas, influencers y grupos que las y los jóvenes observadores siguen, así como de los horarios en que realizan el monitoreo. Además, por razones de seguridad, no se ingresó a ciertos espacios digitales privados. En futuras rondas de observación se buscará ampliar las redes y comunidades monitoreadas, así como diversificar los horarios de observación, con el objetivo de captar una gama más amplia de manifestaciones de ciberviolencia.

En definitiva, los hallazgos de esta prueba piloto muestran que la ciberviolencia en el contexto observado se caracteriza por ataques públicos, colectivos y frecuentemente dirigidos contra individuos, muchas veces enmarcados en dinámicas políticas o en estructuras sociales más amplias de desigualdad. Estos resultados ofrecen una base inicial para fortalecer el sistema de monitoreo del Ciberadar y profundizar el análisis en futuras etapas del proyecto.

Metodología

Este informe se basa en una prueba piloto del Ciberadar realizada del 11 al 22 de febrero de 2026. La observación fue llevada a cabo por cinco jóvenes, distribuidos en distintos horarios, departamentos y redes sociales, como se detalla en la Tabla 1. Además, cada integrante del equipo de Ciberadar fue responsable de monitorear una lista específica de influencers, páginas y grupos dentro de las plataformas asignadas, y medios de comunicación digitales. Esta distribución fue consensuada entre el equipo de Diálogos y el equipo de observación, tomando en cuenta su disponibilidad y conocimiento de las dinámicas departamentales y de las distintas plataformas digitales.

Tabla 1. Distribución de observadores por departamentos y redes sociales

Observador	Departamentos	Redes sociales
Observador 1	Chiquimula, Zacapa, Izabal, Petén	Facebook, Instagram, TikTok
Observador 2	Guatemala, Sacatepéquez, Chimaltenango, Sololá	X/Twitter, Instagram, Facebook, Youtube
Observador 3	Alta Verapaz, Baja Verapaz, Quiché	Instagram, TikTok, FreeFire, Discord
Observador 4	Escuintla, Suchitepéquez, Huehuetenango	TikTok, Instagram, Facebook
Observador 5	Jutiapa, Jalapa, Santa Rosa, El Progreso	Whatsapp, Instagram, Facebook

En términos analíticos, durante esta primera etapa el equipo de observación se enfocó en documentar distintos casos de ciberviolencia, con el objetivo de visibilizar la diversidad de manifestaciones que ocurren en diferentes plataformas digitales. Cada integrante tuvo a su cargo un máximo de diez casos por semana, y se les indicó priorizar la diversidad de situaciones observadas por encima de su cuantificación. Asimismo, es importante notar que la observación incluyó casos que no necesariamente ocurrieron durante el periodo de monitoreo, sino que se remontan a años anteriores, con el fin de comprender el fenómeno en toda su complejidad y la diversidad de casos existentes.

El equipo de Diálogos acompañó al equipo de observación durante todo el proceso de la prueba piloto. Cada lunes se realizaron reuniones virtuales, con una duración promedio de dos horas, en las que ambos equipos discutieron los hallazgos más relevantes, resolvieron dudas y realizaron ajustes al cuestionario para corregir errores identificados durante la implementación.

A cada integrante del Ciberadar se le asignó un código único con el fin de facilitar la coordinación y el seguimiento de casos específicos. Asimismo, una de las observadoras asumió el rol de coordinadora del equipo, dando seguimiento a casos puntuales y manteniendo comunicación constante con los demás integrantes.

La comunicación entre los miembros de Ciberadar y el equipo de Diálogos se mantuvo a través de un grupo de Whatsapp creado específicamente para este propósito.

Hallazgos

En total, el equipo de Ciberadar reportó 38 casos de acciones violentas en el espacio virtual durante el periodo de la prueba piloto, como se muestra en la Tabla 2. La mayoría de los casos (n=17, 45%) corresponde a ataques verbales y discursos de odio, pero una cantidad significativa (n=14, 37%) involucró este tipo de acción en combinación con otras formas de agresión. También cabe destacar que hubo cuatro reportes (10% del total) de casos aislados que involucran la difusión no consentida de contenido, aunque más adelante mostraremos que este tipo de acción violenta se reportó más veces en combinación con otras formas de acciones violentas.

Tabla 2. Tipos de acciones violentas en el espacio virtual reportados por el Ciberadar, 11 a 22 de febrero de 2026.

