DIÁLOGOS

TERCER INFORME

1 al 30 de abril de 2026

Elaborado por Equipo Ciberadar

ciberadar

Juventudes por espacios digitales seguros

CIBER CIUDADANOS
UNODC
unesco
UNFPA
NACIONES UNIDAS GUATEMALA
FONDO PARA LA CONSOLIDACIÓN DE LA PAZ

Créditos

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

Cita sugerida:
Equipo de Ciberadar, Tercer Informe (Ciudad Guatemala: Asociación Civil Diálogos, Observatorio Ciberadar, 2026).

Esta publicación fue posible gracias al apoyo del Fondo para la Consolidación de la Paz de las Naciones Unidas (PBF), en el marco del Proyecto Ciberciudadanos Jóvenes Construyendo Paz, implementado por UNFPA, UNESCO y UNODC.

Una iniciativa de:

CIBER CIUDADANOS

UNODC unesco UNFPA NACIONES UNIDAS GUATEMALA FONDO PARA LA CONSOLIDACIÓN DE LA PAZ

Resumen ejecutivo

Equipo Ciberadar[1]

El presente informe analiza 84 casos de ciberviolencia documentados por el equipo de Ciberadar entre el 1 y el 30 de abril de 2026. Los resultados muestran que los ataques verbales y discursos de odio continúan siendo la forma predominante de violencia digital registrada por el equipo de observación. El 48% de los casos registrados (n=40) correspondió exclusivamente a ataques verbales y discursos de odio, mientras que un 18% adicional (n=15) combinó este tipo de agresión con otras formas de ciberviolencia, especialmente difusión no consentida de contenido, hostigamiento sexual digital, amenazas y vigilancia o acceso no autorizado. El 35% restante (n=29) correspondió a otras acciones violentas, principalmente engaño, fraude y manipulación (41%) y difusión no consentida de contenido (34%). Entre los ataques verbales y discursos de odio aislados, los más frecuentes están relacionados con la actividad profesional de las víctimas (30% de las menciones), seguidos por ataques basados en la apariencia física (21%), sexo o género (14%) y difamación (12%). Estos datos sugieren que gran parte de la violencia observada busca desacreditar públicamente, ridiculizar o erosionar la legitimidad social y profesional de las personas afectadas.

Los hallazgos muestran además que la ciberviolencia observada adopta predominantemente formas colectivas. La mayoría de las víctimas fueron personas individuales (68%, n=57), mientras que el principal tipo de victimario correspondió a grupos de individuos (44%, n=37). Los patrones más frecuentes fueron aquellos en los que grupos de personas ejercieron ataques contra individuos (n=22) o contra otros grupos (n=11), lo cual refuerza un hallazgo consistente en las distintas fases del proyecto: el anonimato y las dinámicas colectivas propias de las redes sociales facilitan la reproducción y amplificación de la violencia digital. Asimismo, el informe documenta que una parte importante de los casos se relaciona con el contexto político nacional y estructuras históricas de desigualdad, especialmente aquellas vinculadas con género, etnicidad y participación política. En ese sentido, los hallazgos continúan respaldando la interpretación de una parte significativa de la ciberviolencia como una forma de violencia política y social ejercida a través de medios digitales.

En relación con las características de las víctimas y victimarios, el informe muestra que el 37% de las víctimas (n=31) correspondió a perfiles masculinos y el 35% (n=29) a perfiles femeninos, mientras que en el 17% de los casos (n=14) no fue posible determinar el género. Respecto a los victimarios, en el 43% de los casos (n=36) se desconoce el género, aunque el 29% (n=24) involucró perfiles masculinos y el 21% (n=18) perfiles tanto masculinos como femeninos.

[1]Algunas secciones de este documento fueron elaboradas con apoyo de inteligencia artificial generativa para tareas de síntesis, estructuración y edición de texto, bajo supervisión y revisión del equipo de Ciberadar.

En cuanto a la edad de las víctimas, los grupos más afectados fueron las personas jóvenes entre 20 y 24 años y entre 25 y 29 años, con 14% de los casos cada uno (n=11 respectivamente). Sin embargo, en más de la mitad de los casos (54%, n=45) no fue posible determinar la edad de las víctimas. Los principales medios utilizados fueron Facebook, donde se documentó el 39% de los casos (n=33), seguido por TikTok y X con 21% cada uno (n=18, respectivamente). Instagram representó el 7% (n=6) y WhatsApp el 8% (n=7).

