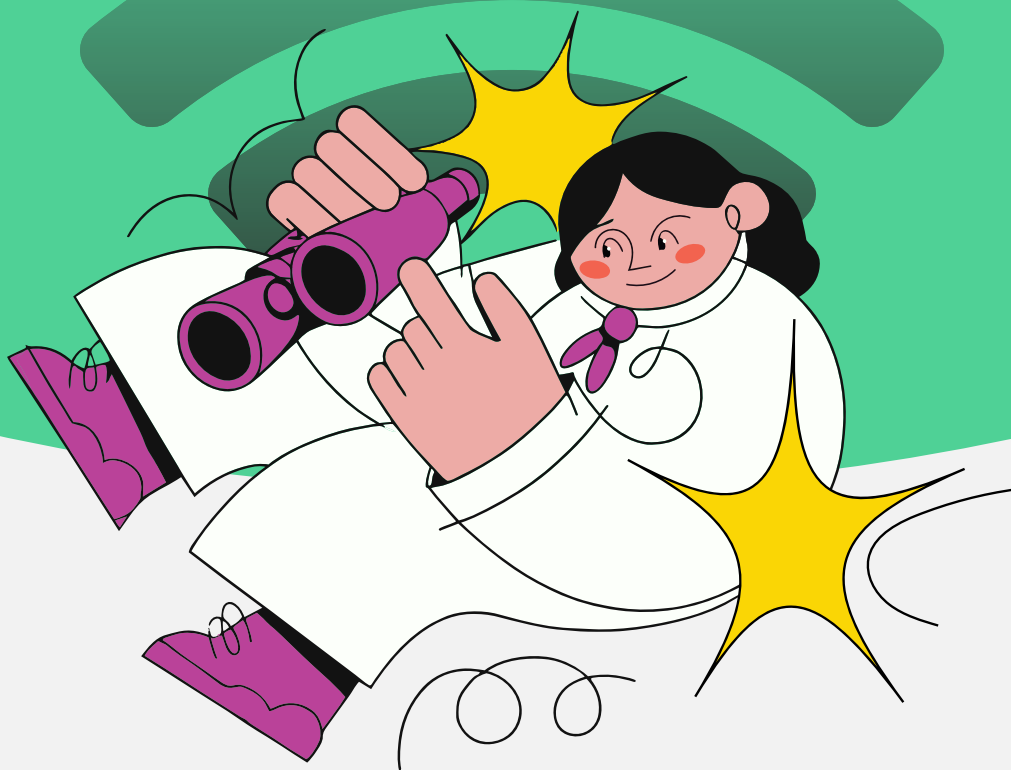


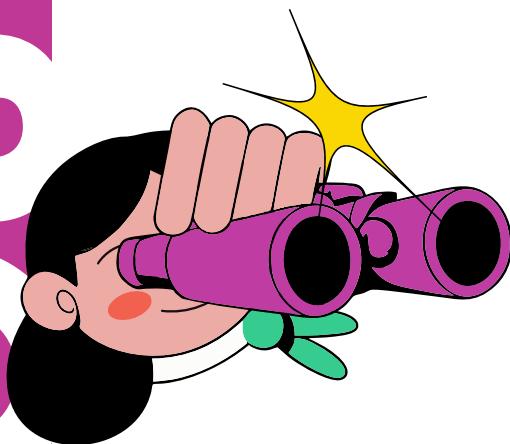
DIÁLOGOS



Ciberviolencia Multidimensional

un abordaje empírico de la violencia digital
en Guatemala

ciberadar
Juventudes por espacios digitales seguros



Autores
Equipo de Ciberadar

Equipo editorial

Walter Corzo, Director Ejecutivo | Daniel Núñez, Director Académico
Karla López, Coordinadora de Investigación
Mayarí Prado, Coordinadora de Comunicación
Pedro Pablo Sánchez, Asistente de Comunicación

Diseño: José Paulo Pérez
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

Esta publicación ha sido elaborada por Diálogos. El análisis y las opiniones contenidas en este documento pertenecen exclusivamente a Diálogos y los autores de cada texto. 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 con fines comerciales requiere autorización previa y por escrito de Diálogos, la cual puede solicitarse 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, *Ciberviolencia multidimensional: un abordaje empírico de la violencia digital en Guatemala* (Ciudad de Guatemala: Asociación Civil Diálogos, octubre de 2026).

El contenido de esta publicación es responsabilidad exclusiva de sus autores y no necesariamente refleja las opiniones o posiciones oficiales de las agencias y organismos cooperantes.

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.

Índice

1. Resumen Ejecutivo	04
2. Construcción del Ciberadar	08
3. Una teoría de partida tridimensional	15
4. Hallazgos y ampliación de la teoría	19
5. Conclusiones	58
6. Recomendaciones	62
7. Anexos	64

1 Resumen Ejecutivo

Ciberadar es un observatorio orientado a identificar, documentar y analizar casos ilustrativos de ciberviolencia en Guatemala, con especial atención a las experiencias que afectan a las juventudes. Su construcción respondió a la necesidad de contar con evidencia que permitiera comprender mejor las distintas formas que puede adoptar la violencia en los entornos digitales, los actores que participan en ella, los espacios en los que ocurre y algunas de sus posibles consecuencias. El observatorio se desarrolló mediante una metodología mixta con predominio cualitativo y a través de un proceso progresivo que combinó una fase exploratoria con grupos focales, la construcción de un marco conceptual, su operacionalización mediante variables observables, el diseño de un sistema de identificación y registro de casos y, finalmente, el análisis y la difusión de la evidencia recopilada.

Como punto de partida, Ciberadar desarrolló una teoría tridimensional para analizar la ciberviolencia a partir de tres características: su finalidad, su duración y su grado de intrusión. La primera distingue entre acciones dirigidas principalmente a causar daño y acciones utilitarias orientadas a obtener algo de la víctima o impedir que realice alguna acción; la segunda diferencia entre agresiones

efímeras y prolongadas; y la tercera entre acciones que se mantienen en espacios públicos digitales y aquellas que invaden la esfera privada. La combinación de estas dimensiones permitió construir ocho tipos ideales de ciberviolencia y ofreció una estructura común para comparar situaciones muy distintas, desde insultos y campañas de desprestigio hasta fraudes, suplantaciones de identidad, hostigamiento sexual y accesos no autorizados.

La observación sistemática se realizó entre el 11 de febrero y el 4 de junio de 2026 y permitió documentar 374 casos. Estos casos no constituyen una muestra aleatoria ni estadísticamente representativa de la ciberviolencia en Guatemala. El sistema fue diseñado deliberadamente para identificar una diversidad de modalidades y situaciones mediante una combinación de muestreos no probabilísticos por conveniencia y máxima variación. Por ello, las frecuencias que presenta este informe describen exclusivamente el conjunto de casos documentados por Ciberadar y no deben interpretarse como estimaciones de la prevalencia de la ciberviolencia en el país. Asimismo, la capacidad de observación estuvo condicionada por las plataformas y espacios accesibles al equipo, por la naturaleza pública o



¹ Este documento fue elaborado con apoyo de inteligencia artificial generativa para tareas de redacción, síntesis, estructuración y edición de texto, bajo supervisión y revisión de miembros del equipo de Diálogos.

privada de las interacciones, por las medidas adoptadas para proteger la seguridad de las personas observadoras, y por los propios sesgos del equipo de observadores.

Dentro de este universo de casos, los ataques verbales y discursos de odio constituyeron la modalidad registrada con mayor frecuencia y representaron el 51% de las menciones de acciones violentas. Les siguieron la difusión no consentida de contenido (15%), el engaño, fraude y manipulación (11%) y la vigilancia, control y acceso no autorizado (11%). Entre los ataques verbales documentados, las menciones más frecuentes correspondieron a difamación, ataques basados en sexo o género, actividad profesional, apariencia física y capacidad intelectual. Los casos muestran, además, que estas categorías pueden superponerse: una misma situación puede combinar amenazas, extorsión, difusión de información, hostigamiento sexual, discriminación y otras formas de agresión.

Uno de los principales hallazgos del observatorio es el carácter colectivo que puede adquirir la ciberviolencia. Aunque las personas individuales constituyeron el principal tipo de víctima identificado, los grupos de individuos representaron la categoría más frecuente entre los victimarios. Los casos documentados muestran cómo publicaciones inicialmente producidas por una persona, página o cuenta pueden ser comentadas, compartidas, modificadas y amplificadas por otros usuarios,

generando dinámicas en las que el daño resulta de la acumulación de múltiples intervenciones. Las plataformas digitales permiten así que una agresión individual pueda transformarse rápidamente en una experiencia colectiva de exposición, señalamiento u hostigamiento.

Un segundo hallazgo es que las agresiones digitales documentadas no pueden comprenderse separadamente de las relaciones sociales y conflictos existentes fuera de Internet. Los casos registrados reflejan desigualdades y formas de discriminación relacionadas con género, orientación sexual, pertenencia étnica y otras características sociales, así como tensiones asociadas con debates políticos, procesos de elección de autoridades, conflictos institucionales y controversias públicas. Los patrones observados por género son ilustrativos: entre los perfiles femeninos, los ataques verbales relacionados con el sexo o género tuvieron un peso particularmente importante, mientras que entre los perfiles masculinos adquirieron mayor relevancia relativa la difamación, los cuestionamientos a la actividad profesional y los ataques relacionados con la orientación sexual. Entre las personas mayas identificadas en los casos, los ataques basados en el origen étnico tuvieron un peso mayor que entre las personas ladinas/mestizas. Estos resultados no permiten estimar el riesgo que enfrenta cada grupo en la población, pero sí muestran cómo desigualdades, estereotipos y relaciones históricas de poder pueden convertirse en recursos para ejercer violencia en los espacios digitales.

Las juventudes ocupan un lugar central en el análisis, aunque las limitaciones de información obligan nuevamente a interpretar los resultados con cautela: en el 60% de los casos no fue posible determinar la edad de la víctima. Entre los casos en los que sí se identificó y específicamente entre las víctimas de 15 a 29 años, los ataques verbales registrados se concentraron principalmente en el sexo o género, la difamación y la apariencia física, que conjuntamente representaron el 58% de las menciones correspondientes a este grupo etario. También se identificaron diferencias según el género: entre los perfiles femeninos jóvenes tuvieron especial peso los ataques basados en sexo o género, mientras que entre los perfiles masculinos jóvenes destacaron la difamación, la apariencia física y la orientación sexual. Más que establecer qué tan frecuente es la ciberviolencia entre las juventudes guatemaltecas, estos casos permiten identificar algunas de las formas que puede adoptar cuando las personas jóvenes son objeto de agresiones digitales.

Un tercer hallazgo es el carácter tecnológicamente dinámico del fenómeno. Facebook fue el espacio donde se registró la mayor cantidad de menciones, seguido por TikTok y X, aunque esta distribución está influida por la accesibilidad y las características del monitoreo y no debe interpretarse necesariamente como una medición del riesgo relativo de cada plataforma. Al mismo tiempo, Ciberadar documentó la incorporación de herramientas de inteligencia artificial a distintas formas

de ciberviolencia. Imágenes y otros contenidos manipulados o generados artificialmente fueron utilizados para ridiculizar, sexualizar, difamar o desacreditar a personas. En ese sentido, la inteligencia artificial reduce las barreras para producir contenidos falsos o manipulados y amplía las posibilidades técnicas disponibles para hacerlo.

Los casos también evidencian que las consecuencias de la ciberviolencia pueden trascender el espacio digital. Cuando fue posible identificar sus efectos, el daño reputacional fue la consecuencia registrada con mayor frecuencia, aunque también se documentaron pérdidas económicas y afectaciones emocionales, psicológicas y sexuales. Sin embargo, en el 57% de las menciones no fue posible determinar las consecuencias experimentadas por las víctimas, por lo que estos impactos probablemente son más difíciles de observar mediante un sistema basado en buena medida en información disponible públicamente. De manera similar, en casi la mitad de las menciones no fue posible establecer cómo respondió la víctima. Entre las respuestas identificadas aparecen la publicación de aclaraciones, las respuestas públicas, el bloqueo o reporte de cuentas y, con menor frecuencia, las acciones legales.

En conjunto, la experiencia de Ciberadar confirma la utilidad de las dimensiones de finalidad, duración e intrusión para clasificar distintas formas de ciberviolencia, pero también muestra la necesidad de ampliar esta perspectiva.

Los hallazgos sugieren incorporar tres elementos adicionales para comprender mejor el fenómeno: su dimensión colectiva, el contexto social y político en el que se produce y el entorno tecnológico que facilita y transforma las posibilidades de agresión. Desde esta perspectiva ampliada, **la ciberviolencia puede entenderse como un proceso social complejo en el que interactúan personas y colectivos, desigualdades y**

conflictos existentes fuera de Internet, y tecnologías que permiten producir, reproducir y amplificar el daño. Más que ofrecer una medición exhaustiva de la ciberviolencia en Guatemala, Ciberadar proporciona una primera cartografía de sus formas y dinámicas y una base conceptual y metodológica sobre la cual continuar construyendo evidencia para informar futuras aproximaciones de política pública.

2 Construcción del Ciberadar

Ciberadar fue concebido como un observatorio orientado a identificar, documentar y analizar casos ilustrativos de ciberviolencia en Guatemala, con especial atención a las experiencias que afectan a juventudes. Su propósito fue generar evidencia que permitiera comprender la diversidad de formas que adopta el fenómeno en el país, las dinámicas mediante las cuales ocurre, los actores involucrados, los espacios digitales en los que se manifiesta y sus posibles consecuencias. En este sentido, Ciberadar se desarrolló mediante una metodología mixta con predominio cualitativo, basada en la identificación sistemática de casos y en su posterior clasificación y análisis.

