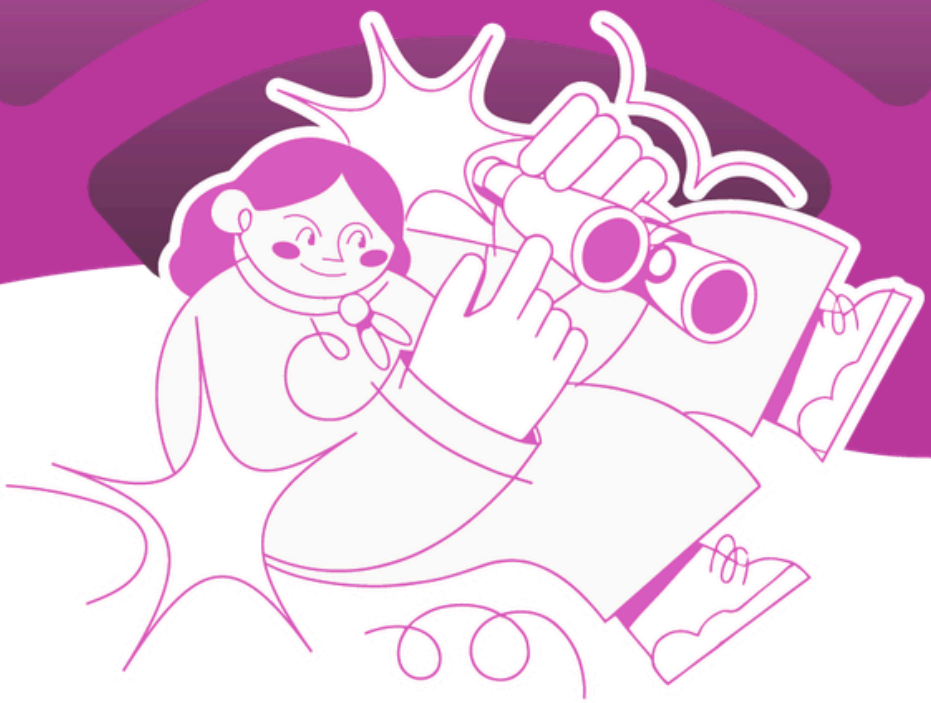
DIÁLOGOS



SEGUNDO INFORME

23 de febrero al 31 de marzo 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, Informe de prueba piloto (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 sistematiza los hallazgos del monitoreo de ciberviolencia realizado por el equipo de Ciberadar entre el 23 de febrero y el 31 de marzo de 2026, periodo en el cual se documentaron 128 casos en distintas plataformas digitales.

Los resultados muestran que los casos registrados se caracterizan por una alta prevalencia de ataques verbales y discursos de odio, ya sea de forma aislada (51%) o en combinación con otras formas de agresión (36%). Estas manifestaciones se concentran principalmente en insultos relacionados con la capacidad intelectual, la ideología política, la actividad profesional y el género.

Un hallazgo central es el carácter predominantemente colectivo de los casos de ciberviolencia registrados: la mayoría de las víctimas son individuos (58%), mientras que los victimarios suelen ser grupos de personas (68%), lo que evidencia dinámicas de violencia colectiva facilitadas por el anonimato y la interacción en redes sociales. Este patrón se refuerza con la alta proporción de casos en los que no es posible identificar a los agresores.

En términos de plataformas, Facebook (51%), TikTok (24%) y X/Twitter (16%) concentran la mayor parte de los casos registrados. Asimismo, se observa que los algoritmos de estas plataformas pueden contribuir a la reproducción y amplificación de este tipo de contenidos.

Desde el punto de vista cualitativo, una proporción significativa de los casos se vincula con el contexto político nacional —particularmente el proceso electoral de segundo grado que se lleva a cabo actualmente— y con estructuras históricas de desigualdad, como el racismo, el sexismo y la discriminación de clase. También se identifican nuevas modalidades de ciberviolencia asociadas al uso de tecnologías emergentes, como la inteligencia artificial, así como prácticas de fraude, extorsión y difusión no consentida de contenido.

Finalmente, en términos teóricos, la mayoría de los casos son de carácter efímero, no intrusivo y orientado a causar daño en el espacio público digital. Sin embargo, existe una proporción relevante de casos prolongados e intrusivos que implican mayores riesgos para las víctimas.

[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.