El análisis cualitativo permitió identificar nuevamente el uso creciente de inteligencia artificial para manipular imágenes, audios y contenido digital con fines de engaño, difamación y ridiculización pública. Los casos documentados muestran cómo herramientas de IA fueron utilizadas para fabricar imágenes falsas de figuras públicas, alterar audios y construir narrativas de desinformación orientadas a desacreditar actores políticos, líderes juveniles y personas visibles en el espacio público. Estos casos sugieren una sofisticación creciente de las estrategias de ciberviolencia y muestran cómo las nuevas tecnologías permiten intervenir cada vez más en la esfera pública y privada de las personas mediante contenidos manipulados difíciles de verificar o contrarrestar rápidamente. El informe también documenta las acciones tomadas por las víctimas para enfrentar estas agresiones, aunque en el 35% de los casos (n=32) se desconoce qué hicieron y en el 25% (n=23) no realizaron ninguna acción. Entre las respuestas identificadas destacan la publicación de aclaraciones en cuentas personales o institucionales (14%, n=13), respuestas públicas no agresivas (11%, n=10) y acciones legales (8%, n=7).

Finalmente, el informe evidencia que las consecuencias de la ciberviolencia pueden ser significativas y trascender el entorno digital. Aunque en el 55% de los casos (n=48) se desconoce qué ocurrió posteriormente, en el 24% (n=21) se registró daño reputacional, en el 13% (n=11) pérdidas económicas y en el 3% (n=3) daños emocionales como tristeza, angustia o miedo. Además, el equipo documentó dos casos en los que dinámicas de violencia iniciadas o sostenidas en plataformas digitales estuvieron seguidas por la muerte de las víctimas. La tipología desarrollada por Ciberadar muestra que la mayoría de los casos fueron efímeros (63%, n=53), dirigidos a causar daño (63%, n=53) y no intrusivos, es decir, se mantuvieron en el espacio público digital (62%, n=52). Sin embargo, también se registró una cantidad relevante de casos utilitarios e intrusivos orientados a obtener algo de las víctimas o intervenir directamente en su esfera privada. Aunque el informe reconoce limitaciones derivadas de los sesgos de observación, las plataformas monitoreadas y las restricciones de seguridad del equipo, los hallazgos ofrecen evidencia sobre la consolidación de nuevas formas de violencia digital en Guatemala y sobre la necesidad de fortalecer los mecanismos de monitoreo, análisis y respuesta frente a este fenómeno.

Metodología

Este informe se basa en el monitoreo realizado por el equipo de observación de Ciberadar del 1 al 30 de abril de 2026. La observación fue llevada a cabo por seis 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
Coordinadora	Chiquimula, Zacapa, Izabal, Petén	Facebook, Instagram, TikTok
Observador 1	San Marcos, Quetzaltenango, Totonicapán, Retalhuleu	Facebook, Instagram, Tiktok, X/Twitter
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 tercera etapa, el equipo de observación se enfocó en documentar distintos casos de ciberviolencia y de conscientemente buscar información sobre casos no incluidos en el informe de la prueba piloto y en el segundo informe, con el objetivo de visibilizar la diversidad de manifestaciones que ocurren en diferentes plataformas digitales. En particular, el equipo de observación buscó casos que hayan invadido la esfera privada de las personas con el fin de obtener algo de ellas o impedir que realizaran alguna actividad, y además casos que hayan tenido alguna repercusión grave sobre la víctima o víctimas. 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.

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.

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

Hallazgos

Análisis cuantitativo

En total, el equipo de Ciberadar reportó 84 casos de acciones violentas en el espacio virtual entre el 1 y 30 de abril, como se muestra en la Tabla 2. La mayoría de los casos (n=40, 48%) corresponde a ataques verbales y discursos de odio, pero una cantidad significativa (n=15, 18%) involucró este tipo de acción en combinación con otras formas de agresión. El 35% (n=29) restante son otras acciones violentas que describiremos más adelante.

Tabla 2. Tipos de acciones violentas en el espacio virtual reportados por el equipo de Ciberadar, 1 al 30 de abril de 2026.

Tipo de acciones violentas en el espacio virtual	Frecuencia	Porcentaje del total
Ataques verbales y discursos de odio	40	48.00%
Ataques verbales y discursos de odio + otras formas de ciberviolencia	15	18.00%
Otras acciones violentas	29	35.00%
Total	**84**	**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 40 casos registrados de forma aislada. Dado que un solo caso puede involucrar más de un tipo de ataque, las frecuencias suman más de 40. Como se puede ver, el tipo más frecuente fue el ataque verbal o insulto basado en actividad profesional (n=17, 30%), seguido por los ataques basados en la apariencia física (n=12, 21%) y sexo/género (n=8, 14%). Juntos, estos cuatro tipos de ataques verbales y discursos de odio representan el 65% de todas las menciones.