La construcción del observatorio se desarrolló como un proceso progresivo que articuló **cinco fases**: una fase exploratoria para entender cómo se experimenta y percibe la violencia digital en Guatemala; la construcción de un marco conceptual sobre la ciberviolencia; la operacionalización de dicho marco mediante variables y categorías observables; el diseño e implementación de un sistema de identificación y registro de casos; y el análisis de la información recopilada para identificar patrones y, al mismo tiempo, revisar y refinar la teoría de partida.

La construcción de Ciberadar inició con una **fase exploratoria y participativa** orientada a comprender cómo se experimenta y percibe la violencia en los espacios digitales en Guatemala y a incorporar estas experiencias al diseño del observatorio. Como parte de esta fase se realizaron grupos focales diferenciados con mujeres jóvenes, hombres jóvenes, jóvenes de la diversidad sexual y personal docente. Para la selección de participantes se utilizó una muestra no probabilística por cuotas, buscando incorporar diversidad territorial y de pertenencia a pueblos. En total participaron 31 personas: nueve mujeres jóvenes, ocho hombres jóvenes, cinco jóvenes de la diversidad sexual y nueve docentes.

Los grupos focales tuvieron una cobertura territorial amplia. Las mujeres jóvenes participantes provenían de Guatemala, Chiquimula, Quetzaltenango, Escuintla, Quiché, Jalapa y Sololá; los hombres jóvenes, de Jutiapa, Totonicapán, Quetzaltenango, Jalapa y Escuintla; las juventudes de la diversidad sexual, de Guatemala, Sacatepéquez y Santa Rosa; y el personal docente incluyó participantes de Chiquimula, Escuintla y Huehuetenango. Asimismo, se procuró incorporar diversidad étnica: entre las juventudes participaron personas mayas, ladinas/mestizas y xincas, mientras que entre el personal docente participaron

personas mayas y ladinas/mestizas. Esta composición permitió incorporar al diseño del observatorio experiencias procedentes de diferentes regiones y contextos socioculturales del país.

Los grupos focales cumplieron una doble función. Por una parte, permitieron explorar las percepciones y experiencias de las juventudes respecto de la violencia en los entornos digitales, incluyendo sus distintas manifestaciones, las motivaciones atribuidas a estas acciones, las características de víctimas y perpetradores y las plataformas en las que ocurrían. Por otra, tuvieron un componente explícitamente orientado al diseño de Ciberadar: mediante herramientas de innovación se solicitaron propuestas sobre las características que debía tener un observatorio de ciberviolencia, las plataformas que debía monitorear, las formas mediante las cuales podían recopilarse casos y posibles nombres para la iniciativa. De esta manera, el diseño del observatorio combinó el desarrollo conceptual realizado por el equipo de Diálogos con conocimiento producido a partir de las experiencias de sus potenciales usuarios y de personas jóvenes directamente familiarizadas con las dinámicas de violencia digital.

Esta participación de las juventudes en la construcción del observatorio es coherente con la perspectiva de Juventud, Paz y Seguridad, que reconoce a las personas jóvenes no solamente como posibles víctimas de violencia, sino también como actores con capacidad para producir conocimiento, promover la convivencia pacífica e incidir en los

asuntos que afectan a sus comunidades.

Los grupos focales también contribuyeron a delimitar el universo de situaciones que posteriormente debía ser capaz de registrar Ciberadar. Las personas participantes identificaron un conjunto amplio de violencias que incluía, entre otras, violencia de género, discursos de odio y discriminación, racismo, ciberacoso y ciberbullying, sextorsión, difusión de contenido íntimo sin consentimiento, suplantación y robo de identidad, phishing, extorsión, grooming y otras formas de engaño y manipulación. Asimismo, señalaron que estas violencias no debían entenderse como fenómenos exclusivamente digitales, pues frecuentemente reproducen desigualdades y formas de violencia existentes fuera de internet y pueden producir consecuencias emocionales, psicológicas, sociales y económicas en la vida de las víctimas. Estas observaciones contribuyeron a que el diseño posterior de Ciberadar no se limitara a una única modalidad de agresión, sino que buscara construir un instrumento suficientemente amplio para registrar formas heterogéneas de ciberviolencia.

La **segunda fase** consistió en delimitar conceptualmente el fenómeno que sería observado. Para fines de Ciberadar, la ciberviolencia fue definida como “el uso de tecnologías de la información y la comunicación (TIC) para causar, directa o indirectamente, daño material, reputacional, emocional, psicológico, sexual o físico a una persona o grupo de personas.” A partir de la revisión conceptual y de los hallazgos obtenidos

durante la fase exploratoria, el equipo de Diálogos formuló como teoría de partida que las distintas manifestaciones de ciberviolencia podían comprenderse a partir de tres dimensiones: la finalidad de la acción, su duración y su grado de intrusión en la esfera privada de la persona. La combinación de estas dimensiones permitió construir una tipología inicial de ocho formas de ciberviolencia, que se desarrolla con mayor detalle en la sección siguiente.

La **tercera fase** consistió en convertir este marco conceptual en un instrumento que permitiera observar y analizar empíricamente los casos. Para ello se diseñó un cuestionario digital basado en principios del Quantitative Discourse Analysis (QDA)², técnica que permite transformar información textual en variables susceptibles de clasificación y análisis sistemático. El instrumento se estructuró alrededor de la tríada básica de quién hizo qué a quién, complementada con información contextual acerca del medio utilizado, el momento y el lugar en que ocurrió el hecho (quién hizo qué a quién, por qué medio, cuándo y dónde). De esta manera, cada caso podía ser descompuesto en un conjunto común de variables y posteriormente comparado con otros casos.

El cuestionario incorporó variables para identificar, entre otros aspectos, el tipo de acción violenta, las características de las víctimas y victimarios, las plataformas

involucradas y las características multidimensionales de la ciberviolencia. Las acciones fueron clasificadas inicialmente en categorías como ataques verbales y discursos de odio; amenazas; hostigamiento sexual digital; engaño, fraude y manipulación; vigilancia, control y acceso no autorizado; y difusión no consentida de contenido³. El instrumento también permitió registrar más de una acción, plataforma o actor dentro de un mismo caso, reconociendo que los episodios de ciberviolencia pueden involucrar simultáneamente distintas conductas y desarrollarse a través de varios espacios digitales⁴.

Las características de las víctimas y victimarios se registraron a partir de la información disponible en la publicación, el perfil o la fuente consultada. El género corresponde al género percibido del perfil (nombre, fotografía, autodescripción o referencias en la publicación o en medios de comunicación). Solo se registró como “Persona trans” a quienes habían expresado públicamente su identidad de género, en sus propias publicaciones o en medios de comunicación. El pueblo de origen y la edad se registraron únicamente cuando la persona los declaraba o aparecían de forma explícita en la publicación o en medios de comunicación.

La **cuarta fase** fue la construcción del sistema de identificación y registro de casos. Ciberadar combinó fuentes



² Ver: Roberto Franzosi (2010). *Quantitative Narrative Analysis*. Quantitative Applications in the Social Sciences. Thousand Oaks, CA: SAGE Publications, Inc.

³ Para las definiciones de cada una de estas categorías, ver Anexo 1.

⁴ Ver Anexo 2.

directas e indirectas de información. Las fuentes directas correspondieron principalmente a casos identificados mediante la observación de publicaciones, páginas, grupos públicos e influencers en redes sociales. Las fuentes indirectas incluyeron información publicada por medios de comunicación y notas de prensa, casos conocidos por terceros y reportados al equipo de observación, así como información recibida mediante un buzón de registro incorporado en la página web de Ciberadar. Este último fue diseñado para que cualquier persona pudiera informar sobre un posible caso que hubiera presenciado o del cual hubiera tenido conocimiento. El buzón tuvo una función de identificación y documentación y no constituyó un

mecanismo de denuncia penal. Para implementar el monitoreo se conformó un equipo de seis jóvenes observadores. Cada integrante tuvo asignados determinados departamentos, plataformas digitales, influencers, páginas, grupos y medios de comunicación digitales. Esta distribución fue acordada entre el equipo de Diálogos y el equipo de observación tomando en consideración la disponibilidad de sus integrantes y su conocimiento de las dinámicas territoriales y de las distintas plataformas. La distribución se presenta en la Tabla 1.

La observación sistemática se desarrolló entre el 11 de febrero y el 4 de junio de 2026. Sin embargo, la unidad de

Tabla 1. Distribución de observadores por departamentos y redes sociales

OBSERVADOR	DEPARTAMENTOS	REDES SOCIALES
Coordinadora	Chiquimula, Zacapa Izabal, Petén	Facebook, Instagram, TikTok
Obserador 1	San Marcos, Quetzaltenango Totonicapán, Retalhuleu	Facebook, Instagram, TikTok, X/Twitter
Obserador 2	Guatemala, Sacatepéquez, Chimaltenango, Sololá	X/Twitter, Instagram, Facebook, Youtube
Obserador 3	Alta Verapaz, Baja Verapaz Quiché	Instagram, TikTok FreeFire, Discord
Obserador 4	Escuintla, Suchitepéquez, Huehuetenango	TikTok, Instagram Facebook
Obserador 5	Jutiapa, Jalapa, Santa Rosa El Progreso	Whatsapp, Instagram, Facebook

análisis —el hecho descompuesto en las variables quién hizo qué a quién, por qué medio, cuándo y dónde— no estuvo restringida a hechos ocurridos durante ese período: también se documentaron casos anteriores cuando estos permitían comprender modalidades particularmente relevantes de ciberviolencia. El período señalado corresponde, por tanto, al período de observación y registro, y no necesariamente a la fecha de ocurrencia de todos los casos contenidos en la base de datos.

El proceso de observación tampoco buscó producir una muestra aleatoria o estadísticamente representativa. El objetivo fue construir deliberadamente un conjunto diverso de casos que permitiera explorar las distintas formas que adopta la ciberviolencia. Cada observador podía registrar un máximo de diez casos por semana y se priorizó la diversidad de situaciones por encima de su cuantificación. Además de registrar los casos encontrados durante el monitoreo ordinario, el equipo realizó búsquedas dirigidas a partir de vacíos o patrones identificados durante el proceso. Particular atención recibieron los casos que involucraban una invasión de la esfera privada de las personas; aquellos orientados a obtener algo de la víctima o impedir alguna de sus actividades; los casos con consecuencias particularmente graves; y aquellos en los que intervenían tecnologías emergentes, incluida la inteligencia artificial. En ese sentido, la técnica de muestreo utilizada fue no probabilística e incluyó un muestreo por

conveniencia y un muestreo de máxima variación. Esta estrategia permitió que la observación evolucionara conforme aumentaba el conocimiento acumulado sobre el fenómeno.

La implementación tuvo, por tanto, un carácter iterativo. A cada integrante se le asignó un código único para facilitar el seguimiento de los registros y una de las observadoras asumió funciones de coordinación. La comunicación cotidiana entre el equipo de observación y el equipo de Diálogos se realizó mediante un grupo de WhatsApp creado específicamente para el proyecto. Adicionalmente, se realizaron reuniones virtuales semanales en las que se discutían los casos identificados, se resolvían dudas de clasificación, se identificaban nuevas modalidades de ciberviolencia y se revisaba el funcionamiento del instrumento. Como resultado de este proceso, el cuestionario fue ajustado durante la implementación para corregir problemas de registro, precisar categorías y responder a situaciones que no habían sido anticipadas durante su diseño inicial.

Finalmente, en la **quinta fase**, la información recopilada fue sistematizada para realizar análisis descriptivos de los casos y explorar patrones entre las distintas variables. Se analizaron las acciones violentas registradas, los perfiles de víctimas y victimarios, el género, la edad y el pueblo de origen cuando esta información estaba disponible, las plataformas utilizadas, las respuestas de las víctimas, las consecuencias

identificadas y la distribución de los casos según las dimensiones de finalidad, duración e intrusión. Debido a que un mismo caso podía contener múltiples acciones, actores o plataformas, algunos análisis se realizaron sobre **menciones** y no exclusivamente sobre el número de casos. Esta distinción permite representar mejor la complejidad de episodios en los que convergen distintas modalidades de violencia.

El proceso tuvo además una dimensión inductiva. La teoría tridimensional funcionó como punto de partida para organizar la observación, pero no como un esquema cerrado. Los casos registrados permitieron contrastar las categorías iniciales con situaciones empíricas y reconocer elementos que no habían sido plenamente considerados al inicio. De esta manera, la relación entre teoría y evidencia fue bidireccional: el marco conceptual orientó qué observar y cómo clasificarlo, mientras que la observación permitió revisar y ampliar la comprensión inicial de la ciberviolencia. Cómo se desarrolla posteriormente en el informe, este proceso permitió identificar con mayor claridad el carácter colectivo de algunas agresiones, la relación de la ciberviolencia con dinámicas políticas y desigualdades sociales más amplias, y la creciente importancia de tecnologías como la inteligencia artificial.