Metodología

Este informe se basa en el monitoreo realizado por el equipo de observación de Ciberadar del 23 de febrero al 31 de marzo 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 segunda 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, 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.

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.

Como resultado, se realizaron modificaciones al cuestionario implementado durante la prueba piloto, incluyendo nuevas opciones y reorganización del enlace entre secciones. Estos cambios facilitaron el flujo de navegación, agilizaron el proceso de registro y mejoraron la calidad de la información recopilada. Asímismo, se desarrolló una guía con los conceptos de los distintos tipos de acciones violentas en el espacio digital, con el propósito de que todo el equipo de observación cuente con criterios unificados al momento de clasificar los casos y facilitar la revisión de la base de datos.

Hallazgos

Análisis cuantitativo

En total, el equipo de Ciberadar reportó 128 casos de acciones violentas en el espacio virtual entre el 23 de febrero y el 31 de marzo, como se muestra en la Tabla 2. La mayoría de los casos (n=65, 51%) corresponde a ataques verbales y discursos de odio, pero una cantidad significativa (n=46, 36%) involucró este tipo de acción en combinación con otras formas de agresión. El 13% (n=17) 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, 23 de febrero al 31 de marzo de 2026

Tipo de acciones violentas en el espacio virtual	Casos reportados	Porcentaje del total
Ataques verbales y discursos de odio	65	51%
Ataques verbales y discursos de odio + otras formas de ciberviolencia	46	36%
Otras acciones violentas	17	13%
Total	**128**	**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 65 casos registrados de forma aislada. Dado que un solo caso puede involucrar más de un tipo de ataque, las frecuencias suman más de 65. Como se puede ver, el tipo más frecuente fue el ataque verbal o insulto basado en la capacidad intelectual (n=17, 15%), seguido por los ataques basados en la ideología política (n=16, 14%), actividad profesional (n=15, 13%) y el sexo/género (n=15, 13%). Juntos, estos cuatro tipos de ataques verbales y discursos de odio representan el 55% de todas las menciones.

Tabla 3. Tipos de ataques verbales y discursos de odio en los 65 casos aislados reportados por el equipo de Ciberadar, 23 de febrero al 31 de marzo de 2026.

Tipo de ataque verbal y discurso de odio	Frecuencia	Porcentaje del total
Ataque verbal o insulto basado en la capacidad intelectual	17	15%
Ataque verbal o insulto basado en la ideología política	16	14%
Ataque verbal o insulto basado en actividad profesional	15	13%
Ataque verbal o insulto basado en el sexo/género	15	13%
Ataque verbal o insulto basado en la apariencia física	14	12%
Difamación	11	10%
Ataque verbal o insulto basado en el origen étnico	8	7%
Ataque verbal o insulto basado en la orientación sexual	6	5%
Ataque verbal o insulto basado en la posición socio económica	5	4%
Ataque verbal o insulto basado en su vida sexual y relaciones personales	5	4%
Ataque verbal o insulto basado en nacionalidad/país de origen	3	3%
Total	**115**	**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 46 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 46. Como se puede observar, los ataques verbales y discursos de odio estuvieron acompañados por la difusión no consentida de contenido en 20 ocasiones (33% del total), seguida por el hostigamiento sexual digital y por la vigilancia, control y acceso no autorizado, con 13 menciones (23% del total) cada una.

Tabla 4. Ataques verbales y discursos de odio + tipos de acciones violentas en el espacio virtual en los 46 casos combinados reportados por el equipo de Ciberadar, 23 de febrero al 31 de marzo de 2026

Tipo de acciones violentas en el espacio virtual	Frecuencia	Porcentaje del total
Difusión no consentida de contenido	20	33%
Hostigamiento sexual digital	13	22%
Vigilancia, control y acceso no autorizado	13	22%
Engaño, fraude y manipulación	6	10%
Amenazas	6	10%
Hostigamiento sexual	2	3%
Total	**60**	**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. El engaño, fraude y manipulación y la difusión no consentida de contenido suman más del 50% de las menciones (n=17, en conjunto), seguidas por la vigilancia, control y acceso no autorizado y el hostigamiento sexual digital, con 5 menciones (17%) cada uno.

Tabla 5. Otras acciones violentas reportadas por el equipo de Ciberadar, 23 de febrero al 31 de marzo de 2026.