Tabla 3. Tipos de ataques verbales y discursos de odio en los 40 casos aislados reportados por el equipo de Ciberadar, 1 al 30 de abril de 2026.

Tipo de ataque verbal y discurso de odio	Frecuencia	Porcentaje del total
Ataque verbal o insulto basado en actividad profesional	17	30%
Ataque verbal o insulto basado en la apariencia física	12	21%
Ataque verbal o insulto basado en el sexo/género	8	14%
Difamación	7	12%
Ataque verbal o insulto basado en la orientación sexual	6	11%
Ataque verbal o insulto basado en el origen étnico	3	5%
Ataque verbal o insulto basado en la capacidad intelectual	2	4%
Ataque verbal o insulto basado en la ideología política	1	2%
Ataque verbal o insulto basado en religión	1	2%
Total	**57**	**100%**

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

La Tabla 4 muestra los tipos de ataques verbales y discursos de odio mencionados en los 15 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 15. Como se puede observar, los ataques verbales y discursos de odio estuvieron acompañados por la difusión no consentida de contenido en 8 ocasiones (44% del total), seguida por el hostigamiento sexual digital (n=4, 22%) y por las amenazas y la vigilancia, control y acceso no autorizado, con 3 casos o 17% del total cada una.

Tabla 4. Ataques verbales y discursos de odio + tipos de acciones violentas en el espacio virtual en los 15 casos combinados reportados por el equipo de Ciberadar, 1 al 30 de abril de 2026.

Tipo de acciones violentas en el espacio virtual	Frecuencia	Porcentaje del total
Difusión no consentida de contenido	18	44%
Hostigamiento sexual digital	4	22%
Amenazas	3	17%
Vigilancia, control y acceso no autorizado	3	17%
Total	**18**	**100%**

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

La Tabla 5 muestra las otras acciones violentas reportadas por el equipo de observación. La difusión no consentida de contenido y el engaño, fraude y manipulación suman el 75% de las menciones (n=24, en conjunto).

Tabla 5. Otras acciones violentas reportadas por el equipo de Ciberadar, 1 al 30 de abril de 2026.

Tipo de acciones violentas en el espacio virtual	Frecuencia	Porcentaje del total
Engaño, fraude y manipulación	13	41%
Difusión no consentida de contenido	11	34%
Vigilancia, control y acceso no autorizado	7	22%
Hostigamiento sexual digital	3	9%
Otros	1	3%
Total	**32**	**100%**

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

En cuanto a los patrones entre víctimas y victimarios, destaca que la mayoría de las víctimas (n=57, 68%) fueron personas individuales, mientras que la mayoría de los victimarios (n=37, 44%) corresponde a grupos de individuos (ver Tabla 6). Esto refuerza el hallazgo de la fase piloto y del segundo informe de que una parte significativa de la ciberviolencia documentada adopta la forma de violencia colectiva. Al igual que en los informes anteriores, en este caso también se documentaron varios casos (n=17, 20%) en los que se desconoce quién o quiénes fueron los victimarios. Como hemos señalado en repetidas ocasiones, el anonimato facilitado por las redes sociales y la violencia colectiva se retroalimentan.

Tabla 6. Víctimas y victimarios de ciberviolencia reportados por el equipo de Ciberadar, 1 al 30 de abril de 2026

Víctima	Cantidad	Porcentaje del total	Victimarios	Cantidad	Porcentaje del total
Individuo	57	68%	Grupo de individuos	37	44%
Grupo de individuos	21	25%	Individuo	28	33%
Entidad u organización	6	7%	Se desconoce	17	20%
Se desconoce	0	0%	Entidad u organización	2	2%
Total	**84**	**100%**	**Total**	**84**	**100%**

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

La Tabla 7 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 (n=22; n=11, respectivamente). También se registraron 21 casos en los que el victimario fue una persona individual en contra de un individuo y 14 en los que se desconoce el victimario y la víctima fue una persona individual.

Tabla 7. Casos según tipo de víctima y victimario registrados por el equipo de Ciberadar, 1 al 30 de abril de 2026.