Tipo de acciones violentas en el espacio virtual	Casos reportados	Porcentaje del total
Ataques verbales y discursos de odio	17	44.74%
Ataques verbales y discursos de odio + otras formas de ciberviolencia	14	36.84%
Difusión no consentida de contenido	4	10.53%
Engaño, fraude y manipulación	1	2.63%
Violencia, control y acceso no autorizado	1	2.63%
Violencia, control y acceso no autorizado + otras formas de ciberviolencia	1	2.63%
Total	38	100%

Nota: Los porcentajes han sido redondeados, por lo que el total puede no sumar exactamente 100%.

La Tabla 3 muestra los tipos de ataques verbales y discursos de odio mencionados en los 17 casos registrados de forma aislada. Dado que un solo caso puede involucrar más de un tipo de ataque, las frecuencias suman más de 17. Como se puede ver, el tipo más frecuente fue la difamación, con 15 menciones que representan el 21% del total. A este le sigue el ataque verbal o insulto basado en la apariencia física, con 11 menciones o 15% del total. Los ataques verbales o insultos basados en la ideología política y en el sexo/género fueron mencionados nueve veces cada uno, representando ambos el 26% de todas las menciones. Juntos, estos cuatro tipos de ataques verbales y discursos de odio representan el 62% de todas las menciones.

Tabla 3. Casos de ataques verbales y discursos de odio en combinación con otras formas de ciberviolencia reportados por el equipo de Ciberadar, 11 al 22 de febrero de 2026.

Tipo de acciones violentas en el espacio virtual	Casos reportados	Porcentaje del total
Ataques verbales y discursos de odio, difusión no consentida de contenido	5	13.16%
Ataques verbales y discursos de odio, amenazas	2	5.26%
Ataques verbales y discursos de odio, engaño, fraude y manipulación, difusión no consentida de contenido	2	5.26%
Ataques verbales y discursos de odio, amenazas, difusión no consentida de contenido	1	2.63%
Ataques verbales y discursos de odio, amenazas, engaño, fraude y manipulación, difusión no consentida de contenido, vigilancia, control y acceso no autorizado	1	2.63%
Ataques verbales y discursos de odio, amenazas, hostigamiento sexual digital	1	2.63%
Ataques verbales y discursos de odio, difusión no consentida de contenido, engaño, fraude y manipulación, vigilancia, control y acceso no autorizado	1	2.63%
Ataques verbales y discursos de odio, vigilancia, control y acceso no autorizado	1	2.63%
Total	14	36.84%

La Tabla 4 muestra los tipos de ataques verbales y discursos de odio mencionados en los 14 casos registrados en combinación con otras formas de agresión. Al igual que en la tabla anterior, un solo caso puede involucrar más de un tipo de acción violenta, por lo que las frecuencias suman más de 14. Como se puede observar, los ataques verbales y discursos de odio estuvieron acompañados por la difusión no consentida de contenido en 14 ocasiones (31% del total), seguidos por las amenazas, el engaño, fraude y manipulación, y la vigilancia, control y acceso no autorizado con 5 menciones u 11% del total cada uno.

Tabla 4. Ataques verbales y discursos de odio + tipos de acciones violentas en el espacio virtual en los 14 casos combinados reportados por el equipo de Ciberadar, 11 al 22 de febrero de 2026.

Tipo de acciones violentas en el espacio virtual	Frecuencia	Porcentaje del total	Tipo de acciones violentas en el espacio virtual	Frecuencia	Porcentaje del total
Ataques verbales y discursos de odio	14	31%	Ataques verbales y discursos de odio	14	31%
Difusión no consentida de contenido	14	31%	Difusión no consentida de contenido	14	31%
Amenazas	5	11%	Amenazas	5	11%
Engaño, fraude y manipulación	5	11%	Engaño, fraude y manipulación	5	11%
Vigilancia, control y acceso no autorizado	5	11%	Vigilancia, control y acceso no autorizado	5	11%
Hostigamiento sexual digital	1	2%	Hostigamiento sexual digital	1	2%
Persecución digital coordinada / campaña de cancelación digital	1	2%	Persecución digital coordinada / campaña de cancelación digital	1	2%
Total	45	100%	Total	45	100%

Nota: Los porcentajes han sido redondeados, por lo que el total puede no sumar exactamente 100%.

Un primer patrón emergente es que, aunque muchos casos de ciberviolencia responden a dinámicas propias de las redes sociales, otros se alimentan del contexto político nacional, por lo que pueden ser considerados como formas de violencia política digital. Ejemplos de esto son los casos de ataques verbales y discursos de odio documentados por el equipo de Ciberadar que hacen alusión directa al proceso de elección de cortes que se está llevando a cabo en el país, como lo ilustran los dos siguientes:

La página de noticias denominada "Xela News" difundió información falsa sobre las protestas realizadas el 16 de febrero en Antigua Guatemala. A través de sus publicaciones, calificó a los manifestantes (en su mayoría líderes indígenas) como "terroristas" y afirmó que fueron enviados por el actual presidente, Bernardo Arévalo, con el supuesto objetivo de boicotear la elección de magistrados de la Corte de Constitucionalidad por parte del Consejo Superior Universitario.