Los resultados deben interpretarse tomando en cuenta el carácter exploratorio del observatorio. Ciberadar no constituye una muestra estadísticamente representativa de la ciberviolencia en

Guatemala, por lo que las frecuencias registradas no deben interpretarse como estimaciones de prevalencia del fenómeno en la población. La cobertura depende de los espacios digitales observados, de los horarios de monitoreo y de la posibilidad de acceder de manera segura a determinadas plataformas y comunidades, y de los propios sesgos del equipo de observación. Asimismo, por razones de seguridad, el equipo no ingresó a algunos espacios privados o potencialmente riesgosos. Los hallazgos deben entenderse, en consecuencia, como evidencia sobre formas, patrones y dinámicas de ciberviolencia identificadas durante el ejercicio con una muestra determinada, y no como una medición exhaustiva de su magnitud en Guatemala.

En términos de comunicación y difusión, el proyecto Ciberadar desarrolló distintas acciones orientadas a divulgar tanto el proceso de construcción del observatorio como los hallazgos generados durante el monitoreo. Como parte de este esfuerzo, se publicaron cuatro informes que presentaron los resultados del monitoreo de la ciberviolencia y, de manera complementaria, cuatro infografías que permitieron comunicar de forma sintética y accesible los principales hallazgos conforme estos fueron surgiendo. Previamente al inicio de estas publicaciones periódicas, también se elaboraron y difundieron algunas piezas comunicativas basadas en información obtenida durante los grupos focales exploratorios, lo que permitió comenzar a visibilizar algunas de las experiencias y patrones identificados en la etapa inicial

del proyecto. Asimismo, Ciberadar realizó un evento de lanzamiento en el que se presentó públicamente el observatorio y se explicaron su metodología, la teoría de partida, sus objetivos y componentes, así como algunos de los resultados preliminares obtenidos. El evento se desarrolló de manera presencial y fue transmitido simultáneamente mediante

redes sociales, ampliando así su alcance a audiencias que no pudieron participar presencialmente. En conjunto, estas acciones permitieron que la comunicación acompañara las distintas etapas del proyecto, desde la exploración inicial y el lanzamiento del observatorio hasta la difusión progresiva de los resultados generados por el monitoreo.



Una teoría de partida tridimensional

La **teoría tridimensional de la ciberviolencia**, desarrollada por Diálogos, parte de la premisa de que las distintas manifestaciones de violencia en los entornos digitales no pueden comprenderse únicamente a partir de la conducta específica que ejecuta el agresor —por ejemplo, una amenaza, un insulto o la difusión no consentida de contenido—, sino que también es necesario considerar la lógica que orienta la agresión, la forma en que esta se desarrolla en el tiempo y el grado en que invade la esfera privada de la víctima. Desde esta perspectiva, la teoría propone un marco analítico basado en tres dimensiones complementarias: **la finalidad, la duración y el nivel de intrusión**. Estas dimensiones permiten clasificar y comparar casos muy diversos de ciberviolencia, identificar patrones comunes y comprender mejor la experiencia de las víctimas, al tiempo que ofrecen una base conceptual para el diseño de estrategias de prevención, atención e investigación.

La primera dimensión corresponde a la **finalidad** de la agresión. En este eje se distingue entre acciones dirigidas y utilitarias. Las acciones dirigidas tienen como propósito principal producir un daño sobre una persona o un grupo específico. Este daño puede manifestarse en forma de

intimidación, humillación, hostigamiento, silenciamiento, discriminación o afectación de la reputación, sin que el agresor busque necesariamente obtener un beneficio adicional. Se trata de actos cuyo objetivo es la víctima misma. En contraste, las acciones utilitarias utilizan la violencia como un medio para alcanzar otro fin. En estos casos, el propósito principal consiste en obtener un recurso, una ventaja o un beneficio, como dinero mediante extorsión, información personal mediante fraude o phishing, acceso a cuentas digitales, imágenes íntimas o cualquier otro activo que pueda ser explotado posteriormente. Aunque ambas categorías pueden generar consecuencias similares para las víctimas, distinguir analíticamente entre ellas resulta importante para comprender las motivaciones de los agresores y desarrollar respuestas institucionales diferenciadas.

La segunda dimensión se refiere a la **duración** de la violencia. La teoría distingue entre acciones efímeras y prolongadas. Las primeras corresponden a hechos aislados o de corta duración, que ocurren en uno o pocos episodios y cesan sin continuidad aparente. Un insulto publicado durante una discusión, un intento único de fraude o la difusión

puntual de un rumor constituyen ejemplos de esta categoría. Las acciones prolongadas, por el contrario, implican una continuidad temporal y se caracterizan por la repetición o persistencia de las conductas violentas. En estos casos, la violencia deja de ser un evento aislado para convertirse en un proceso sostenido que puede extenderse durante días, semanas o incluso meses. El acoso sistemático, las campañas coordinadas de hostigamiento, la persecución reiterada de una persona en distintas plataformas o la vigilancia constante son ejemplos de esta modalidad. Incorporar la duración como dimensión analítica permite reconocer que el impacto de la ciberviolencia depende no solo de la gravedad de cada acción individual, sino también de su persistencia y acumulación en el tiempo.

La tercera dimensión corresponde al **nivel de intrusión** de la agresión. Este eje diferencia entre acciones no intrusivas e intrusivas. Las primeras se desarrollan principalmente en espacios públicos o abiertos y no requieren acceder directamente a la esfera privada de la víctima. Entre ellas se encuentran los insultos en publicaciones abiertas, los comentarios discriminatorios, la difusión de rumores en redes sociales o las campañas públicas de desprestigio. Aunque estas acciones pueden tener

consecuencias importantes para la reputación, la salud mental y la participación pública de las víctimas, no implican necesariamente una vulneración de su privacidad. Las acciones intrusivas, en cambio, suponen un acceso o una intervención directa sobre el ámbito privado de la persona. Esto incluye el acceso no autorizado a cuentas o dispositivos, la vigilancia digital, la obtención de información personal mediante engaño, el control de comunicaciones privadas, la difusión de contenido íntimo sin consentimiento o cualquier otra conducta que invada la esfera personal de la víctima. Esta dimensión resulta especialmente relevante porque la intrusión suele incrementar significativamente la sensación de vulnerabilidad, el riesgo de revictimización y la dificultad para recuperar el control sobre la propia identidad digital.

La combinación de estas tres dimensiones da lugar a **ocho tipos ideales de ciberviolencia**, producto de la intersección entre acciones dirigidas o utilitarias, efímeras o prolongadas, e intrusivas o no intrusivas.

Tabla 2. Tipos de ciberviolencia según su finalidad, duración y grado de intrusión

Tipo de ciberviolencia	Finalidad	Duración	Intrusión	Descripción
Dirigida efímera no intrusiva	Hacer daño	Efímera	No intrusiva	Agresión puntual realizada en un espacio público digital con la finalidad de causar daño a una persona o grupo.
Dirigida efímera intrusiva	Hacer daño	Efímera	Intrusiva	Agresión puntual orientada a causar daño que invade la esfera privada de la víctima.
Dirigida prolongada no intrusiva	Hacer daño	Prolongada	No intrusiva	Agresión reiterada orientada a causar daño que se desarrolla en espacios públicos digitales.
Dirigida prolongada intrusiva	Hacer daño	Prolongada	Intrusiva	Agresión reiterada orientada a causar daño que invade la esfera privada de la víctima.
Utilitaria efímera no intrusiva	Obtener algo o impedir una acción	Efímera	No intrusiva	Acción puntual realizada en un espacio público digital para obtener algo de la víctima o impedir que haga algo.
Utilitaria efímera intrusiva	Obtener algo o impedir una acción	Efímera	Intrusiva	Acción puntual que invade la esfera privada para obtener algo de la víctima o impedir que haga algo.
Utilitaria prolongada no intrusiva	Obtener algo o impedir una acción	Prolongada	No intrusiva	Acción reiterada desarrollada en espacios públicos digitales para obtener algo de la víctima o impedir que haga algo.
Utilitaria prolongada intrusiva	Obtener algo o impedir una acción	Prolongada	Intrusiva	Acción reiterada que invade la esfera privada para obtener algo de la víctima o impedir que haga algo.

Estos tipos no pretenden describir categorías rígidas ni mutuamente excluyentes, sino ofrecer un marco conceptual que facilite el análisis comparado de los casos y permita identificar regularidades entre formas de violencia aparentemente distintas. Un mismo caso puede evolucionar de un tipo a otro conforme cambian sus características; por ejemplo, una agresión inicialmente efímera puede convertirse en prolongada si el hostigamiento continúa, o una acción no intrusiva puede transformarse en intrusiva cuando el agresor obtiene acceso a información privada de la víctima.

En conjunto, la teoría tridimensional constituye una propuesta para

comprender la ciberviolencia más allá de la descripción de conductas aisladas. Al incorporar simultáneamente las motivaciones del agresor, la temporalidad de la violencia y el grado de invasión de la privacidad, este enfoque permite capturar mejor la complejidad del fenómeno y generar categorías analíticas útiles tanto para la investigación como para la formulación de políticas públicas. Asimismo, proporciona una base conceptual para el trabajo del Observatorio Ciberadar, facilitando la clasificación sistemática de casos, la identificación de patrones emergentes y el desarrollo de respuestas más específicas frente a las distintas formas que adopta la violencia en los entornos digitales.

4 Hallazgos y ampliación de la teoría

Las tres dimensiones de la teoría de partida —finalidad, duración y grado de intrusión— permitieron clasificar los casos registrados en ocho tipos ideales y ofrecieron un marco conceptual útil para ordenar empíricamente la observación y las distintas manifestaciones de la violencia en línea. Sin embargo, el análisis sistemático de los casos documentados por Ciberadar durante el período de estudio permitió identificar elementos que no podían explicarse únicamente mediante estas tres dimensiones y que, por tanto, enriquecen y amplían la teoría inicial. En particular, los hallazgos muestran que **la ciberviolencia debe entenderse también como un fenómeno colectivo, contextual y tecnológicamente dinámico.**

Los resultados que se presentan a continuación permiten desarrollar este argumento. Primero se examinan las principales formas de ciberviolencia encontradas durante el monitoreo. Posteriormente se analiza quiénes participan en estos procesos y se muestra la importancia de las dinámicas colectivas. En tercer lugar, se examina cómo las agresiones digitales reproducen conflictos, desigualdades y relaciones de poder existentes fuera de internet. Finalmente, se analiza el papel de las plataformas y de las nuevas tecnologías, las respuestas de las víctimas y las consecuencias registradas. Este recorrido permite regresar, al final de la sección, a las tres dimensiones de la teoría de partida y valorar tanto su utilidad como los elementos que deben incorporarse para ampliar su capacidad explicativa.

★ Las formas que adopta la ciberviolencia

La Tabla 3 muestra que la ciberviolencia documentada por Ciberadar durante el período analizado estuvo dominada por los ataques verbales y los discursos de odio, que representaron la mitad (51%) de todas las acciones violentas registradas. Esta proporción confirma que la violencia digital registrada se manifiesta principalmente mediante agresiones dirigidas a desacreditar, humillar o excluir a las personas a través del lenguaje, más que mediante formas de violencia que requieren un mayor nivel de sofisticación técnica. En un segundo nivel aparecen la difusión no consentida

de contenido (15%), el engaño, fraude y manipulación (11%) y la vigilancia, control y acceso no autorizado (11%), lo que evidencia que una proporción importante de los casos documentados trasciende la agresión verbal e implica vulneraciones directas a la privacidad y la seguridad digital de las víctimas. En contraste, las amenazas (5%) y las formas más específicas de violencia, como el hostigamiento sexual digital (6%) aparecen con menor frecuencia.

Estos resultados muestran que la violencia verbal constituye una de las principales manifestaciones de la ciberviolencia registrada por Ciberadar, aunque una parte importante de los casos incorpora también modalidades de agresión más invasivas. Además, las categorías no necesariamente representan hechos independientes, ya que un mismo episodio puede combinar varias acciones violentas.

Tabla 3. Menciones de acciones violentas registradas por el equipo de Ciberadar, del 11 de febrero al 4 de junio 2026

Tipo de acción violenta	Frecuencia	% del total de menciones
Ataques verbales y/o discursos de odio	272	51%
Difusión no consentida de contenido	83	15%
Engaño, fraude y manipulación	61	11%
Vigilancia, control y acceso no autorizado	58	11%
Hostigamiento sexual digital	34	6%
Amenazas	29	5%
Total	537	100%

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

Caso ilustrativo.

Un caso documentado por Ciberadar muestra cómo distintas modalidades de ciberviolencia pueden combinarse y

escalar dentro de una misma situación. En febrero de 2026, un joven de 21 años recibió llamadas y mensajes de un desconocido que le exigía dinero bajo la

amenaza de que habían pagado para hacerle daño. Después de que la víctima bloqueara el número, el agresor continuó contactándolo desde otros números a través de WhatsApp y comenzó además a enviarle imágenes sexuales explícitas sin su consentimiento. El caso combina extorsión, amenazas, hostigamiento persistente y hostigamiento sexual digital, y muestra que las categorías utilizadas por Ciberadar no necesariamente representan hechos independientes, sino dimensiones que pueden coexistir dentro de un mismo episodio de violencia.

Caso ilustrativo.

Ciberadar también documentó modalidades de ciberviolencia orientadas a obtener información o recursos económicos mediante engaño. En un caso registrado en Facebook se difundió una supuesta promoción para adquirir una tableta Samsung Galaxy Tab A11 por Q90. La publicación utilizaba una historia diseñada para generar confianza y afirmaba que otras personas ya habían aprovechado la oferta. Para concretar la supuesta compra, se remitía a los usuarios a un formulario de Google Forms en el que se solicitaban datos personales y bancarios. El caso muestra cómo el engaño digital puede combinar estrategias de persuasión, suplantación de promociones comerciales y recopilación fraudulenta de información sensible, transformando el entorno digital en un mecanismo para obtener beneficios económicos a costa de las potenciales víctimas.