Víctima	Victimario				
	Grupo de individuos	Individuo	Se desconoce	Entidad u organización	Total general
Individuo	22	21	14	0	**57**
Grupo de individuos	11	5	3	2	**21**
Entidad u organización	4	2	0	0	**6**
Total general	**37**	**28**	**17**	**2**	**84**

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

Respecto al género de las víctimas y los victimarios, la Tabla 8 muestra que en 31 de los 84 casos (37%), las víctimas fueron perfiles masculinos, mientras que en 29 de los 84 casos (35%), fueron perfiles femeninos. En 17% de los casos (n=14) se desconoce el género de la víctima. En cuanto a los victimarios, en la mayoría de los casos (n=36, 43%) no fue posible determinar el género, mientras que en 24 casos (29%) se identificó que se trataba de personas masculinas. En 18 casos (21%) los victimarios involucraron a perfiles tanto masculinos como femeninos.

Tabla 8. Género de las víctimas y victimarios en los casos registrados por el equipo de Ciberadar, 1 al 30 de abril de 2026

Género de la víctima	Frecuencia	Porcentaje del total	Género del victimario	Frecuencia	Porcentaje del total
Masculino	31	37%	Se desconoce	36	43%
Femenino	29	35%	Masculino	24	29%
Se desconoce	14	17%	Masculino, Femenino	18	21%
Masculino, Femenino	9	11%	Femenino	6	7%
Femenino, Trans	1	1%			
Total	**84**	**100%**	**Total**	**84**	**100%**

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

Un patrón emergente en los casos analizados sugiere que la ciberviolencia adopta formas diferenciadas según el género de las personas afectadas. Como se muestra en la Tabla 9, en el caso de las mujeres, predominan claramente los ataques vinculados al sexo/género (n=10, 35%), la apariencia física (n=6, 21%) y, en menor medida, la actividad profesional (n=4, 14%), lo que evidencia una tendencia a deslegitimarlas a partir de atributos corporales, identitarios o estereotipos de género. Por el contrario, en los hombres destacan relativamente más los ataques relacionados con la actividad profesional (n=9, 29%), la difamación (n=7, 23%) y la orientación sexual (n=5, 16%), orientados principalmente a cuestionar su reputación, desempeño o posición social. Estos hallazgos sugieren que la ciberviolencia reproduce patrones de desigualdad y normas de género preexistentes, utilizando distintos repertorios de agresión dependiendo del género de la víctima. La Tabla 9 resume estos hallazgos, las frecuencias y los porcentajes corresponden a menciones y solo a los casos en los que las víctimas fueron individuos, por lo que el total no suma 84.

Tabla 9. Tipo de ataque por género de la víctima en los casos registrados por el equipo de Ciberadar, 1 al 30 de abril de 2026

Tipo de ataque	Femenino n (%)	Masculino n (%)	Total
Sexo/género	10 (35%)	0 (0.0%)	10
Apariencia física	6 (21%)	6 (19%)	12
Actividad profesional	4 (14%)	9 (29%)	13
Difamación	3 (10%)	7 (23%)	10
Origen étnico	2 (7%)	2 (7%)	4
Pertenencia a organización criminal compleja	1 (3%)	0 (0.0%)	1
Capacidad intelectual	1 (3%)	0 (0.0%)	1
Rendimiento en el juego	0 (0.0%)	1 (3%)	1
Orientación sexual	0 (0.0%)	5 (16%)	5
Religión	0 (0.0%)	1 (3%)	1
Ideología política	0 (0.0%)	0 (0.0%)	0
Total menciones de ataques	**27 (93%)**	**31 (100%)**	**58**
No aplica	**13 (45%)**	**6 (19%)**	**19**

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

En cuanto a las edades de las víctimas de los casos de ciberviolencia registrados, la Tabla 10 muestra que más de una cuarta parte (n=22, 26%) ocurrió en contra de jóvenes entre los 20 y 29 años, mientras que en 5 casos (6%) las víctimas tenían 50 años o más. En más de la mitad de los casos (n=45, 54%) se desconoce la edad de la víctima.

Tabla 10. Rangos de edad de las víctimas de los casos de ciberviolencia registrados por el equipo de Ciberadar, 1 al 30 de abril de 2026

Rango de edad	Frecuencia	Porcentaje del total
5 a 9 años	1	1%
10 a 14 años	1	1%
15 a 19 años	2	2%
20 a 24 años	11	13%
25 a 29 años	11	13%
30 a 34 años	3	4%
35 a 39 años	1	1%
40 a 44 años	2	2%
45 a 49 años	2	2%
50 o más años	5	6%
Se desconoce	45	54%
Total	**84**	**100%**

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

En relación con los medios utilizados, la mayoría de los casos documentados por el equipo de Ciberadar ocurrieron en Facebook (n=33, 39%), seguido por TikTok (n=18, 21%) y X/Twitter (n=18, 21%). En esta fase también se registraron casos en Instagram (n=6, 7%) y Whatsapp (n=7, 8%). La Tabla 11 resume las menciones de los medios.