La cuenta "denunciaspoliticas" en TikTok realizó una campaña de desprestigio contra la influencer Jenn Te Informa, al publicar un video en el que la señala como responsable de haber dirigido la destrucción y los daños materiales a las oficinas de la carrera de Derecho en la Universidad de San Carlos de Guatemala. Estos hechos se dan en el contexto del proceso universitario para integrar el cuerpo electoral encargado de elegir al nuevo rector, donde la página se caracteriza por promover campaña negra contra la Planilla No. 3 de Derecho, aunque en este caso focaliza principalmente los señalamientos contra Jenn, quien, ante las acusaciones, compareció públicamente y respondió de manera cortés, rechazando y desvirtuando tales acusaciones con una imagen de prueba.

Según lo observado, algunos casos de ciberviolencia también están atravesados por estructuras más amplias de poder y desigualdad basadas en el sexo/género, la etnia/raza y la clase o posición socioeconómica de las personas. Un ejemplo de ello es el caso de una página de "funas" en la plataforma Facebook, en la que se expuso la vida íntima de una mujer de Santiago Sacatepéquez en enero de este año. Otro caso es el de María Nohemí Gómez, coronada reina de la feria 2023–2024 en San Juan Cotzal, Quiché, quien posteriormente recibió comentarios ofensivos masivos sobre su apariencia física en redes sociales, situación que algunos medios aseveraron la llevó al suicidio. Este caso ilustra claramente cómo la ciberviolencia no solo puede alimentarse del contexto no digital en el que surge, sino también producir efectos reales sobre él. En ambos casos, la violencia basada en género y las dinámicas del sistema patriarcal moldearon las formas de ciberviolencia, reproduciendo roles y estereotipos históricamente construidos y atentando sobre los cuerpos de las mujeres.

En cuanto a los patrones entre víctimas y victimarios, destaca que la mayoría de las víctimas (n=23, 60%) fueron personas individuales, mientras que la

mayoría de los victimarios (n=22,58%) corresponden a grupos de individuos (ver Tabla 5). Esto indica que una parte significativa de la ciberviolencia documentada adopta la forma de violencia colectiva, alimentada por el anonimato que facilitan las redes sociales y que, a su vez, contribuye a reforzarlo. Ejemplos de esto son los siguientes:

Un grupo de 141 personas atacó verbalmente a una activista y defensora de Derechos Humanos por medio de comentarios en Facebook el 3 de enero de 2026 en el departamento de Guatemala.

Una chica por medio de TikTok sube contenido sobre política, en un video que publicó donde hablaba de la importancia de comunicar e informar a las niñeces sobre lo que pasa en el país, con información clara y certera. Usuarios de la misma plataforma le dejan comentarios despectivos por haber utilizado el término "Niñeces", alegando que es una imposición ideológica y haciendo comentarios sobre su aspecto físico y otros comentarios donde indican que por las políticas de la aplicación no le dicen realmente lo que piensan sobre ella y su contenido.

Jóvenes tomaron fotos de la cuenta de Instagram de sus compañeras del mismo colegio y sometieron esas fotos a la Inteligencia Artificial para editarlas y que salieran desnudas. Esto ocurrió el 9 de agosto de 2024 en la zona 17 de la ciudad de Guatemala. Luego esos mismos jóvenes difundieron las fotos alteradas en redes sociales.

Tabla 5. Víctimas y victimarios de ciberviolencia reportados por el equipo de Ciberadar, 11 al 22 de febrero de 2026.

Víctima	Cantidad	Porcentaje del total	Victimarios	Cantidad	Porcentaje del total
Individuo	23	60%	Grupo de individuos	22	58%
Grupo de individuos	13	34%	Se desconoce	13	34%
Entidad u organización	1	3%	Individuo	3	8%
Se desconoce	1	3%			
Total	38	100%		38	100%

Nota: Los porcentajes han sido redondeados, por lo que el total puede no sumar exactamente 100%.

La Tabla 6 muestra que los patrones más comunes registrados hasta el momento son los de ciberviolencia ejercida por un grupo de individuos en contra de una persona individual o grupo de individuos. Los casos registrados en los que el victimario es una persona individual fueron pocos e involucraron a influencers y otras figuras públicas atacando a personas puntuales.