Dentro de los ataques verbales también

se observan patrones definidos. La difamación constituye el tipo más frecuente (16%), seguida por los ataques o insultos basados en el sexo o género (15%), la actividad profesional (14%), la apariencia física (14%) y la capacidad intelectual (12%). En conjunto, estas cinco categorías representan poco más del 71% de todas las menciones registradas. También destacan, aunque con una frecuencia menor, los ataques basados en la ideología política (9%), el origen étnico (7%) y la orientación sexual (5%). En contraste, las agresiones relacionadas con la posición socioeconómica (3%), la nacionalidad o país de origen (1%) y la religión (1%), aparecen con mucha menor frecuencia.

En conjunto, estos datos muestran que los ataques verbales documentados por Ciberadar se concentran principalmente en la descalificación de la persona y su reputación, así como en características identitarias o atributos fácilmente utilizados para dirigir una agresión, particularmente el sexo o género, la actividad profesional, la apariencia física y la capacidad intelectual. Al mismo tiempo, la presencia de ataques relacionados con la ideología política, el origen étnico y la orientación sexual evidencia que una parte relevante de la violencia verbal documentada también se articula alrededor de identidades y posiciones sociales que pueden convertirse en marcadores de confrontación, discriminación o estigmatización en los espacios digitales.

Tabla 4. Menciones de tipos de ataques verbales y/o discursos de odio registrados por el equipo de Ciberadar, del 11 de febrero al 4 de junio de 2026

Tipo de ataque verbal y/ o discurso de odio	Frecuencia	% del total de menciones
Difamación	80	16%
Ataque verbal o insulto basado en el sexo/género	76	15%
Ataque verbal o insulto basado en actividad profesional	74	14%
Ataque verbal o insulto basado en la apariencia física	73	14%
Ataque verbal o insulto basado en la capacidad intelectual	62	12%
Ataque verbal o insulto basado en la ideología política	46	9%
Ataque verbal o insulto basado en el origen étnico	38	7%
Ataque verbal o insulto basado en la orientación sexual	27	5%
Ataque verbal o insulto basado en la posición socioeconómica	17	3%
Ataque verbal o insulto basado en nacionalidad/ país de origen	7	1%
Ataque verbal o insulto basado en religión	4	1%
Otros	8	2%
Total	512	100%

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

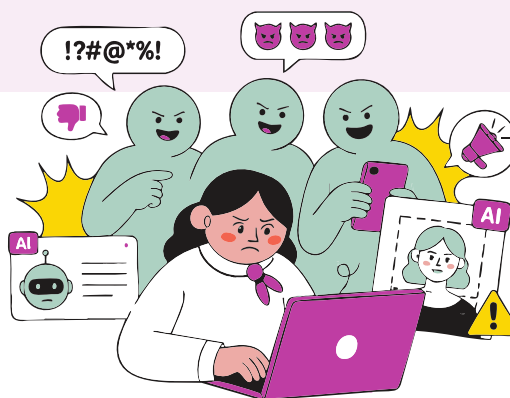
Caso ilustrativo.

La cuenta de X *El Republicano* publicó señalamientos contra Rodolfo Chang, candidato a rector de la Universidad de San Carlos de Guatemala, afirmando que recibía financiamiento de China y que mantenía vínculos con dirigentes de China y Corea del Norte. La publicación fue acompañada por una imagen manipulada mediante inteligencia artificial en la que Chang aparecía junto a Xi Jinping y Kim Jong-un. El caso constituye un ejemplo de difamación en el que se combinan acusaciones dirigidas a desacreditar públicamente a una persona con el uso de contenido manipulado para reforzar su aparente veracidad.

Caso ilustrativo.

En una publicación de Facebook de *Prensa Comunitaria* se difundió un videomensaje de Mariel Molina, integrante de la Red Multicultural de Mujeres Trans (REDMUTRANS), quien participó en una marcha realizada en Alta Verapaz en el marco del 8 de marzo para visibilizar a las mujeres trans. En los comentarios, algunos usuarios cuestionaron su identidad de género y afirmaron que las mujeres trans no son mujeres, mientras otros dirigieron ataques contra su apariencia física y su origen étnico. El caso muestra cómo los ataques verbales pueden combinar y entrelazar distintas formas de discriminación, como la transfobia y el racismo, al convertir las características personales e identitarias de una misma persona, en recursos para su descalificación pública.

★ La dimensión colectiva de la ciberviolencia



Un primer elemento que amplía la teoría inicial es el carácter colectivo que adquiere una parte importante de la ciberviolencia. La teoría de partida permitía distinguir las agresiones según su finalidad, duración e intrusión, pero no consideraba explícitamente el número y tipo de actores que intervienen en la

producción y amplificación del daño.

Los datos muestran que la ciberviolencia registrada se dirige principalmente contra personas individuales, quienes representan el 58% de las víctimas identificadas. Los grupos de individuos constituyen cerca de un tercio de los

casos (32%), mientras que las entidades u organizaciones representan únicamente el 9%. Del lado de los victimarios, la distribución presenta un patrón diferente: los grupos de individuos constituyen la categoría más frecuente, con el 55% de los casos, mientras que los individuos representan el 22%. En un 23% de los casos se desconoce la identidad o naturaleza del victimario, y las entidades u organizaciones representan solamente el 1%.

Este contraste muestra una característica importante de la ciberviolencia registrada por Ciberadar: mientras la victimización

se concentra principalmente en personas individuales, la agresión presenta un marcado componente colectivo. En otras palabras, una proporción considerable de los casos corresponde a situaciones en las que múltiples personas participan en la producción o amplificación del daño dirigido contra una persona. Este hallazgo permite incorporar a la teoría inicial una dimensión adicional relacionada con la configuración de los actores involucrados y, particularmente, con la capacidad de los entornos digitales para transformar una agresión inicialmente individual en una dinámica colectiva.

Tabla 5. Víctimas y victimarios de ciberviolencia reportados por el equipo de Ciberadar, del 11 de febrero al 4 de junio 2026

Víctima	Cantidad	% del total	Victimarios	Cantidad	% del total
Individuo	216	58%	Grupo de individuos	204	55%
Grupo de individuos	119	32%	Se desconoce	85	23%
Entidad u organización	34	9%	Individuo	82	22%
Se desconoce	5	1%	Entidad u organización	3	1%
Total	374	100%	Total	374	100%

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

El cruce entre víctimas y victimarios permite observar esta dinámica con mayor precisión. La combinación predominante corresponde a grupos de individuos que agreden a otros individuos, con 110 casos registrados, seguida por individuos que atacan a personas individuales, con 57 casos. En conjunto, estas dos modalidades concentran la mayor parte de los registros. En términos generales, la Tabla 6 confirma que la violencia digital documentada por Ciberadar tiene un carácter predominantemente colectivo, aunque las acciones individuales representan un componente importante que también merece atención.

Tabla 6. Casos según tipo de víctima y victimario registrados por el equipo de Ciberadar, del 11 de febrero al 4 de junio 2026

Víctima	Victimario				
	Grupo de individuos	Individuo	Se desconoce	Entidad u organización	Total general
Individuo	110	57	49	0	216
Grupo de individuos	80	13	23	3	119
Entidad u organización	13	11	10	0	34
Se desconoce	1	1	3	0	5
Total	204	82	85	3	374

Esta dinámica coincide con lo señalado por la literatura especializada en el tema. Keats⁵, por ejemplo, sostiene que la violencia en línea puede escalar rápidamente hacia formas de agresión colectiva conocidas como *cyber mobs* o “ciberturbas”, en las que múltiples personas, a menudo desconocidas entre sí, se suman al ataque contra una

víctima e incluso compiten por emitir los comentarios más ofensivos o humillantes. El daño no depende únicamente del contenido original, sino también del efecto acumulativo de la participación de múltiples actores, quienes además pueden no sentirse responsables individualmente porque cada uno contribuye sólo parcialmente al ataque.



⁵ Danielle Keats Citron, *Hate Crimes in Cyberspace*, Cambridge, MA: Harvard University Press, 2014, p. 5.

La dimensión colectiva de la ciberviolencia ayuda a explicar por qué algunas agresiones alcanzan una intensidad y persistencia mucho mayores que otras y por qué determinadas víctimas experimentan procesos de hostigamiento que trascienden el comportamiento de un único agresor. El hallazgo obliga, por tanto, a ampliar una conceptualización de la ciberviolencia centrada exclusivamente en la relación entre un agresor y una víctima.

En Guatemala, la dimensión colectiva puede adoptar distintas formas. En algunos casos, el equipo del Ciberadar detectó páginas y cuentas que funcionan como espacios desde los cuales se inicia o articula el ataque. En otros, usuarios que no necesariamente mantienen vínculos entre sí se incorporan progresivamente a una agresión iniciada por otra persona. La participación puede consistir en insultar directamente, compartir contenido, amplificar publicaciones mediante comentarios o reacciones, producir nuevos contenidos ofensivos o reforzar socialmente la agresión mediante mecanismos de aprobación.

Caso ilustrativo.

En la página de Facebook del medio Noticias De Impacto Guatemala, diversos usuarios, tanto hombres como mujeres, realizaron comentarios ofensivos dirigidos a una joven del municipio de Ipala, luego de que se publicara una nota informando que la joven, quien había sido reportada como desaparecida, fue localizada sana y salva. A través de la sección de

comentarios, los usuarios difundieron mensajes y memes de índole sexual en los que cuestionaban su virtud y sugerían que su desaparición estaba relacionada con actividad sexual, generando críticas y burlas contra la joven después de difundirse la información en dicha página.

Caso ilustrativo.

Entre el 27 de febrero y el 1 de marzo de 2026, la página de Facebook *pachuco panarra* realizó una serie de 13 publicaciones en las que expuso públicamente a 26 personas —14 mujeres y 12 hombres— del municipio de Santa Catarina Mita, Jutiapa. Las publicaciones mostraban a estas personas bajo el mensaje “infieles Catocha”, señalándolas públicamente en relación con supuestas infidelidades. En lugar de tratarse de una publicación aislada dirigida contra una sola persona, la página difundió este tipo de contenido de manera reiterada durante varios días, convirtiendo la exposición de personas de la comunidad en una práctica sostenida. El caso resulta ilustrativo de una dinámica de ciberviolencia basada en la exposición y el señalamiento público de aspectos relacionados con la vida íntima y las relaciones interpersonales.

Caso ilustrativo.

En Concepción Las Minas, Chiquimula, una cuenta de TikTok dedicada a “quemar” públicamente a personas del municipio difundió de manera reiterada contenidos sobre distintos miembros de la comunidad. Los administradores invitaban a otros usuarios a enviar información personal, rumores o

señalamientos para posteriormente publicarlos, incluyendo ataques dirigidos contra jóvenes que habían participado como representantes de belleza del municipio. Las publicaciones generaban además comentarios, burlas y nuevas acusaciones por parte de otros usuarios. Este tipo de caso muestra cómo una plataforma o cuenta puede funcionar como punto de articulación de una dinámica colectiva de exposición pública, en la que el daño no proviene únicamente del administrador de la página, sino que es ampliado por la participación de múltiples integrantes de la comunidad digital.

Caso ilustrativo.

La dimensión colectiva de la ciberviolencia también se observa en un caso registrado en febrero de 2026, cuando un estudiante universitario que participaba como candidato a representante del cuerpo

electoral para la elección de rector de la Universidad de San Carlos de Guatemala fue objeto de una campaña de difamación y desprestigio en Facebook y X. Diversos usuarios difundieron de manera reiterada señalamientos sobre una supuesta vinculación del estudiante con un diputado del Congreso de la República. Aunque otros usuarios advirtieron que la información era falsa y que podía tratarse de una confusión de nombres, los señalamientos continuaron circulando y afectando su reputación pública. El caso muestra una modalidad de violencia colectiva en la que el daño no depende únicamente de la publicación original, sino de la participación sucesiva de múltiples usuarios que reproducen, comentan y amplifican una acusación, aumentando su alcance y dificultando que la persona afectada pueda controlar la información que circula sobre ella.

La ciberviolencia como expresión de conflictos y desigualdades sociales

Un segundo hallazgo que amplía la teoría de partida es que la ciberviolencia no surge en un vacío social. Por el contrario, una proporción considerable de los incidentes registrados se encuentra vinculada al contexto político y social del país. Los debates sobre corrupción, procesos electorales, decisiones

judiciales, seguridad pública, conflictos políticos o políticas gubernamentales generan escenarios especialmente propicios para la aparición de ataques y campañas de desprestigio. Cuando estas agresiones se dirigen contra personas jóvenes que participan en esos debates, pueden desalentar su expresión

pública y restringir sus oportunidades de liderazgo e incidencia, una preocupación central para la agenda de Juventud, Paz y Seguridad.

Caso ilustrativo.

En TikTok, la página “guate.te informa (Líderes Guatemaltecos)” inició una campaña de desprestigio contra el joven político Alejandro Sapón y su organización La Liga Juvenil, mediante una publicación en la que se le acusaba de malas gestiones, tráfico de influencias, vínculos con otros políticos y de utilizar a jóvenes para aumentar su influencia. Los usuarios reaccionaron de forma dividida: algunos apoyaron las acusaciones mediante juicios negativos, mientras otros defendieron a Sapón y a la organización, aunque estos últimos comentarios fueron presuntamente ocultados o eliminados por la página.

Caso ilustrativo.