Tabla 11. Medios utilizados en los casos de ciberviolencia registrados por el equipo de Ciberadar, 1 al 30 de abril de 2026.

Medio	Frecuencia	Porcentaje
Facebook	33	39%
Tik Tok	18	21%
X	18	21%
Instagram	6	7%
Whatsapp	7	8%
Free Fire	1	1%
Otro	3	4%
Se desconoce	1	1%
Total	**84**	**100%**

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

Análisis cualitativo

Al igual que el informe anterior, este ejercicio de observación permitió confirmar y robustecer los patrones emergentes identificados en el informe de la prueba piloto, a saber: 1) la mayoría de los actos de ciberviolencia adoptan la forma de violencia colectiva, amplificada por condiciones de anonimato; y 2) una proporción significativa de los casos se nutre del contexto político nacional o de estructuras históricas de desigualdad, lo cual nos ha llevado a interpretarlos como expresiones de violencia política.

Algunos ejemplos de ataques verbales y discursos de odio:

> *El 13 de abril de 2026 el medio de comunicación "Región Más Noticias" publicó en Facebook que una adolescente de 15 años fue asesinada en Génova Costa Cuca, Quetzaltenango. Usuarios agredieron verbalmente a la difunta por sus relaciones interpersonales, apariencia física y por su género.*
>
> *El 14 de abril de 2026 una usuaria dueña de un negocio publicó en Tik Tok un vídeo promocionando los monopatines eléctricos en Retalhuleu. En el vídeo se ve a una mujer en falda sentada mientras lo prueba, usuarios la agredieron verbalmente por su género al hacer varios comentarios sexuales.*
>
> *Un usuario publicó en Facebook un meme ofensivo dirigido al alcalde Neto Bran, en el que lo insultaba y hacía insinuaciones sobre su orientación sexual, lo que provocó que otros usuarios reaccionaran replicando conductas discriminatorias mediante comentarios con insultos relacionados con su orientación sexual y su apariencia étnica y física.*

Una persona usuaria de la red social Facebook realizó un comentario ofensivo y sexualizado en contra de una mujer reportada como desaparecida. Específicamente, escribió "A hechar pata… buen finde tuvo", insinuando que la desaparición de la mujer se debía a un encuentro sexual, lo cual constituye una forma de violencia simbólica y revictimización. Esto ocurrió en el momento en que se publicó la ficha de búsqueda de la mujer en la página de Isabel Claudina, dentro de la sección de comentarios de dicha publicación.

El 25 de abril de 2026, una cuenta en X/Twitter publicó un mensaje dirigido al ministro de Cultura y Deportes, Luis Méndez Salinas, acompañado de fotografías en una ceremonia espiritual indígena. En la publicación se utilizaron expresiones despectivas hacia el funcionario, referencias ofensivas a prácticas religiosas y comentarios discriminatorios hacia pueblos indígenas.

En la plataforma de Facebook, una página publicó un video de un estudiante que participaba modelando para un concurso de Chico y Chica Verano en su Escuela de Ciclo básico, en el Municipio de Chiquimula , y por medio de esta publicación diversos usuarios reaccionaron negativamente, dirigiendo ataques hacia el joven por su forma de modelar, cuestionando su capacidad intelectual y haciendo suposiciones ofensivas sobre su orientación sexual, lo que derivó en una serie de comentarios de burla y descalificación en su contra dentro de dicha red social.

De igual forma, en el ejercicio anterior identificamos algunas formas de ciberviolencia que hacen uso de tecnología nueva para irrumpir en la vida privada de las personas. En esta ocasión, el equipo de Ciberadar volvió a registrar algunos casos de este tipo, en particular casos en los que la inteligencia artificial fue utilizada de manera cada vez más alarmante para engañar a usuarios, entrometerse en su vida privada y/o obtener algo de ellos. Algunos ejemplos:

El 3 de abril del 2026 la plataforma X la cuenta "El Republicano" difundió un mensaje compartiendo una fuente de información no verificada la cual afirmaba que Rodolfo Chang – candidato a rector de la USAC – recibía financiamiento de China. La publicación asegura que Rodolfo Chang tiene vínculos con líderes de países de China y Corea del Norte, así como con la ideología comunista. La imagen que acompaña la publicación modifica con IA a Rodolfo Chang acompañado de Xi Jinping y Kim Jong-un. Después de un tiempo el post fue removido de X.