Tipo de acciones violentas en el espacio virtual	Frecuencia	Porcentaje del total
Engaño, fraude y manipulación	10	34%
Difusión no consentida de contenido	7	24%
Vigilancia, control y acceso no autorizado	5	17%
Hostigamiento sexual digital	5	17%
Amenazas	2	7%
Total	**29**	**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=74, 58%) fueron personas individuales, mientras que la mayoría de los victimarios (n=87, 68%) corresponde a grupos de individuos (ver Tabla 6). Esto refuerza el hallazgo de la fase piloto de que una parte significativa de la ciberviolencia documentada adopta la forma de violencia colectiva. Al igual que en la fase piloto, en este caso también se documentaron varios casos (n=17, 13%) en los que se desconoce quién o quiénes fueron los victimarios. Como señalamos anteriormente, el anonimato facilitado por las redes sociales alimenta la violencia colectiva y ésta, a la vez, lo refuerza.

Tabla 6. Víctimas y victimarios de ciberviolencia reportados por el equipo de Ciberadar, 23 de febrero al 31 de marzo de 2026

Víctima	Cantidad	Porcentaje del total	Victimarios	Cantidad	Porcentaje del total
Individuo	74	58%	Grupo de individuos	87	68%
Grupo de individuos	43	34%	Individuo	23	18%
Entidad u organización	9	7%	Se desconoce	17	13%
Se desconoce	2	2%	Entidad u organización	1	1%
Total	**128**	**100%**	**Total**	**128**	**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=47 y n=35, respectivamente). También se registraron 23 casos en los que el victimario fue una persona individual y 17 en los que se desconoce.

Tabla 7. Casos según tipo de víctima y victimario registrados por el equipo de Ciberadar, 23 de febrero al 31 de marzo de 2026

Víctima	Victimario				
	Entidad u organización	Grupo de individuos	Individuo	Se desconoce	Total
Grupo de individuos	4	35	47	1	**87**
Individuo	5	0	17	1	**23**
Se desconoce	0	7	10	0	**17**
Entidad u organización	0	1	0	0	**1**
Total	**9**	**43**	**74**	**2**	**128**

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 49 de los 128 casos (38%), las víctimas fueron perfiles femeninos, mientras que en 32 de los 128 casos (25%), se desconoce el género. En 24% de los casos (n=31) la víctima fue masculina. En cuanto a los victimarios, en la mayoría de los casos (n=53, 41%) no fue posible determinar el género, mientras que en 40 casos (31%) se identificó que se trataba de personas femeninas y masculinas (porque los casos involucraron a grupos de individuos). Los perfiles masculinos representaron el 27% (n=34) de los victimarios registrados.

Tabla 8. Género de las víctimas y victimarios en los casos registrados por el equipo de Ciberadar, 23 de febrero al 31 de marzo de 2026

Género de la víctima	Frecuencia	Porcentaje del total	Género del victimario	Frecuencia	Porcentaje del total
Femenino	49	38%	Se desconoce	53	41%
Se desconoce	32	25%	Masculino, Femenino	40	31%
Masculino	31	24%	Masculino	34	27%
Masculino, Femenino	13	10%	Femenino	1	1%
Trans	3	2%	Trans	0	0
Total	**128**	**100%**	**Total**	**128**	**100%**

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 9 muestra que casi una cuarta parte (n=31, 24%) ocurrió en contra de jóvenes entre los 10 y 29 años, mientras que en 13 casos (10%) las víctimas tenían 45 años o más.

Tabla 9. **Rangos de edad de las víctimas de los casos de ciberviolencia registrados por el equipo de Ciberadar, 23 de febrero al 31 de marzo de 2026**

Rango de edad	Frecuencia	Porcentaje del total
10 a 14 años	3	2%
15 a 19 años	9	7%
20 a 24 años	11	9%
25 a 29 años	8	6%
30 a 34 años	5	4%
35 a 39 años	5	4%
40 a 44 años	4	3%
40 a 44 años	1	1%
45 a 49 años	4	3%
50 o más años	9	7%
Se desconoce	69	54%
Total	**128**	**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=65, 51%), seguido por TikTok (n=31, 24%) y X/Twitter (n=21, 16%). En esta fase también se registraron casos en Instagram (n=9, 7%) y Whatsapp (n=6, 5%). La Tabla 10 resume las menciones de los medios, y dado que un solo caso puede involucrar más de un medio, las frecuencias suman más de 128.