Tabla 6. Casos según tipo de víctima y victimario registrados por el equipo de Ciberadar, 11 al 22 de febrero de 2026.

Victimario	Víctima	Cantidad de casos	Porcentaje del total
Grupo de individuos	Individuo	12	32%
Grupo de individuos	Grupo de individuos	10	26%
Individuo	Individuo	2	5%
Individuo	Grupo de individuos	1	3%
Se desconoce	Grupo de individuos/Individuo	13	34%
Total		38	100%

Nota: Los porcentajes han sido redondeados, por lo que el total puede no sumar exactamente 100%.

Cabe señalar que se registraron también ataques en los que se desconoce si el victimario fue un individuo o un grupo de individuos. Estos ataques por lo general corresponden a páginas anónimas en las que se difama o se publica información personal o fotos íntimas de personas. Ejemplos de este tipo son los siguientes:

Una página de TikTok anónima expuso perfiles de adolescentes con descripciones y mensajes ofensivos que incitan al odio. Estas páginas se conocen comúnmente como páginas de "Quemados".

En 2023, una cuenta anónima de Instagram publicó contenido difamatorio contra una estudiante de un centro educativo en la ciudad de Guatemala, acusándola de enviar contenido íntimo y de involucrarse con varios compañeros, además de difundir su fotografía sin consentimiento. Esto ocurrió en el entorno digital de Instagram, pero con impacto directo dentro de la comunidad escolar, constituyendo un caso de ciberacoso y exposición pública contra una menor de edad.

Respecto al género de las víctimas y los victimarios, la Tabla 7 muestra que en 14 de 23 casos individuales (61%) las víctimas fueron perfiles femeninos, mientras que en 7 de 23 (30%) fueron masculinos. En cuanto a los victimarios, en la mayoría de los casos (n=13, 34%) no fue posible determinar su género, mientras que en tres casos se identificó que se trataba de personas masculinas.

Tabla 7. Género de las víctimas y victimarios en los casos registrados por el equipo de Ciberadar que involucran a individuos, 11 al 22 de febrero de 2026.

Género de la víctima	Frecuencia	Género del victimario	Frecuencia
Femenino	14	Se desconoce	13
Masculino	7	Masculino	3
Trans	1	Femenino	0
Se desconoce	1	Trans	0
Total	23		16

En relación con los medios utilizados, la mayoría de los casos documentados por el equipo de Ciberadar ocurrieron en Facebook (n=22, 58%), seguido por TikTok (n=8, 21%), Instagram (n=4, 10%) y X/Twitter (n=3, 8%), como lo muestra la Tabla 8. En esta fase inicial de observación, no se evidencia ningún patrón claro entre medios y tipos de ciberviolencia.

Tabla 8. Medios utilizados en los casos de ciberviolencia registrados por el equipo de Ciberadar, 11 al 22 de febrero de 2026.

Medio	Frecuencia	Porcentaje del total
Facebook	22	58%
TikTok	8	21%
Instagram	4	10%
X	3	8%
Se desconoce	1	3%
Total	38	100%

Nota: Los porcentajes han sido redondeados, por lo que el total puede no sumar exactamente 100%.

La Tabla 9 muestra las distintas categorías de ciberviolencia que surgen después de combinar las tres dimensiones de cada hecho: duración (efímeras o prolongadas), grado de intrusión (intrusiva y no intrusiva) y finalidad (hacer daño o tratar de obtener algo/impedir que la persona haga algo). Como se puede observar, la mayoría de los casos ocurrieron de manera prolongada, buscaron hacerle daño a la persona o grupo de personas, y se mantuvieron en el espacio público. Sin embargo, es importante notar que en materia de duración, hubo una cantidad de casos considerable que fueron efímeros, y que además en todas las dimensiones se documentaron casos que se desconoce en dónde encajarían.

Tabla 9. Duración, finalidad y grado de intrusión de los casos registrados por el equipo de Ciberadar, 11 al 22 de febrero de 2026.

Duración	Cantidad de casos	Finalidad	Cantidad de casos	Grado de intrusión	Cantidad de casos
Efímera (1 o 2 veces)	11	Hacerle daño a la persona	24	No intrusiva (se mantuvo en el espacio público)	27
Prolongada (3 o más veces)	15	Obtener algo de la persona o impedir que la persona haga algo	4	Intrusiva (invadió la esfera privada de la persona)	2
Se desconoce	12	Se desconoce	10	Se desconoce	9
Total	38	Total	38	Total	38

La Tabla 10 resume las frecuencias para las distintas categorías que surgen después de combinar las tres dimensiones de los casos en los que se lograron documentar todas ellas. Cabe señalar que el tipo predominante es el dirigido no intrusivo tanto para los casos efímeros como para los prolongados. En otras palabras, la mayoría de los casos registrados hasta el momento han sido ataques que buscaron hacerle daño directamente a una persona o grupo de personas en el espacio público. Fueron pocos los casos que se desviaron de este patrón.