La página de TikTok "noticias.delamate" difundió un video difamatorio generado mediante inteligencia artificial en contra del líder juvenil Ricardo Sánchez, vicepresidente de la ONG Jóvenes por la Transformación, en el contexto del proceso de elección del rector de la USAC. El contenido manipulaba un audio para hacer parecer que Sánchez apoyaba la elección de Mazariegos, constituyendo una difusión no consentida de material alterado con fines de desinformación. Este hecho ocurrió una o dos veces y fue publicado desde un perfil anónimo, en el marco de una relación exclusivamente digital entre víctima y victimario, propia de comunidades en línea donde interactúan seguidores, detractores o cuentas sin identificación clara.

El 15 de marzo de 2026, en la red social X (Twitter), una cuenta con seudónimo publicó contenido dirigido contra la diputada Andrea Reyes, del partido Semilla, consistente en una imagen manipulada mediante inteligencia artificial en la que se altera su rostro y cuerpo con fines de burla. La publicación incluía referencias ofensivas hacia su apariencia física, promoviendo la ridiculización y el desprestigio público. La cuenta emisora, cuya identidad se desconoce y que aparenta estar dedicada sistemáticamente a desacreditar a figuras políticas —posiblemente vinculada a dinámicas de netcenter—, difundió este contenido en un contexto de interacción exclusivamente digital. La víctima es una funcionaria pública, mujer mestiza de entre 35 y 39 años, ubicada en Palencia al momento del hecho.

En este ejercicio de observación, el equipo de Ciberadar también documentó las acciones que tomaron las víctimas para lidiar con la ciberviolencia y algunos casos con repercusiones serias para las víctimas. En general, como se puede observar en la Tabla 12, en la mayoría de los casos no se sabe qué hicieron las víctimas (n=32, 35%) o no tomaron ninguna acción (n=23, 27%). Sin embargo, en una proporción importante (n=13, 14%) las víctimas publicaron una aclaración en su cuenta personal o institucional o respondieron públicamente a la persona sin agredirla (n=10, 11%). Como se ha mencionado con tablas anteriores, esta tabla resume las menciones, y dado que un solo caso puede involucrar más de una acción, las frecuencias suman más de 84.

Tabla 12. Acciones que tomaron las víctimas para lidiar con la ciberviolencia en los casos registrados por el equipo de Ciberadar, 1 al 30 de abril de 2026.

Acción	Frecuencia	Porcentaje del total
Se desconoce	32	35%
Ninguna	23	25%
Publicó una aclaración en su cuenta personal o institucional	13	14%
Respondió públicamente a la persona sin agredirla	10	11%
Tomó acciones legales contra la persona	7	8%
Bloqueó o reportó la cuenta	3	3%
Limitó los comentarios del video	1	1%
Restringió los comentarios en todas sus redes sociales	1	1%
Puso sus cuentas privadas	1	1%
Reemplazó la imagen generada con IA	1	1%
Total	**92**	**100%**

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

En cuanto a las consecuencias que tuvieron los actos de ciberviolencia, la Tabla 13 muestra que en más de la mitad de los casos (n=48, 55%) se desconoce qué ocurrió, pero en un porcentaje significativo (n=35, 40%) las personas experimentaron daño reputacional, material o emocional. La tabla resume las menciones, por lo que las frecuencias suman más de 84.

Tabla 13. Consecuencias que tuvieron en las víctimas los casos de ciberviolencia registrados por el equipo de Ciberadar, 1 al 30 de abril de 2026

Tipo de consecuencia	Frecuencia	Porcentaje del total
Se desconoce	48	55%
Daño reputacional (afectación de imagen pública)	21	24%
Daño material (pérdidas económicas)	11	13%
Daño emocional (tristeza, angustia, miedo)	3	3%
Muerte a manos de otra persona	2	2%
Daño sexual (afectación de la integridad sexual)	1	1%
Daño simbólico/cultural y de identidad	1	1%
Total	**87**	**100%**

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

Cabe señalar que en dos ocasiones los actos de ciberviolencia estuvieron seguidos por la muerte de la persona. Estos casos son los siguientes:

> *El 17 de octubre de 2024, en el gimnasio municipal de Colomba, Quetzaltenango, un adolescente de 14 años fue baleado por un niño de 11 años en un hecho que, según la Policía Nacional Civil (PNC), se originó a partir de un conflicto de ciberacoso en el videojuego Free Fire. De acuerdo con la información disponible, las interacciones previas entre ambos, quienes eran compañeros de escuela, incluyeron ataques verbales relacionados con el rendimiento en el juego, así como dinámicas de vigilancia digital y seguimiento dentro de la plataforma. Además, se reportaron amenazas de agresión física y contra la vida, lo que evidencia una escalada progresiva de la violencia desde el entorno virtual hacia el físico. El joven herido falleció el 6 de octubre como consecuencia del ataque*[2].