Tabla 10. Medios utilizados en los casos de ciberviolencia registrados por el equipo de Ciberadar, 23 de febrero al 31 de marzo de 2026

Medio	Frecuencia	Porcentaje del total
Facebook	65	51%
TikTok	31	24%
X/Twitter	21	16%
Instagram	9	7%
Whatsapp	6	5%
Telegram	2	2%
Otro	2	2%
Messenger	1	1%
Roblox	1	1%
Total	**138**	**100%**

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

Análisis cualitativo

Este ejercicio de observación permitió confirmar y robustecer los patrones emergentes identificados en el informe de la prueba piloto. En particular: 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 que permite interpretarlos como expresiones de violencia política en entornos digitales.

Ejemplos de ciberviolencia colectiva amplificada por condiciones de anonimato son los siguientes:

> *En la plataforma de TikTok, la cuenta @concepcionlasminas ha realizado publicaciones dirigidas contra diversas personas del municipio de Concepción Las Minas, mediante contenidos en los que se expone o "quema" públicamente a individuos de la comunidad. A través de videos y publicaciones dentro de la plataforma, los administradores de la cuenta solicitan a otros usuarios enviar información personal o señalamientos sobre diferentes personas para difundirlos públicamente, incluyendo en varias ocasiones mensajes difamatorios y críticas reiteradas hacia jóvenes que han sido representantes de belleza del municipio. Estas publicaciones han generado interacción de otros usuarios de la red social, quienes, en la sección de comentarios, refuerzan este comportamiento al incentivar que continúen las funas, así como al publicar mensajes ofensivos o de odio dirigidos hacia las personas expuestas.*

En una página de "Quemados" en la red social de TikTok, los administradores publicaron un video en el que aparecen tres jóvenes, acompañándolo con una canción cuyo contenido sugiere una situación de infidelidad por parte de una joven, dando a entender, por el contexto, que ella mantiene una relación con dos personas al mismo tiempo. A partir de esta publicación, usuarios de la plataforma reaccionaron en la sección de comentarios con risas, burlas y opiniones sobre lo que interpretaron del video.

En cuanto a los casos que se nutren del contexto político nacional o de estructuras históricas de desigualdad, en esta ocasión se registraron de nuevo acciones violentas relacionadas con el proceso de elecciones de segundo grado y ataques racistas, sexistas y de clase. Un ejemplo de difamación relacionado con el proceso electoral en marcha es el siguiente:

La cuenta de TikTok "denunciaspoliticas" publicó un video en el que señalaba a la influencer y activista digital "Jenn Te Informa" como presunta responsable de haber dirigido la destrucción y daños materiales en las oficinas de la carrera de Derecho de la Universidad de San Carlos de Guatemala. Estas acusaciones se produjeron en el contexto del proceso universitario para integrar el cuerpo electoral encargado de elegir al nuevo rector. La página se caracteriza por promover campañas de desprestigio contra la Planilla No. 3 de Derecho, y en este caso focalizó los señalamientos principalmente contra Jenn. Ante estas acusaciones, ella compareció públicamente en sus redes sociales y respondió de manera cortés, rechazando y desvirtuando las afirmaciones mediante la presentación de una imagen como prueba. La víctima es una mujer de entre 20 y 24 años, ladina/mestiza, residente en Guatemala, quien participa como activista digital y forma parte del cuerpo electoral de la Planilla No. 3 de Derecho. La identidad de la persona o personas responsables de la ciberviolencia se desconoce, así como su género, edad, origen o ubicación.

Ejemplos de casos moldeados por estructuras históricas de desigualdad, en particular racismo y sexismo, son los siguientes:

El 25 de febrero de 2026, el medio de comunicación Noticias del Valle compartió en Facebook la noticia de un pickup que causó daño a un puesto de ventas de Coatepeque, Quetzaltenango. Al tratar de escapar los afectados golpearon el vehículo. Usuarios que comentaron la noticia agredieron verbalmente a los afectados del puesto de venta por su capacidad intelectual, origen étnico y origen departamental.

El 8 de marzo de 2026, en Guatemala, la vicepresidenta Karin Herrera publicó en la red social X un video conmemorativo por el Día Internacional de la Mujer. En respuesta a esta publicación, el usuario Luis Hernández realizó una cadena de respuestas con mensajes ofensivos en los que descalificó el feminismo, utilizando expresiones como "femibolche" y "muerte al marxismo cultural". Además, compartió imágenes manipuladas del símbolo feminista con contenido sexualizado y vulgar para ridiculizar el movimiento, constituyendo un caso de ciberviolencia y discurso de odio basado en género e ideología.