En la página de Facebook Denuncia Chimalteca, usuarios realizaron críticas contra el diputado Víctor Vicente Bonilla Gonzales, representante de Chimaltenango, después de que la página publicara un mensaje señalando que únicamente contaba con tercero básico y cuestionando su capacidad para legislar. En los comentarios, usuarios lo calificaron de inepto y corrupto, generando una ola de críticas contra el diputado.

Caso ilustrativo.

El 6 de marzo de 2026, la diputada Ivanna Luján Padilla fue objeto de ataques y expresiones de odio en la red social X

después de emitir un voto distinto al de los demás integrantes de su bloque durante el proceso de elección de magistrados. A partir de su decisión, distintos usuarios dirigieron ataques contra la diputada, convirtiendo una actuación vinculada al proceso de elección de autoridades del sistema de justicia en un motivo de agresión digital. El caso ilustra cómo los procesos de elección de magistrados y conformación de las altas cortes pueden trasladar las disputas y tensiones políticas al espacio digital, donde las decisiones de los actores involucrados generan dinámicas de señalamiento, deslegitimación y violencia verbal.

Esta relación entre contexto y ciberviolencia no se limita a los conflictos políticos. Numerosos casos reflejan la reproducción de desigualdades y formas de discriminación históricas y estructurales relacionadas con el sexo, la identidad de género, la orientación sexual, la pertenencia étnica, la posición socioeconómica o las diferencias ideológicas. Los patrones de género registrados por Ciberadar permiten observar con especial claridad esta dinámica.

Los perfiles femeninos constituyen el grupo de víctimas identificado con mayor frecuencia (35%), seguidos por los perfiles masculinos (28%). Sin embargo, en casi una cuarta parte de los casos (24%) no fue posible determinar el género de la víctima, mientras que otro 12% involucró simultáneamente a perfiles masculinos y femeninos. Del lado de los victimarios, casi la mitad de los casos (48%) no permitió

identificar el género del agresor. Entre los casos identificables predominan los masculinos (26%), seguidos por grupos mixtos (22%), mientras que los perfiles femeninos representan únicamente el 4% de los victimarios registrados.

Tabla 7. Género de las víctimas y victimarios en los casos registrados por el equipo de Ciberadar, del 11 de febrero al 4 de junio 2026

Género de la víctima	Frecuencia	% del total	Género del victimario	Frecuencia	% del total
Femenino	130	35%	Se desconoce/ No registrado*	180	48%
Masculino	105	28%	Masculino	97	26%
Se desconoce/ No registrado*	89	24%	Masculino, Femenino	83	22%
Masculino, Femenino	45	12%	Femenino	14	4%
Persona trans**	5	1%			
Total	374	100%	Total	374	100%

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

*Incluye los casos en que se desconoce o no se registró esta característica, y los casos dirigidos a entidades u organizaciones.

**Se registró como "Persona trans" únicamente a quien había expresado públicamente su identidad de género.

Pero las diferencias más significativas aparecen al observar cómo son atacadas las personas según su género. Entre los perfiles femeninos, los insultos relacionados con el sexo o género constituyen la categoría más frecuente (27%), seguidos por aquellos dirigidos contra la apariencia física (16%), la actividad profesional (13%) y la capacidad intelectual (11%). En

contraste, entre los perfiles masculinos predominan la difamación (22%), los ataques relacionados con la actividad profesional (18%), la apariencia física (15%) y la orientación sexual (11%). Entre las personas trans identificadas, los ataques se concentran en el sexo o género, la apariencia física y la orientación sexual (27% cada uno). En otras palabras, mientras que los perfiles femeninos son atacados con mayor frecuencia por su condición femenina, mediante estereotipos de feminidad y

cuestionamientos a su apariencia física y capacidad intelectual, los perfiles masculinos parecen ser objeto de agresiones dirigidas principalmente a cuestionar su reputación, desempeño profesional o masculinidad, y las personas trans, a cuestionar su identidad de género y su cuerpo. Estas diferencias reflejan que la ciberviolencia reproduce desigualdades y normas sociales pre existentes, adaptándolas al contexto digital.

Tabla 8. Tipo de ataque verbal y/o discurso de odio por género de la víctima en los casos registrados por el equipo de Ciberadar, del 11 de febrero al 4 de junio 2026

Tipo de ataque verbal y/o discurso de odio	Femenino n (%)	Masculino n (%)	Perfiles mixtos n (%)	Persona trans n (%)	Se desconoce / No registrado* n (%)
Sexo/género	51 (27%)	1 (1%)	7 (10%)	3 (27%)	14 (12%)
Actividad profesional	25 (13%)	23 (18%)	8 (12%)	0 (0%)	18 (15%)
Difamación	23 (12%)	29 (22%)	10 (15%)	1 (9%)	17 (15%)
Apariencia física	29 (16%)	20 (15%)	9 (13%)	3 (27%)	12 (10%)
Capacidad intelectual	21 (11%)	15 (11%)	11 (16%)	0 (0%)	15 (13%)
Ideología política	14 (8%)	10 (8%)	4 (6%)	0 (0%)	18 (15%)
Origen étnico	8 (4%)	9 (7%)	11 (16%)	1 (9%)	9 (8%)

Tipo de ataque verbal y/o discurso de odio	Femenino n (%)	Masculino n (%)	Perfiles mixtos n (%)	Persona trans n (%)	Se desconoce / No registrado* n (%)
Orientación sexual	2 (1%)	14 (11%)	2 (3%)	3 (27%)	6 (5%)
Posición socioeconómica	4 (2%)	4 (3%)	3 (4%)	0 (0%)	6 (5%)
Nacionalidad/país de origen	1 (1%)	4 (3%)	1 (1%)	0 (0%)	1 (1%)
Vida sexual, afectiva o relaciones personales	5 (3%)	0 (0%)	1 (1%)	0 (0%)	0 (0%)
Religión	2 (1%)	1 (1%)	0 (0%)	0 (0%)	1 (1%)
Pertenencia a una organización criminal	1 (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
Rendimiento en el juego	0 (0%)	1 (1%)	0 (0%)	0 (0%)	0 (0%)
Total	186 (100%)	131 (100%)	67 (100%)	11 (100%)	117 (100%)

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

*Incluye los casos en que se desconoce o no se registró esta característica, y los casos dirigidos a entidades u organizaciones.

Los siguientes casos muestran cómo la ciberviolencia contra las mujeres puede manifestarse mediante expresiones misóginas, la desacreditación de las víctimas y la sexualización de sus cuerpos.

Caso ilustrativo.

Una mujer denunció públicamente a un hombre que realizaba actos de masturbación mientras se encontraba dentro del transporte público. Después de que la denuncia circulara en redes sociales, varios hombres reaccionaron con burlas y comentarios misóginos y machistas dirigidos contra la propia denunciante. El caso muestra cómo una mujer que denuncia una conducta de carácter sexual puede convertirse ella misma en objeto de agresión digital, desplazando la atención de la conducta denunciada hacia la desacreditación y el ataque contra la mujer.

Caso ilustrativo.

Una influencer dio a conocer a través de redes sociales que había sido víctima de un asalto mientras se encontraba junto con su familia cerca de un río en el departamento de Escuintla. La publicación tenía como punto de partida un hecho delictivo sufrido por ella y su familia; sin embargo, después de que relatara públicamente lo ocurrido, la conversación en las plataformas digitales derivó también en ataques dirigidos contra la propia víctima. Diversos usuarios publicaron mensajes de odio y expresiones misóginas contra la mujer, convirtiendo el espacio de comentarios y reacciones en un nuevo ámbito de agresión. El caso resulta ilustrativo porque la violencia digital no estuvo relacionada únicamente con cuestionamientos sobre las circunstancias del asalto, sino que incorporó descalificaciones dirigidas contra ella en su condición de

mujer. De esta manera, una persona que inicialmente había sido víctima de un hecho de violencia fuera de línea quedó posteriormente expuesta a una segunda forma de victimización en el espacio digital, donde el sexo y el género funcionaron como recursos para insultarla y desacreditarla.

El monitoreo también documentó 44 menciones relacionadas con el hostigamiento sexual digital, entre ellas el envío de mensajes, comentarios o contenidos de carácter sexual no solicitados. De estas menciones, el 66% correspondió al envío de mensajes con insinuaciones sexuales; el 23%, al envío de imágenes o videos de genitales o partes íntimas; y en el 11% no fue posible determinar la forma específica de hostigamiento sexual.

Al analizar estas menciones según el género de la víctima, el 80% correspondió a perfiles femeninos, el 9% a perfiles masculinos, el 2% a perfiles mixtos (masculino y femenino) y otro 2% a una persona trans. En el 7% restante se desconoce o no se registró el género. Este patrón es consistente con lo expresado en los grupos focales, donde las mujeres señalaron que se encuentran expuestas a comentarios públicos o privados con insinuaciones o contenidos sexuales no solicitados, y que estas prácticas pueden ser perpetradas por amistades, personas conocidas o desconocidas.

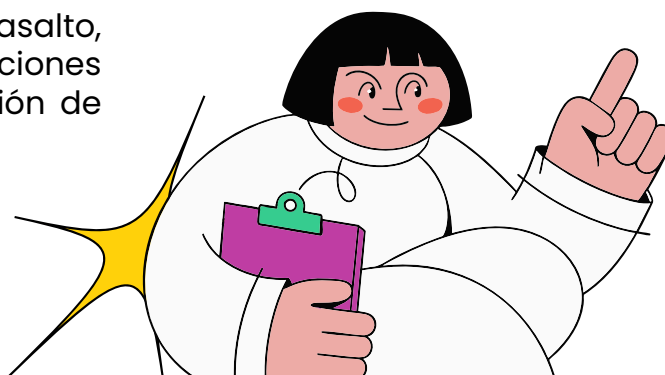


Tabla 9. Tipo de hostigamiento sexual digital por género de la víctima en los casos registrados por el equipo de Ciberadar, del 11 de febrero al 4 de junio 2026

Tipo de hostigamiento sexual digital	Femenino n (%)	Masculino n (%)	Perfiles mixtos n (%)	Persona trans n (%)	Se desconoce / No registrado* n (%)
Envío de mensajes con insinuaciones sexuales	25 (71%)	2 (50%)	0 (0%)	0 (0%)	2 (67%)
Envío de mensajes con imágenes o videos de genitales o partes íntimas	6 (17%)	2 (50%)	1 (100%)	0 (0%)	1 (33%)
Se desconoce el tipo de hostigamiento	4 (11%)	0 (0%)	0 (0%)	1 (100%)	0 (0%)
Total	35 (100%)	4 (100%)	1 (100%)	1 (100%)	3 (100%)

Nota: Los porcentajes han sido redondeados, por lo que el total puede no sumar exactamente 100%.
*Incluye los casos en que se desconoce o no se registró esta característica, y los casos dirigidos a entidades u organizaciones.

Caso ilustrativo.

A principios de junio de 2026, varias mujeres jóvenes y adolescentes denunciaron públicamente en redes sociales a un fotógrafo por presuntas conductas de acoso, hostigamiento, presión y manipulación. Según los testimonios difundidos por las denunciantes, el señalado habría utilizado Instagram y WhatsApp para contactarlas y enviarles de manera reiterada comentarios, propuestas e insinuaciones de carácter sexual no deseadas, algunas de ellas relacionadas con sesiones fotográficas y supuestas ofertas laborales. El caso ejemplifica el hostigamiento sexual

digital, pues muestra cómo los canales de comunicación pueden utilizarse para dirigir conductas sexuales no consentidas de forma persistente.

Caso ilustrativo.

Una influencer publicó en TikTok un video en el que aparecía bailando y disfrutando en traje de baño. A partir de la publicación, diversos usuarios difundieron comentarios sexistas, insinuaciones sexuales y expresiones dirigidas a evaluar y criticar su cuerpo. El caso ejemplifica cómo la participación de las mujeres en los espacios digitales puede generar formas de hostigamiento sexual y sexualización,

mediante comentarios no solicitados que convierten su apariencia y su cuerpo en objetos de valoración pública.

De igual forma, el monitoreo registró 89 menciones relacionadas con la difusión no consentida de contenido. Del total, 27 menciones (30%) corresponden a perfiles femeninos, 26 (29%) a perfiles masculinos, 11 (12%) involucran simultáneamente perfiles femeninos y masculinos, y 2 (2%) corresponden a personas trans. En las 23 menciones restantes (26%) se desconoce o no se registró el género de las víctimas, incluidas las dirigidas a entidades u organizaciones.

La distribución muestra diferencias según el género de las víctimas. Entre los perfiles femeninos, la difusión de contenidos personales modificados mediante inteligencia artificial y la difusión no

consentida de contenidos de índole sexual representaron, cada una, el 33% de las menciones, seguidas por la difusión de información personal (26%). Entre los perfiles masculinos predominaron la difusión de contenidos personales modificados mediante inteligencia artificial (46%) y la difusión de información personal (38%), mientras que la difusión no consentida de contenidos de índole sexual representó sólo el 4%.

Por tanto, aunque esta categoría comprende diversas modalidades, los contenidos de carácter sexual adquirieron un mayor peso relativo entre los perfiles femeninos, lo que muestra una sexualización de los cuerpos principalmente de las mujeres, como objetos de consumo público, la cual puede relacionarse con nuevas formas de violencia sexual en el espacio digital.