Tabla 10. Tipos de ciberviolencia registrados por el equipo de Ciberadar según tipología basada en la duración, finalidad y grado de intrusión, 11 al 22 de febrero de 2026

Efímeras	Cantidad de casos	Prolongadas	Cantidad de casos
Utilitaria no intrusiva	1	Utilitaria no intrusiva	1
Utilitaria intrusiva	1	Utilitaria intrusiva	0
Dirigida no intrusiva	6	Dirigida no intrusiva	9
Dirigida intrusiva	0	Dirigida intrusiva	0
Se desconoce	3	Se desconoce	5
Total	11	Total	15

Es importante señalar que, aunque en este informe hemos identificado ciertos patrones emergentes, los resultados deben interpretarse con cautela, ya que están condicionados por un sesgo y limitación de reporte inherente al proceso de observación. En particular, los casos documentados dependen de las redes sociales, influencers, páginas y grupos que el equipo de observación monitorea, así como de los horarios en que realiza este monitoreo. Asimismo, la observación está sujeta a limitaciones derivadas de consideraciones de seguridad, como la decisión de no ingresar a grupos privados o espacios digitales potencialmente riesgosos para el equipo. En futuras fases de observación se buscará ampliar el espectro de redes, páginas y grupos analizados, así como de los horarios, con el objetivo de captar una gama más amplia de manifestaciones de ciberviolencia y reducir, en la medida de lo posible, estos sesgos de observación.

Conclusiones

La prueba piloto del Ciberadar permitió identificar patrones iniciales relevantes sobre las formas en que se manifiesta la ciberviolencia en el entorno digital monitoreado. En primer lugar, los hallazgos muestran que los ataques verbales y los discursos de odio constituyen la forma más frecuente de ciberviolencia registrada, ya sea de manera aislada o combinada con otras prácticas como amenazas, manipulación, difusión no consentida de contenido o acceso no autorizado a información. Esto sugiere que una parte de la ciberviolencia se articula alrededor de dinámicas de hostigamiento público que se amplifican mediante la interacción entre usuarios en redes sociales.

Asimismo, el análisis evidencia que una proporción importante de los ataques adopta la forma de violencia colectiva, en la que grupos de usuarios se dirigen contra individuos o contra otros grupos. Este patrón parece estar facilitado por el anonimato y la lógica de participación masiva que caracteriza a las plataformas digitales, que contribuyen a intensificar los efectos de la agresión sobre las víctimas.

Los resultados también muestran que los perfiles femeninos aparecen con mayor frecuencia entre las víctimas individuales, lo que sugiere que la ciberviolencia reproduce y amplifica desigualdades sociales preexistentes, particularmente aquellas relacionadas con el género. En varios de los casos documentados, las agresiones estuvieron vinculadas con dinámicas de humillación pública, exposición de la vida íntima o ataques sobre la apariencia física, lo que refleja patrones de violencia digital ampliamente documentados en la literatura internacional.

Otro hallazgo relevante es que algunos episodios de ciberviolencia se encuentran vinculados con el contexto político y social del país. En estos casos, la desinformación, el hostigamiento y las campañas de desprestigio se utilizan como herramientas para intervenir en debates públicos o procesos políticos en curso. Esto sugiere que, además de ser un fenómeno social y cultural propio de los entornos digitales, la ciberviolencia puede funcionar también como una forma de confrontación política en línea.

En términos de plataformas, Facebook concentró la mayor parte de los casos registrados, seguido por TikTok, Instagram y X, lo que confirma la importancia de estas redes como espacios centrales de interacción y conflicto digital en el contexto observado. A su vez, la mayoría de los casos registrados correspondió a ataques dirigidos a causar daño en espacios públicos digitales, ya sea de manera efímera o prolongada.

Finalmente, es importante reiterar que los patrones identificados en este informe deben interpretarse como hallazgos preliminares, ya que los datos están condicionados por limitaciones inherentes al proceso de observación, como las redes y comunidades monitoreadas, los horarios de seguimiento y las restricciones de seguridad que impiden acceder a ciertos espacios digitales privados. En futuras rondas de observación se buscará ampliar el alcance del monitoreo para capturar una mayor diversidad de casos y profundizar el análisis de las distintas manifestaciones de ciberviolencia.

DIÁLOGOS

ciberadar

Juventudes por espacios digitales seguros