Algunos casos no responden a categorías ni a dinámicas políticas locales, sino más bien provienen de tendencias o "modas" internacionales. Este es el caso de los ataques registrados hacia los llamados "therians" o personas que se identifican con animales no humanos:

En la página de Facebook "Chiquimula a lo Meme", se publicó una imagen que hacía un llamado a una reunión del colectivo therian en el municipio de Chiquimula. La publicación fue realizada por los administradores de la página dentro de la plataforma de Facebook y, en sí misma, no contenía mensajes ofensivos. Sin embargo, posteriormente varios usuarios que interactuaron con la publicación realizaron comentarios en los que incitaban a la violencia o burla hacia las personas identificadas con el colectivo therian, expresando frases como que "había que cazarlos", "darles bocado" y etiquetando a otros usuarios para burlarse de ellos y relacionándolos con dicho grupo.

En esta ocasión, el ejercicio permitió identificar otras formas de ciberviolencia que hacen uso de la tecnología para irrumpir en la vida privada de las personas. Los casos registrados de este tipo no fueron tan frecuentes como los otros, pero vulneran de forma significativa la esfera privada de las personas y por lo tanto requieren especial atención. Los hechos van desde las estafas individuales y masivas y amenazas por medio de servicios de mensajería instantánea, como Whatsapp y Telegram, hasta el uso de inteligencia artificial para publicar videos falsos de personas diciendo o haciendo algo que nunca dijeron o hicieron. Algunos ejemplos:

En la plataforma de Facebook, un usuario difundió una publicación en la que promocionaba una supuesta oferta para adquirir una Samsung Galaxy Tab A11 por un precio de Q90 quetzales, dirigiendo el mensaje a otros usuarios de la red social con el fin de que realizaran la compra. Para ello, el usuario utilizó una publicación con un trasfondo trágico que buscaba generar confianza e incentivar a las personas a aprovechar la supuesta promoción, indicando que él mismo había realizado la compra. Como medio para concretar la estafa, se incluía un enlace a un formulario de Google Forms donde se solicitaba a los interesados ingresar datos personales y bancarios para acceder a la oferta. La publicación estaba acompañada de una imagen que aparentaba ser una prueba de compra, pero que presentaba indicios de haber sido modificada con herramientas digitales. Además, en los comentarios aparecían cuentas que afirmaban haber recibido el producto, aunque las fotografías mostraban señales de ser falsas y los perfiles que las publicaban parecían cuentas vacías o creadas recientemente, lo que evidencia un posible intento de fraude dentro de la plataforma digital.

El 8 de marzo de 2026, la página de Facebook "Espectador Pananeco" publicó que usuarios de la población a nivel nacional recibieron mensajes mediante WhatsApp haciéndose pasar por el Ministerio de Desarrollo Social solicitando que ingresaran a un enlace y proporcionaran datos personales (número de teléfono, dirección, nombre completo y DPI) y datos bancarios. Esto con el fin de obtener el "bono mujer" de Q800 por el Día de la Mujer para mujeres mayores de 18 años. Expertos en ciberseguridad han advertido que este tipo de plataformas no oficiales funcionan con el dominio de "guatemalabonomujer". Este tipo de estafas son conocidas como phishing y son diseñadas para obtener información sensible de usuarios.

El 6 de mayo de 2025 Prensa Libre publicó un reportaje en el que se detalla una red de estafadores que operaban bajo las empresas KEDA, KMEC y XTRA. Estas empresas buscaban reclutar trabajadores en masa para que estas invirtieran en una estructura piramidal. La dinámica de la estafa consistía en descargar aplicaciones específicas y realizar distintas acciones en Telegram. Entre los departamentos afectados se encuentra San Marcos, sin especificar el municipio. La nota también indica que funcionaban en Honduras.