Tabla 10. Tipo de difusión no consentida de contenido según el género de las víctimas en los casos registrados por el equipo de Ciberadar, del 11 de febrero al 4 de junio 2026

Tipo de difusión no consentida de contenido	Femenino n (%)	Masculino n (%)	Perfiles mixtos n (%)	Persona trans n (%)	Se desconoce / No registrado* n (%)
Difusión de imágenes, stickers, vídeos o audios personales modificados mediante IA	9 (33%)	12 (46%)	2 (18%)	1 (50%)	10 (43%)
Difusión de imágenes, vídeos o audios con información personal	7 (26%)	10 (38%)	7 (64%)	0 (0%)	9 (39%)

Tipo de difusión no consentida de contenido	Femenino n (%)	Masculino n (%)	Perfiles mixtos n (%)	Persona trans n (%)	Se desconoce / No registrado* n (%)
Difusión no consentida de imágenes, stickers, vídeos o audios de índole sexual (packs)	9 (33%)	1 (4%)	2 (18%)	0 (0%)	2 (9%)
Difusión de imágenes, stickers, vídeos o audios de índole sexual modificados mediante IA	1 (4%)	3 (12%)	0 (0%)	0 (0%)	1 (4%)
Se desconoce el subtipo de difusión	1 (4%)	0 (0%)	0 (0%)	1 (50%)	1 (4%)
Total	27 (100%)	26 (100%)	11 (100%)	2 (100%)	23 (100%)

Nota: Los porcentajes han sido redondeados, por lo que el total puede no sumar exactamente 100%.
*Incluye los casos en que se desconoce o no se registró esta característica, y los casos dirigidos a entidades u organizaciones.

Caso ilustrativo.

El 28 de febrero de 2026, la página de Facebook Heber The Style Chapín publicó capturas de pantalla de un video de índole sexual en el que aparecía una mujer. Aunque la publicación se presentaba como una forma de defenderla y condenar la circulación de sus videos íntimos, varios usuarios utilizaron la sección de comentarios para compartir el video original y otros materiales íntimos de distintas mujeres, sin que existiera evidencia de su consentimiento. El caso muestra cómo una publicación que busca denunciar este tipo de violencia puede convertirse en un nuevo espacio

de difusión y revictimización, ampliando el alcance de contenidos sexuales compartidos sin autorización.

Caso ilustrativo.

Según el registro realizado el 11 de abril de 2026, una cuenta de TikTok difundió imágenes íntimas de mujeres mayas de Chichicastenango, Quiché, sin evidencia de su consentimiento. En los comentarios, otros usuarios solicitaron acceder a los videos completos, contribuyendo a ampliar la exposición y sexualización de las mujeres afectadas. El caso ejemplifica una forma de violencia sexual digital basada en la difusión no consentida de

contenido íntimo y muestra cómo la participación de otros usuarios puede reforzar y extender la vulneración.

La ciberviolencia de género también puede entrelazarse con otras formas de violencia y discriminación, como el racismo y la transfobia. Desde una perspectiva interseccional, los siguientes casos permiten observar cómo distintas características identitarias pueden incidir simultáneamente en las formas que adoptan las agresiones digitales.

Caso ilustrativo.

Una cuenta dedicada a publicar contenido de mujeres que utilizan indumentaria maya difundió un video de una joven en el que se enfatizaban partes de su cuerpo mediante acercamientos de cámara. En los comentarios, algunos usuarios solicitaron el “video completo” y ofrecieron intercambiar otros materiales similares. El caso resulta especialmente relevante porque la agresión articula género, sexualización y pertenencia étnica, y evidencia cómo las características identitarias de las mujeres pueden convertirse simultáneamente en objetos de exposición y violencia en los espacios digitales.

Caso ilustrativo.

En el marco de la conmemoración del 28 de junio, Día del Orgullo LGBTQ+, la cuenta de TikTok de Noficcionggt publicó un video en el que presentó la historia de Carla, una mujer trans y maya que ha experimentado desplazamiento y discriminación debido a su identidad. Tras la publicación del

video, varios usuarios reaccionaron en la sección de comentarios con expresiones negativas y transfóbicas dirigidas contra Carla. El caso muestra cómo la visibilización de experiencias de personas trans en las plataformas digitales puede generar respuestas de rechazo y ataques verbales basados directamente en la identidad de género de la persona, reproduciendo en el espacio digital formas de discriminación que también se manifiestan fuera de Internet.

En esta misma línea, la distribución de los ataques verbales y discursos de odio también presenta diferencias importantes según el grupo étnico de las víctimas. Entre las personas ladinas/mestizas, las menciones se concentran principalmente en la difamación (24%) y los ataques basados en la actividad profesional (22%), seguidos por aquellos relacionados con la apariencia física (14%) y el sexo o género (11%). Entre las personas mayas, adquieren un peso similar entre sí los ataques relacionados con el sexo o género, la apariencia física, la capacidad intelectual y la ideología política, cada uno con aproximadamente el 14% de las menciones. Sin embargo, los ataques basados en el origen étnico constituyen la categoría más frecuente (20%), con una proporción considerablemente mayor que la observada entre las personas ladinas/mestizas (2%).

Estos datos sugieren que la pertenencia étnica no sólo constituye una característica de las víctimas, sino que, particularmente en el caso de las personas mayas, se convierte directamente en un

motivo de agresión. En contraste, entre las personas ladinas/mestizas, los ataques se articulan en mayor medida alrededor de la reputación y el desempeño o actividad profesional. En este punto, sin embargo, debe considerarse que, en una cantidad importante de los registros, se desconoce el grupo étnico de la víctima, por lo que

estas diferencias deben interpretarse como patrones observados en los casos en los que fue posible identificar esta característica en una muestra no probabilística, y no como estimaciones de la prevalencia de estos ataques en cada población.

Tabla 11. Menciones de ataques verbales y/o discursos de odio registrados por el equipo del Ciberadar por pueblo de origen de la víctima (Ladino/Mestizo y Maya), del 11 de febrero al 4 de junio de 2026.

Tipo de ataque verbal y/o discurso de odio	Ladino/Mestizo	Maya	Se desconoce/ No registrado*
Sexo/género	15 (11%)	9 (14%)	49 (16%)
Difamación	34 (24%)	5 (8%)	41 (14%)
Apariencia física	19 (14%)	9 (14%)	44 (15%)
Capacidad intelectual	11 (8%)	9 (14%)	40 (13%)
Actividad profesional	31 (22%)	6 (9%)	36 (12%)
Orientación sexual	11 (8%)	5 (8%)	11 (4%)
Ideología política	11 (8%)	9 (14%)	26 (9%)
Origen étnico	3 (2%)	13 (20%)	21 (7%)
Posición socioeconómica	2 (1%)	1 (2%)	13 (4%)
Nacionalidad/país de origen	0 (0%)	0 (0%)	6 (2%)

Tipo de ataque verbal y/o discurso de odio	Ladino/Mestizo	Maya	Se desconoce/ No registrado*
Vida sexual, afectiva o relaciones personales	1 (1%)	0 (0%)	5 (2%)
Religión	1 (1%)	0 (0%)	3 (1%)
Rendimiento en el juego	0 (0%)	0 (0%)	1 (<1%)
Pertenencia a organización criminal	0 (0%)	0 (0%)	1 (<1%)
Total	139 (100%)	66 (100%)	297 (100%)

Nota: Los porcentajes han sido redondeados, por lo que el total puede no sumar exactamente 100%. No se incluyen las menciones de ataques verbales y/o discursos de odio dirigidos a personas extranjeras. *Incluye los casos en que se desconoce o no se registró esta característica, y los casos dirigidos a entidades u organizaciones.

Caso ilustrativo.

El 28 de mayo de 2026, Emisoras Unidas publicó en Facebook la noticia de que un niño de Cajolá, Quetzaltenango, había sido trasladado al Hospital Regional de Occidente debido a un cuadro de desnutrición crónica. En los comentarios, varios usuarios dirigieron expresiones racistas contra la población indígena, incluyendo el uso despectivo de la palabra “indios” y comentarios que proponían medidas violentas, como la esterilización de mujeres indígenas. El caso muestra de manera particularmente explícita cómo una noticia referida a una situación individual puede desencadenar ataques

que generalizan la agresión hacia un grupo étnico completo.

Caso ilustrativo.

El 9 de mayo de 2026, el medio Noticias de Totonicapán publicó en Facebook información sobre un perro que había sido atropellado. A partir de la publicación, algunos usuarios trasladaron la responsabilidad del hecho hacia la población del departamento y emitieron ataques verbales contra sus habitantes basados tanto en su origen étnico como en supuestas deficiencias en su capacidad intelectual. El caso evidencia cómo la violencia verbal puede partir

de un acontecimiento particular para producir generalizaciones despectivas sobre una población indígena, vinculando su pertenencia étnica con atributos negativos sobre sus capacidades.

Caso ilustrativo.

El 3 de abril de 2026, el medio *5to Poder La Verdad sin Miedo* publicó en X contenido sobre la tradicional práctica de peleas a puño limpio que se realiza en Chivarreto, San Francisco El Alto, Totonicapán. La publicación se refirió de manera despectiva a quienes participan en esta tradición, calificándolos de “salvajes” y vinculando esta caracterización con su origen étnico y sus prácticas culturales. El caso ilustra una forma de violencia verbal en la que una práctica cultural específica se utiliza como punto de partida para construir una representación degradante de una población indígena. Más allá de la crítica a la actividad en sí misma, la agresión reproduce estereotipos históricos que representan a los pueblos indígenas como atrasados, incivilizados o inferiores, mostrando cómo este tipo de imaginarios racistas también encuentran espacios de reproducción y circulación en las plataformas digitales.

En conjunto, estos hallazgos sugieren que la ciberviolencia no constituye un fenómeno separado de la violencia estructural existente fuera de Internet, sino una de sus expresiones contemporáneas.

En la literatura especializada⁶, a esta característica de la ciberviolencia se

le suele denominar “continuo de la violencia”, término que resalta el grado en el que se interrelacionan el mundo *online* y el mundo *offline*. Esta perspectiva cuestiona la idea de que la violencia digital constituye una forma de agresión separada de aquella que ocurre en los espacios físicos y sociales. Por el contrario, se argumenta que ambos ámbitos se encuentran estrechamente conectados y pueden reforzarse mutuamente.

Desde esta perspectiva, la violencia puede iniciar en el ciberespacio y trasladarse o generar consecuencias en el mundo físico; por ejemplo, cuando amenazas realizadas en redes sociales producen temor por la seguridad personal, cuando la divulgación de información privada facilita la localización de una víctima o cuando una campaña de hostigamiento afecta sus relaciones familiares, laborales o comunitarias. De manera inversa, una agresión, conflicto o relación de poder que se origina fuera de Internet, y que puede tener raíces históricas profundas, puede trasladarse a las plataformas digitales, donde adquiere nuevas formas y potencialmente una audiencia mucho más amplia. Una disputa interpersonal, un acto de discriminación, una agresión sexual o un conflicto político pueden continuar mediante insultos, amenazas, difusión de información, fotografías o videos, campañas de desprestigio y otras formas de hostigamiento digital. En algunos casos, además, este tránsito puede ocurrir repetidamente: por ejemplo, cuando una agresión física genera



⁶ Organización de los Estados Americanos, *La violencia de género en línea contra las mujeres y niñas: Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta*. Preparado por Katya N. Vera Morales. OEA/Ser.D/XXV.25. Washington, DC, 2021.

contenido y reacciones digitales que, a su vez, producen nuevas consecuencias fuera de línea.

Así, las plataformas digitales funcionan como espacios donde conflictos políticos, prejuicios sociales y relaciones históricas de poder encuentran nuevas formas de manifestarse, amplificarse y difundirse. En ese sentido, la ciberviolencia no constituye un fenómeno aislado de las dinámicas sociales que existen fuera de Internet, sino que reproduce y, en determinadas circunstancias, intensifica desigualdades, estigmas y formas de discriminación previamente existentes.

Esto último resulta particularmente relevante en Guatemala, donde el racismo y la discriminación contra los pueblos indígenas tienen profundas raíces históricas y han atravesado las relaciones sociales, económicas y políticas del país. Los hallazgos de Ciberadar sugieren que estas estructuras de discriminación también se trasladan al espacio digital: entre las víctimas mayas cuyo origen étnico pudo ser identificado, los ataques basados precisamente en ese origen constituyen la categoría más frecuente de violencia verbal registrada. Los casos

observados muestran, además, que estas expresiones pueden recurrir a estereotipos que asocian la identidad indígena con características negativas, como una supuesta menor capacidad intelectual, o incluso transformar acontecimientos particulares en descalificaciones generalizadas contra comunidades o poblaciones indígenas enteras. Las redes sociales ofrecen condiciones particulares para la reproducción de estas prácticas, pues permiten que expresiones discriminatorias sean replicadas, comentadas y amplificadas por numerosos usuarios, haciendo posible que una agresión individual adquiera rápidamente un carácter colectivo.

Comprender la ciberviolencia exige, por tanto, analizar no solamente las interacciones que ocurren en las plataformas digitales, sino también las estructuras de desigualdad, los prejuicios sociales y las relaciones históricas de poder que hacen posibles determinadas formas de agresión y ayudan a explicar por qué ciertos grupos y características identitarias se convierten en blancos recurrentes de la violencia digital.