[2] Ver nota de Prensa Libre sobre este caso aquí: https://www.prensalibre.com/guatemala/justicia/juego-de-free-fire-fue-la-causa-por-la-que-un-adolescente-le-disparo-a-estudiante-en-colomba/

A inicios de 2026 la cuenta de una chica menor de edad en Tik Tok tenía constantemente comentarios del Barrio 18 con símbolos recurrentes. Aparentemente ella pertenecía a la MS-13 y tenía conflicto con el Barrio 18. En sus publicaciones a veces respondía a las provocaciones, y algunos vídeos hacían referencia a conflictos por medio de redes sociales como el hostigamiento y amenazas de muerte. Lamentablemente, el 13 de abril fue asesinada presuntamente por algún miembro del Barrio 18[3].

La Tabla 14 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, y al igual que en el informe anterior, la mayoría de los casos ocurrieron de manera efímera, buscaron hacerle daño a la persona o grupo de personas, y se mantuvieron en el espacio público.

Tabla 14. Duración, finalidad y grado de intrusión de los casos registrados por el equipo de Ciberadar, 1 al 30 de abril de 2026.

Duración	Cantidad de casos	Finalidad	Cantidad de casos	Grado de intrusión	Cantidad de casos
Efímera (1 o 2 veces)	53	Hacerle daño a la persona	53	No intrusiva (se mantuvo en el espacio público)	52
Prolongada (3 o más veces)	22	Obtener algo de la persona o impedir que la persona haga algo	17	Intrusiva (invadió la esfera privada de la persona	19
Se desconoce	9	Se desconoce	14	Se desconoce	13
Total	**84**	**Total**	**84**	**Total**	**84**

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

La Tabla 15 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. Al igual que en el informe anterior, 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 han sido ataques que buscaron hacerle daño directamente a una persona o grupo de personas en el espacio público. Sin embargo, en esta ocasión, el equipo de Ciberadar registró una cantidad relevante de casos utilitarios intrusivos tanto efímeros como prolongados (n=8, 10%, en conjunto).

[3] Caso registrado por equipo de Ciberadar a través del monitoreo de diferentes redes sociales. Para una nota de Prensa Comunitaria sobre el asesinato, ver aquí: https://www.chapintv.com/noticia/identifican-a-menor-fallecida-tras-balacera-en-quetzaltenango/

Tabla 15. Tipos de ciberviolencia registrados por el equipo de Ciberadar según tipología basada en la duración, finalidad y grado de intrusión, 1 al 30 de abril 2026.

Efímeras	Cantidad de casos	Porcentaje del total
Dirigida no intrusiva	33	39%
Utilitaria intrusiva	4	5%
Utilitaria no intrusiva	2	2%
Dirigida intrusiva	2	2%
Prolongadas	**Cantidad de casos**	**Porcentaje del total**
Dirigida no intrusiva	11	13%
Utilitaria intrusiva	4	5%
Dirigida intrusiva	3	4%
Utilitaria no intrusiva	0	0%
Se desconoce (al menos una dimensión faltante	**25**	**30%**
Total	**84**	**100%**

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

Como hemos mencionado en informes anteriores, es relevante destacar que los resultados de este informe deben interpretarse con cautela, ya que están condicionados por un sesgo y limitación de reporte inherentes 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.

Conclusiones

Los hallazgos de este informe confirman que la ciberviolencia registrada hasta el momento constituye un fenómeno complejo, persistente y cada vez más sofisticado, que no puede entenderse únicamente como una serie de agresiones aisladas entre individuos en plataformas digitales. Por el contrario, los patrones observados sugieren que gran parte de la violencia documentada se encuentra estrechamente vinculada con dinámicas colectivas, conflictos políticos, relaciones desiguales de poder y procesos históricos de discriminación y exclusión que se trasladan y amplifican en el espacio digital. La alta frecuencia de ataques colectivos contra personas individuales, así como la importancia del anonimato y de las cuentas pseudónimas o coordinadas, muestran que las redes sociales funcionan como escenarios donde se producen, reproducen y escalan distintas formas de violencia pública.