Un joven gay de 21 años del departamento de Guatemala, fue víctima de un caso de ciberviolencia y extorsión digital. Un individuo masculino, de identidad, edad y lugar de origen desconocido lo contactó inicialmente por vía telefónica y posteriormente a través de WhatsApp, exigiéndole dinero bajo la amenaza de que supuestamente "habían pagado para hacerle daño". Durante la interacción, el agresor también adoptó una conducta de hostigamiento sexual digital, iniciando comentarios de coqueteo hacia la persona que sufrió la ciberviolencia. No existía relación previa entre ambas personas. El agresor sería presuntamente parte de un grupo desconocido de crimen organizado. Tras negarse a cumplir con las exigencias económicas, la víctima bloqueó el número inicial; sin embargo, el agresor continuó el hostigamiento utilizando números adicionales de WhatsApp para enviar mensajes y, posteriormente, imágenes explícitas de sus genitales sin el consentimiento del joven. El incidente ocurrió en una o dos ocasiones y tuvo como finalidad principal la obtención de dinero, implicando además una invasión del espacio personal de la víctima a través de medios digitales. La víctima procedió a bloquear y reportar los números utilizados, así como a presentar una denuncia formal ante el Ministerio Público.

Desde una cuenta de Facebook, aprovechando el anonimato, se creó y difundió una imagen generada con inteligencia artificial que muestra al alcalde de Huehuetenango y a funcionarios municipales entregándose flores amarillas, en alusión a una fecha conmemorativa. La imagen fue publicada en esta red social sin el consentimiento de las personas involucradas, utilizando sus rostros y representación. A partir de la publicación, usuarios realizaron comentarios homofóbicos y ofensivos que afectan la imagen, dignidad y reputación de las personas representadas.

En la plataforma TikTok, la cuenta "sandytorresgt" difundió un video manipulado con inteligencia artificial de la política Sandra Torres, en el cual se le muestra realizando un trend viral: primero baila y luego aparece con un traje de superhéroe mientras continúa bailando. Este contenido fue dirigido al público en general de la red social, y en el espacio de comentarios, varios usuarios reaccionaron negativamente expresando disgusto (como decir que les dio asco verlo) y comparándolo con otros videos similares de figuras públicas también alteradas con IA.

En la red social Facebook, la página "Chiquimula a lo meme" difundió una imagen creada con inteligencia artificial en la que presenta a las dos mujeres transgénero conocidas como Zuleyka y Valentina en un supuesto enfrentamiento de boxeo denominado "la velada del año", con lo cual reaviva una riña pasada ocurrida años atrás en Chiquimula (aproximadamente en 2017). Esta publicación fue dirigida al público de la plataforma, y en los comentarios, diversos usuarios reforzaron el contenido con mensajes que incitan al odio por la identidad de género de las víctimas, críticas a la conducta de la población local y burlas al etiquetar a otras personas insinuando relaciones románticas con ellas.

El día 23 de febrero del 2026 en las redes sociales oficiales de Facebook de la Marimba Orquesta de Fidel Funes dio a conocer que los miembros de la banda estaban siendo víctimas de suplantación de identidad digital en el videojuego Roblox. La cantidad de víctimas fue entre 2 a 10 personas, cuya edad se estima entre 40 y 44 años de género masculino. En este caso no se tiene certeza de quiénes son los atacantes, de dónde son, qué tipo de individuos son o el tamaño del grupo que realizó la violencia, debido a que actuaron de forma anónima y no se puede determinar o identificar a los responsables directos. Esto fue identificado después de que se viralizaron videos de Tik Tok, invitando a los eventos de Roblox.

A estos casos facilitados por la tecnología es necesario agregar el hecho de que el equipo de observación ha notado que conforme ha ido registrando más casos de ciberviolencia en distintas plataformas, los algoritmos de estas plataformas han ido cambiando para ofrecerles más publicaciones similares a las que han registrado. Esto sugiere que los algoritmos mismos facilitan o incluso ejercen directamente la ciberviolencia.

La Tabla 11 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 efímera, 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 prolongados, y que además en todas las dimensiones se documentaron casos que se desconoce dónde encajarían.

Tabla 11. Duración, finalidad y grado de intrusión de los casos registrados por el equipo de Ciberadar, 23 de febrero al 31 de marzo de 2026

Duración	Cantidad de casos	Finalidad	Cantidad de casos	Grado de intrusión	Cantidad de casos
Efímera (1 o 2 veces)	93	Hacerle daño a la persona	91	No intrusiva (se mantuvo en el espacio público)	112
Prolongada (3 o más veces)	27	Obtener algo de la persona o impedir que la persona haga algo	11	Intrusiva (invadió la esfera privada de la persona	9
Se desconoce	8	Se desconoce	26	Se desconoce	7
Total	**128**	**Total**	**128**	**Total**	**128**