Edad de las víctimas y espacios donde ocurre la ciberviolencia

La distribución por edad debe interpretarse con cautela debido a que en el 60% de los casos no fue posible identificar la

edad de la víctima. No obstante, entre aquellos en los que fue posible obtener esta información, se observa una mayor

concentración en personas jóvenes. Los grupos de 20 a 24 años (9%) y 25 a 29 años (7%) registran las mayores frecuencias, seguidos por las personas de 50 años o más (7%) y los adolescentes de 15 a 19 años (5%). Este patrón observado en la muestra podría estar relacionado con un uso más intensivo de redes sociales

y plataformas digitales por personas jóvenes y/o con los propios sesgos del equipo de observación conformado también por jóvenes. El elevado porcentaje de información desconocida impide establecer conclusiones definitivas sobre el perfil etario de las víctimas.

Tabla 12. Rangos de edad de las víctimas de los casos de ciberviolencia registrados por el equipo de Ciberadar, del 11 de febrero al 4 de junio 2026

Rango de edad	Frecuencia	Porcentaje del total
5 a 9 años	1	0%
10 a 14 años	8	2%
15 a 19 años	17	5%
20 a 24 años	34	9%
25 a 29 años	28	7%
30 a 34 años	11	3%
35 a 39 años	9	2%
40 a 44 años	9	2%
45 a 49 años	9	2%
50 o más años	25	7%
Se desconoce/No registrado*	223	60%
Total	374	100%

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

*Incluye los casos en que se desconoce o no se registró esta característica, y los casos dirigidos a entidades u organizaciones.

Entre las personas jóvenes de 15 a 29 años, los ataques verbales y discursos de odio registrados por Ciberadar se concentran principalmente en características personales e identitarias. Los ataques basados en el sexo o género constituyen

la categoría más frecuente, con el 23% de las menciones, seguidos por la difamación (18%) y los ataques relacionados con la apariencia física (17%). En conjunto, estas tres categorías representan el 58% de las menciones registradas contra jóvenes.

También tienen una presencia relevante las agresiones basadas en la capacidad intelectual (11%) y la actividad profesional (8%), mientras que aquellas relacionadas con la orientación sexual (7%), la ideología política (6%) y el origen étnico (5%) aparecen con menor frecuencia. Los ataques vinculados con la posición socioeconómica (3%), las relaciones interpersonales (1%) y la pertenencia a una organización criminal (1%) son comparativamente poco frecuentes.

En términos generales, la distribución muestra que la violencia verbal dirigida contra jóvenes registrada por el

Ciberadar se articula principalmente alrededor del sexo o género, la reputación y la apariencia física, lo cual evidencia el peso que adquieren las características identitarias y personales como recursos para la descalificación y la agresión en los espacios digitales. Estas formas de descalificación pueden tener efectos que van más allá del daño individual, ya que pueden erosionar la confianza necesaria para expresarse o incluso organizarse y participar en la vida cívica, especialmente cuando se trata de jóvenes que defienden derechos humanos o impulsan iniciativas de convivencia pacífica.

Tabla 13. Tipos de ataque verbal y/o discurso de odio registrados por el equipo de Ciberadar en contra de jóvenes de 15 a 29 años, del 11 de febrero al 4 de junio de 2026.

Tipo de ataque verbal y/ o discurso de odio	Frecuencia	Porcentaje del total
Ataque verbal o insulto basado en el sexo/ género	29	23%
Difamación	23	18%
Ataque verbal o insulto basado en la apariencia física	22	17%
Ataque verbal o insulto basado en la capacidad intelectual	14	11%
Ataque verbal o insulto basado en actividad profesional	10	8%
Ataque verbal o insulto basado en la orientación sexual	9	7%
Ataque verbal o insulto basado en la ideología política	8	6%

Tipo de ataque verbal y/ o discurso de odio	Frecuencia	Porcentaje del total
Ataque verbal o insulto basado en el origen étnico	6	5%
Ataque verbal o insulto basado en la posición socio económica	4	3%
Otros	2	2%
Total	127	100%

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

La distribución de los ataques verbales y discursos de odio muestra diferencias importantes según el género de las víctimas jóvenes de entre 15 y 29 años. Entre los perfiles femeninos, los ataques basados en el sexo o género constituyen la categoría predominante, con el 35% de las menciones, muy por encima de la difamación y los ataques basados en la capacidad intelectual (14% cada uno) y la apariencia física (13%). Entre los perfiles masculinos, en cambio, no se registraron ataques basados específicamente en el sexo o género; la principal forma de agresión fue la difamación (32%), seguida por los ataques relacionados con la apariencia física (22%) y la orientación sexual (16%). Esta última categoría presenta una diferencia particularmente

marcada, pues representa apenas el 1% de las menciones entre los perfiles femeninos. También destaca que los ataques relacionados con la capacidad intelectual tienen un mayor peso relativo entre los perfiles femeninos (14%) que entre los masculinos (5%). En conjunto, estos datos sugieren que las formas que adopta la violencia verbal contra jóvenes varían según el género: mientras que en los perfiles femeninos adquieren especial relevancia las agresiones vinculadas directamente con su condición de género, entre los masculinos predominan mecanismos de descalificación relacionados con la reputación, la apariencia física y la orientación sexual.

Tabla 14. Tipos de ataque verbal y/o discurso de odio registrados por el equipo de Ciberadar por el género de la víctima (casos con víctimas individuales y grupales de 15 a 29 años), del 11 de febrero al 4 de junio de 2026.

Tipo de ataque verbal y/o discurso de odio	Femenino	Masculino	Perfiles mixtos
Ataque basado en sexo/género	25 (35%)	0 (0%)	2 (17%)
Difamación	10 (14%)	12 (32%)	1 (8%)
Ataque basado en apariencia física	9 (13%)	8 (22%)	4 (33%)
Ataque basado en capacidad intelectual	10 (14%)	2 (5%)	1 (8%)
Ataque basado en actividad profesional	4 (6%)	4 (11%)	2 (17%)
Ataque basado en orientación sexual	1 (1%)	6 (16%)	1 (8%)
Ataque basado en ideología política	4 (6%)	2 (5%)	0 (0%)
Ataque basado en origen étnico	4 (6%)	1 (3%)	1 (8%)
Ataque basado en posición socioeconómica	2 (3%)	2 (5%)	0 (0%)
Vida sexual, afectiva o relaciones personales	1 (1%)	0 (0%)	0 (0%)
Ataque por pertenencia a organización criminal	1 (1%)	0 (0%)	0 (0%)
Total	71 (100%)	37 (100%)	12 (100%)

Nota: Los porcentajes han sido redondeados, por lo que el total puede no sumar exactamente 100%. No se incluyen 7 menciones en las que se desconoce el género del perfil.

Caso ilustrativo.

El 15 de abril de 2026, la página de Facebook *Noticias Carranza San Juan Sacatepéquez* publicó la imagen de una joven de 21 años acompañada de información sobre su vida íntima y sexual, sin evidencia de que hubiera consentido su difusión. A partir de la publicación, múltiples usuarios, principalmente hombres, realizaron comentarios que sexualizaban a la joven, sugerían actos sexuales hacia ella y utilizaban expresiones denigrantes y burlas. El caso ejemplifica la importancia que adquieren el sexo y el género como ejes de las agresiones dirigidas contra las mujeres jóvenes y muestra cómo la exposición pública de información personal puede propiciar dinámicas colectivas de sexualización y descalificación.

Caso ilustrativo.

En junio de 2025, una persona anónima publicó en el grupo de Facebook *Conductores inDrive Guatemala* una fotografía de Carlos Vivar, de 22 años, acusándolo de solicitar viajes y huir sin pagarlos. La publicación utilizaba además un término peyorativo relacionado con su orientación sexual para desacreditarlo. Según el relato del joven, la acusación era falsa y buscaba exponerlo públicamente debido a que es abiertamente gay. Otros usuarios se sumaron posteriormente a la publicación, reforzando los señalamientos e incluso aportando información sobre su posible lugar de residencia. El caso ilustra la combinación entre difamación y ataques basados en la orientación sexual, dos formas de agresión que tienen

un peso particularmente importante entre las menciones correspondientes a hombres jóvenes.

En cuanto a los espacios donde ocurre la ciberviolencia, Facebook fue el principal escenario donde se registraron los casos documentados por Ciberadar. Esta plataforma concentra el 45% de todas las menciones, más del doble que TikTok (21%) y más de tres veces las registradas en X (13%). WhatsApp (7%) e Instagram (7%) aparecen en un segundo nivel, mientras que Telegram, Messenger y los videojuegos representan una proporción marginal de los registros. Es altamente probable que estos resultados reflejan las limitaciones propias del ejercicio de observación mencionadas en repetidas ocasiones, pero quizás también la naturaleza pública de muchas de las interacciones que ocurren en ciertas plataformas.



Tabla 15. Medios utilizados en los casos de ciberviolencia registrados por el equipo de Ciberadar, del 11 de febrero al 4 de junio 2026

Medio	Frecuencia	Porcentaje del total
Facebook	180	45%
TikTok	82	21%
X	53	13%
WhatsApp	29	7%
Instagram	26	7%
Otro	18	5%
Telegram	3	1%
Se desconoce	2	1%
Free Fire (videojuego)	1	0%
Messenger	1	0%
Roblox (videojuego)	1	0%
Total	396	100%

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



✨ Un fenómeno tecnológicamente dinámico

La distribución entre plataformas constituye solamente una parte del componente tecnológico de la ciberviolencia. Un tercer hallazgo que amplía la teoría de partida es que la

rápida evolución tecnológica está transformando las formas de ejercer la ciberviolencia y los desafíos para comprenderla.

El desarrollo reciente de herramientas de inteligencia artificial generativa, la proliferación de imágenes, audios y videos sintéticos o francamente falsos, así como la creciente facilidad para automatizar la creación y difusión de contenido, están modificando el panorama de riesgos digitales. Durante el período analizado fue posible documentar casos en los que imágenes generadas mediante inteligencia artificial fueron utilizadas para ridiculizar, desacreditar o difamar a personas específicas. Por lo tanto, estas tecnologías han dejado de representar únicamente un riesgo hipotético y ya forman parte de las dinámicas observadas por Ciberadar.

Caso ilustrativo.

En abril de 2026, una joven conocida en redes sociales como “Jenn te informa” denunció que terceros habían creado y difundido a través de WhatsApp un *sticker* utilizando una imagen suya alterada mediante inteligencia artificial. El contenido circuló dentro de su facultad y fue asociado negativamente con su persona, lo que llevó a la joven a publicar aclaraciones en X e Instagram señalando que la imagen no correspondía a ella y denunciando el intento de dañar su reputación. El caso ilustra cómo las tecnologías de generación y manipulación de imágenes reducen las barreras para fabricar contenido falso o engañoso y permiten que este circule rápidamente entre distintos espacios digitales.

Caso ilustrativo.

El 30 de abril de 2026, el influencer

Abel Ixco fue objeto de ataques en TikTok relacionados con su apariencia física y su origen étnico después de publicar contenido sobre su visita a un restaurante en Quetzaltenango. Como parte de las agresiones, se creó mediante inteligencia artificial una imagen que fusionaba su apariencia con la de un sapo, la cual fue utilizada para burlarse de sus rasgos físicos. El caso muestra cómo las herramientas de inteligencia artificial pueden incorporarse a formas ya existentes de violencia digital, facilitando la creación de contenidos manipulados específicamente diseñados para ridiculizar a una persona. En este caso, la tecnología permitió transformar características físicas e identitarias de la víctima en material visual de burla, agregando una nueva dimensión a los ataques verbales que circulaban alrededor de la publicación.

La incorporación de estas tecnologías introduce nuevos desafíos para la seguridad, la privacidad y la confianza pública. La facilidad y velocidad con la que pueden producirse y viralizarse contenidos falsificados dificulta distinguir entre información auténtica y manipulada, incrementa las posibilidades de fraude y extorsión, facilita nuevas formas de violencia sexual digital mediante la creación de imágenes íntimas falsas y amplía las capacidades para realizar campañas de desinformación y manipulación política.

Como advierte uno de los estudios citados anteriormente⁷, desde el origen de Internet, la violencia se ha ido transformando a

medida que las plataformas digitales y herramientas tecnológicas han avanzado y se han interrelacionado con la vida real. Sin embargo, la inteligencia artificial generativa, a diferencia de otras tecnologías, permite la automatización, segmentación y un mayor realismo del contenido, todo lo cual amplifica el potencial de daño⁸. Al mismo tiempo, estos avances plantean desafíos metodológicos para la investigación de la ciberviolencia, ya que las categorías tradicionales pueden resultar insuficientes para describir fenómenos que evolucionan rápidamente y trascienden los límites conceptuales existentes.

Caso ilustrativo.

El 13 de marzo de 2026, la cuenta denominada *El noticiero-502gt* difundió en la red social X una imagen manipulada mediante inteligencia artificial del activista Sergio Morataya. La imagen había sido alterada para representarlo de manera sexualizada, incorporando objetos y elementos de carácter sexual y asociándolo de forma burlesca con el activismo LGBTIQ+. El caso muestra una de las formas en que las herramientas de inteligencia artificial pueden ampliar las posibilidades de agresión en las plataformas digitales. La tecnología permite crear representaciones falsas de una persona identificable y colocarla visualmente en situaciones en las que nunca estuvo, produciendo contenido que puede resultar verosímil a primera vista y que puede circular independientemente

de la imagen original.

Caso ilustrativo.