Asimismo, el informe evidencia que los ataques verbales y discursos de odio siguen siendo el principal mecanismo de agresión digital documentada, particularmente a través de ataques dirigidos contra la actividad profesional, la apariencia física, el sexo o género y otros rasgos identitarios de las víctimas. Esto sugiere que la ciberviolencia opera frecuentemente como un mecanismo de desacreditación pública y control simbólico orientado a erosionar la legitimidad, reputación o participación de determinadas personas en la esfera pública. La recurrencia de casos relacionados con actores políticos, líderes juveniles, figuras públicas y personas expuestas mediáticamente también refuerza la interpretación de una parte importante de la ciberviolencia como una forma de violencia política digital, especialmente en contextos altamente polarizados o conflictivos.

Un hallazgo particularmente relevante de este ejercicio de observación es la creciente utilización de inteligencia artificial para generar contenido manipulado con fines de desinformación, ridiculización y engaño. Las imágenes alteradas, audios manipulados y contenidos generados artificialmente documentados en este informe muestran que las nuevas tecnologías están ampliando significativamente las capacidades para intervenir en la vida pública y privada de las personas. Este fenómeno representa un desafío importante porque dificulta la identificación de contenidos falsos, incrementa la velocidad de propagación de campañas de desprestigio y reduce las capacidades de respuesta de las víctimas y de las instituciones. La presencia de este tipo de prácticas sugiere que la ciberviolencia podría volverse más compleja y dañina en los próximos años si no se desarrollan mecanismos adecuados de regulación, alfabetización mediática e informacional.

El informe también evidencia que las consecuencias de la ciberviolencia pueden trascender significativamente el entorno digital. Aunque en muchos casos no fue posible documentar el impacto posterior sobre las víctimas, los datos disponibles muestran afectaciones reputacionales, emocionales y económicas importantes. Además, los dos casos documentados en los que la violencia digital estuvo seguida por la muerte de las víctimas ilustran de manera particularmente clara

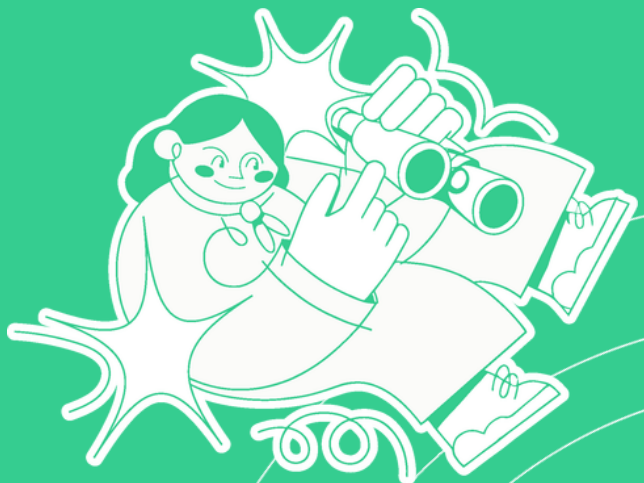
cómo las fronteras entre violencia virtual y violencia física pueden diluirse progresivamente. Esto refuerza la necesidad de abandonar visiones que minimizan la ciberviolencia como un fenómeno exclusivamente simbólico o inofensivo, y reconocerla como una problemática con potenciales consecuencias materiales y humanas graves.

Finalmente, los resultados subrayan la importancia de fortalecer mecanismos institucionales, sociales y tecnológicos para prevenir, monitorear y responder a la ciberviolencia. La limitada cantidad de acciones legales registradas, el alto porcentaje de casos en los que se desconoce la respuesta de las víctimas y las dificultades para identificar a los victimarios muestran que todavía existen importantes vacíos de protección, denuncia y acompañamiento. Aunque este informe reconoce las limitaciones inherentes al proceso de observación —incluyendo sesgos derivados de las plataformas monitoreadas, los horarios de observación y las restricciones de seguridad del equipo—, los patrones identificados son suficientemente consistentes como para afirmar que la ciberviolencia constituye un fenómeno con potenciales consecuencias dañinas para el ejercicio de la libre expresión, la participación ciudadana de las juventudes y la convivencia pacífica en Guatemala.

DIÁLOGOS

ciberadar

Juventudes por espacios digitales seguros



CIBER CIUDADANOS

UNODC unesco UNFPA NACIONES UNIDAS GUATEMALA | FONDO PARA LA CONSOLIDACIÓN DE LA PAZ