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

La Tabla 12 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 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 12. **Tipos de ciberviolencia registrados por el equipo de Ciberadar según tipología basada en la duración, finalidad y grado de intrusión, 23 de febrero al 31 de marzo de 2026**

Efímeras	Cantidad de casos	Porcentaje del total
Utilitaria no intrusiva	4	3%
Utilitaria intrusiva	2	2%
Dirigida no intrusiva	74	58%
Dirigida intrusiva	3	2%
Prolongadas	**Cantidad de casos**	**Porcentaje del total**
Utilitaria no intrusiva	0	0%
Utilitaria intrusiva	2	2%
Dirigida no intrusiva	22	17%
Se desconoce (al menos una dimensión faltante	21	16%
Total	**128**	**100%**

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

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.

Conclusiones

Este informe confirma que los casos de ciberviolencia registrados se configuran predominantemente como un fenómeno de carácter colectivo. La interacción entre múltiples usuarios, muchas veces amparados en el anonimato, genera dinámicas en las que grupos de individuos atacan a personas específicas, amplificando el daño y dificultando la identificación de los responsables. Esto sugiere que la ciberviolencia no puede entenderse únicamente como un conjunto de agresiones individuales, sino como un proceso social mediado por las lógicas propias de las plataformas digitales.

Entre las acciones violentas registradas, los ataques verbales y los discursos de odio ocupan un lugar central. Estos constituyen la forma más extendida de agresión y funcionan como base sobre la cual se articulan otras formas de ciberviolencia más complejas, como la difusión no consentida de contenido, el hostigamiento sexual digital o las amenazas. Esta centralidad evidencia la importancia del lenguaje como medio para ejercer violencia y como mecanismo de escalamiento hacia otras modalidades más intrusivas.

Asimismo, una proporción significativa de los casos documentados se vincula con el contexto político nacional y con estructuras históricas de desigualdad, como el racismo, el sexismo y la discriminación de clase. Esto permite interpretar la ciberviolencia como una extensión de conflictos sociales y políticos en el entorno digital, en donde las tensiones existentes se amplifican por medio de la tecnología y nuevas formas de interacción.

El análisis también muestra otras formas de ciberviolencia no registradas antes, facilitadas por tecnologías emergentes. Casos de manipulación de contenido mediante inteligencia artificial, fraudes digitales y prácticas de extorsión evidencian niveles crecientes de sofisticación y la capacidad de estas tecnologías para intensificar los riesgos y las formas de daño hacia las víctimas.

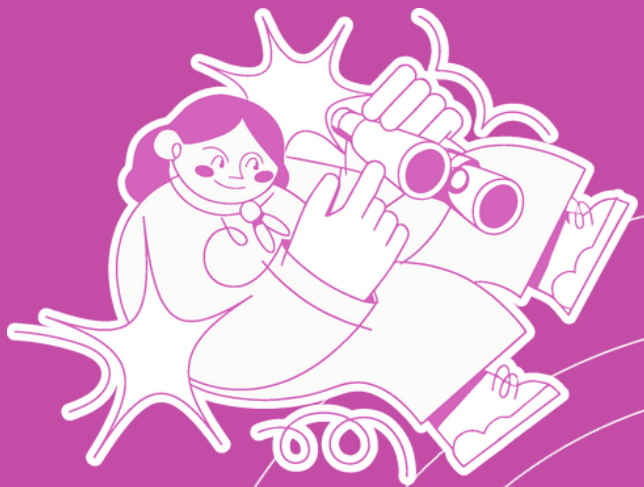
Por otro lado, aunque la mayoría de los casos se desarrolla en el espacio público digital y tiene un carácter efímero, la presencia de casos prolongados e intrusivos revela la existencia de formas de ciberviolencia que trascienden lo visible y afectan directamente la esfera privada de las personas. Estos casos, aunque registrados con menor frecuencia, implican mayores niveles de vulnerabilidad y requieren especial atención.

Finalmente, es importante subrayar que los hallazgos deben interpretarse con cautela. El ejercicio de observación está condicionado por limitaciones inherentes al proceso de monitoreo, incluyendo la selección de plataformas, actores y contenidos, así como restricciones de acceso a ciertos espacios digitales. En este sentido, los resultados permiten identificar patrones relevantes, pero no constituyen una representación exhaustiva del fenómeno.

DIÁLOGOS

ciberadar

Juventudes por espacios digitales seguros



CIBER CIUDADANOS

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