La página de Facebook *Tradición de Guatemala* publicó un video generado mediante inteligencia artificial en el que aparecían dos mujeres jóvenes. La composición y presentación visual del video sugerían una insinuación de carácter sexual. Después de su difusión, el contenido generó numerosas reacciones en la sección de comentarios. Algunos usuarios identificaron que las imágenes habían sido creadas mediante inteligencia artificial; sin embargo, una proporción mayor de las interacciones se concentró en evaluar y comentar la apariencia física de las mujeres representadas. Los comentarios incluyeron tanto expresiones de aprobación como descalificaciones y burlas, entre ellas críticas relacionadas con su peso y con la indumentaria que utilizaban. El caso resulta relevante porque muestra una forma particular en la que la inteligencia artificial puede incorporarse a las dinámicas de ciberviolencia. En este caso, la inteligencia artificial no fue utilizada para modificar la imagen de una víctima identificable, sino para producir desde el inicio un contenido visual que representaba cuerpos femeninos y que posteriormente generó interacciones centradas en su sexualización y valoración física. De esta manera, las herramientas generativas pueden contribuir a producir nuevos objetos de interacción alrededor de los cuales se reproducen patrones previamente existentes de violencia



⁷ Organización de los Estados Americanos, *La violencia de género en línea*, p. 10. Morales. OEA/Ser.D/XXV.25. Washington, DC, 2021.

⁸ Rebecca Umbach, Nicola Henry, Renee Shelby, Gemma Stevens, and Kwynn Gonzalez-Pons, "AI-Generated Image-Based Sexual Abuse: Perpetration and Consumption across Three Regions," *Computers in Human Behavior* 179: 108935, 2026.

verbal, particularmente aquellos relacionados con los estereotipos de género, la sexualización de las mujeres y la evaluación pública de sus cuerpos.

Caso ilustrativo.

Una cuenta que utilizaba el nombre “Aurora Fashion” tomó un video de una periodista de *Plaza Pública* y manipuló su voz para posteriormente difundir el contenido modificado en redes sociales como parte de un anuncio fraudulento. La periodista denunció públicamente el hecho el 13 de marzo de 2026 a través de Instagram. El caso muestra una modalidad de ciberviolencia en la que las herramientas digitales permiten apropiarse de la imagen y la voz de una persona y alterar el contenido original para hacer parecer que comunica o respalda un mensaje que en realidad nunca emitió. A diferencia de otras formas de manipulación de contenido utilizadas principalmente para ridiculizar o desacreditar a una víctima, en este caso la modificación tuvo una finalidad instrumental: aprovechar la identidad y credibilidad de una periodista para promover contenido fraudulento. La agresión afecta así tanto el control de la víctima sobre su propia imagen y voz como su reputación, pues terceras personas pueden interpretar el material manipulado como una comunicación auténtica. El caso de “Aurora Fashion” ilustra, por tanto, cómo las nuevas herramientas de generación y modificación de contenido pueden ampliar las posibilidades de suplantación de identidad en el entorno digital, haciendo cada vez más difícil

distinguir entre contenidos auténticos y contenidos artificialmente manipulados.

Si bien la inteligencia artificial introduce nuevas posibilidades para la creación y manipulación de contenidos utilizados en las agresiones digitales, otras formas de ciberviolencia recurren a mecanismos más tradicionales de engaño y suplantación facilitados por la tecnología con el objetivo de obtener un beneficio económico, como muestran los siguientes casos de estafa registrados por el equipo del Ciberadar.

Caso ilustrativo.

Personas desconocidas enviaron de manera masiva mensajes de WhatsApp a usuarios en distintas partes de Guatemala informándoles falsamente que tenían pendiente el pago de una multa de tránsito supuestamente emitida por EMETRA. Los mensajes incorporaban un elemento adicional de presión al advertir a los destinatarios que disponían de aproximadamente 12 horas para realizar el pago. Para cancelar la supuesta sanción, las víctimas eran dirigidas hacia un enlace fraudulento que aparentaba conducir a un sitio oficial, pero que no correspondía al portal de la Superintendencia de Administración Tributaria (SAT). El caso ilustra una modalidad de estafa basada en la suplantación de instituciones públicas y en la generación de urgencia. Al combinar la aparente autoridad de una institución estatal con un plazo reducido para actuar, el engaño buscaba disminuir la posibilidad de que las personas verificaran la autenticidad

del mensaje antes de ingresar al enlace o realizar alguna acción. Su difusión masiva mediante WhatsApp muestra, además, cómo las plataformas digitales permiten ampliar rápidamente el número de potenciales víctimas con un costo relativamente bajo para quienes realizan el fraude.

Caso ilustrativo.

La cuenta de TikTok *Gyto Car Orellana* fue señalada por múltiples usuarios, páginas informativas y medios digitales por realizar una presunta estafa relacionada con la venta de vehículos. La cuenta publicaba fotografías de automóviles obtenidas de otras fuentes y las presentaba como vehículos disponibles para la venta a precios accesibles, generando así la apariencia de que se trataba de un negocio legítimo. Una vez que una persona manifestaba interés en adquirir alguno de los automóviles anunciados, se le solicitaba realizar un depósito bancario anticipado. Después de recibir el dinero, los responsables dejaban de responder a los compradores y el vehículo ofrecido no era entregado. El caso muestra cómo las plataformas digitales pueden ser utilizadas para construir una identidad comercial aparentemente legítima y generar confianza suficiente para inducir a las víctimas a realizar transferencias de dinero. Las fotografías de vehículos funcionaban como evidencia visual de productos que, en realidad, no pertenecían a quienes administraban la cuenta. Además, el supuesto negocio afirmaba estar ubicado en Chiquimula y mantenía restringidos los comentarios

en TikTok, una práctica que dificultaba que otras personas pudieran publicar advertencias o denuncias directamente en el contenido promocional. De esta manera, el caso combina apropiación de imágenes, construcción de una identidad comercial engañosa y solicitud de pagos anticipados, mostrando cómo las características de las redes sociales pueden ser aprovechadas no sólo para captar potenciales víctimas, sino también para limitar la circulación de información que permita identificar el fraude.

Los casos anteriores muestran cómo el engaño digital puede dirigirse contra personas para obtener dinero o información. Sin embargo, los hallazgos de Ciberadar evidencian que las instituciones públicas también pueden convertirse en blancos directos de ataques digitales, en ocasiones con consecuencias que trascienden a la propia institución y afectan a miles de ciudadanos.

Caso ilustrativo.

El 7 de abril de 2026, el hacker identificado como “Gordon Freeman” realizó un ciberataque contra el sistema de la Dirección General de Control de Armas y Municiones (DIGECAM). El ataque combinó la saturación e intrusión del sistema web y permitió la extracción de información correspondiente a aproximadamente 18 mil usuarios, incluidos registros relacionados con armas de personas individuales, empresas y entidades públicas. El incidente comenzó alrededor de las 3:00 horas y se prolongó durante aproximadamente 13 horas. Aunque

las autoridades señalaron que la información obtenida era pública y no sensible, especialistas advirtieron que la posibilidad de relacionar distintos datos —como nombres, identificadores y licencias de armas— podía generar riesgos adicionales para la seguridad y privacidad de las personas afectadas.

Caso ilustrativo.

El 27 de abril de 2026, el hacker identificado como “Gordon Freeman” realizó otro ciberataque, esta vez contra el portal *Tu Empleo* del Ministerio de Trabajo y Previsión Social (MINTRAB). Mediante el acceso no autorizado a una API antigua y vulnerable, el atacante logró extraer más de 200 mil registros y alrededor de 40 GB de información confidencial. Entre los datos comprometidos se encontraban currículums, números de DPI, información de contacto, direcciones e historiales académicos, laborales y salariales de usuarios del servicio. De acuerdo con la información recopilada por Ciberadar, el ataque aprovechó vulnerabilidades en la infraestructura tecnológica del sistema y posteriormente el atacante habría exigido un pago en bitcoin a cambio de no vender la información sustraída. El caso muestra cómo un ataque dirigido inicialmente contra una infraestructura estatal puede trasladar sus consecuencias a miles de ciudadanos que habían entregado información personal a una institución pública.

Caso ilustrativo.

El 1 de mayo de 2026 se reportó un presunto ciberataque atribuido al hacker identificado como “MrGoblinciano”

contra el Tribunal Supremo Electoral (TSE). El ataque habría vulnerado el portal de firma electrónica de la institución y permitido la filtración y distribución gratuita de 2,136 imágenes en formato JPG correspondientes a firmas electrónicas de empleados autorizados para validar documentos oficiales. Ante los posibles riesgos derivados de la utilización de esta información, el TSE suspendió temporalmente su sitio web, activó un plan de respuesta y contención e inició investigaciones técnicas orientadas a prevenir nuevos accesos no autorizados y reforzar la seguridad de sus sistemas. A diferencia de otros ataques cuyo principal efecto es la exposición de datos personales, este caso resulta especialmente relevante por tratarse de una institución vinculada directamente con la administración de los procesos electorales y por el posible uso de las firmas filtradas para la falsificación de documentos.

Caso ilustrativo.

Un antecedente registrado por Ciberadar ocurrió en enero de 2020, cuando *La Prensa de Occidente* informó que la página de Facebook de la Municipalidad de Quetzaltenango había sido hackeada por personas desconocidas. El incidente fue reportado el 9 de enero, después de que el día anterior apareciera un mensaje relacionado con el robo de datos de cuentas. Aunque no se pudo establecer el alcance de la información comprometida, el caso muestra una modalidad diferente de ataque contra una institución estatal: en lugar de vulnerar una base de datos o un sistema administrativo, el acceso

se produjo sobre uno de sus canales oficiales de comunicación digital. La apropiación de este tipo de cuentas puede comprometer la capacidad de una institución para comunicarse con la ciudadanía y genera el riesgo de que terceros difundan información haciéndose pasar por una fuente oficial.

En conjunto, estos casos muestran que las instituciones estatales también constituyen objetivos directos de la ciberviolencia y que los ataques pueden afectar simultáneamente tres dimensiones: la infraestructura institucional, la información bajo custodia del Estado y la ciudadanía que utiliza sus servicios. Los casos de DIGECAM y MINTRAB evidencian particularmente esta última característica: aunque el acceso no autorizado se produce contra sistemas estatales, una parte sustantiva del daño potencial recae sobre las personas cuyos datos se encuentran almacenados en

ellos. El caso del TSE agrega una dimensión adicional, pues la vulneración afecta información asociada con la validación de documentos de una institución central para el funcionamiento del sistema electoral. Finalmente, el hackeo de la Municipalidad de Quetzaltenango muestra que incluso los canales institucionales de comunicación pueden convertirse en blancos de ataques.

En este sentido, los casos observados por Ciberadar sugieren que la ciberviolencia contra el Estado no debe entenderse únicamente como un problema técnico de ciberseguridad, ya que la creciente digitalización de los servicios públicos hace que una vulneración institucional pueda tener consecuencias sobre la privacidad, la seguridad y la confianza de la ciudadanía en las instituciones públicas.

★ Respuestas y consecuencias de la ciberviolencia



La Tabla 16 muestra que, en buena parte de los casos registrados, no fue posible determinar cómo reaccionó la víctima, ya que en casi la mitad de las menciones (49%) esta información se desconoce. Sin embargo, entre los casos en los que

sí fue posible identificar una respuesta, el patrón más frecuente fue no realizar ninguna acción (23%), seguido por publicar una aclaración en la cuenta personal o institucional (10%) y responder públicamente al agresor sin recurrir

a nuevas agresiones (7%). En menor medida, algunas víctimas optaron por tomar acciones legales (4%) o bloquear y reportar la cuenta del agresor (2%), mientras que fueron muy pocos los casos en los que respondieron con una agresión directa (1%).

El resto de las medidas —como restringir comentarios, cerrar cuentas, hacer privadas las redes sociales, verificar la cuenta o reemplazar contenido generado con inteligencia artificial— aparecen únicamente de forma aislada.

En conjunto, estos resultados sugieren que las víctimas de los casos registrados por el Ciberadar tendieron a adoptar estrategias principalmente reactivas y de bajo nivel de confrontación, orientadas a aclarar públicamente los hechos o limitar el contacto con el agresor, mientras que las respuestas institucionales o legales fueron relativamente poco frecuentes. No obstante, el elevado porcentaje de información desconocida limita la posibilidad de extraer conclusiones definitivas sobre los mecanismos de afrontamiento más utilizados.

Tabla 16. Acciones que tomaron las víctimas para lidiar con la ciberviolencia en los casos registrados por el equipo de Ciberadar, del 11 de febrero al 4 de junio 2026

Acción	Frecuencia	Porcentaje del total
Se desconoce	195	49%
Ninguna	92	23%
Publicó una aclaración en su cuenta personal o institucional	38	10%
Respondió públicamente a la persona sin agredirla	28	7%
Tomó acciones legales contra la persona	16	4%
Bloqueó o reportó la cuenta	8	2%
Agredió a la persona en línea o en persona	5	1%
Otras	13	3%
Total	395	100%

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

La Tabla 17 muestra una limitación semejante para identificar las consecuencias. En el 57% de las menciones no fue posible determinar las consecuencias específicas experimentadas por la víctima. Entre los casos en los que sí fue posible identificar algún impacto, el daño reputacional⁹ fue, con amplia diferencia, la consecuencia más frecuente (28%), reflejando que una parte importante de la ciberviolencia busca afectar la imagen pública, la credibilidad o la reputación de las personas frente a sus comunidades, audiencias o redes sociales.

En un segundo nivel aparecen las pérdidas económicas o daños materiales (6%), seguidas por los daños emocionales, como tristeza, angustia o miedo¹⁰ (4%). También se registraron consecuencias relacionadas con la afectación de la integridad sexual (2%) y daños psicológicos, incluyendo ansiedad,

depresión o pánico (2%). Los casos de homicidio, suicidio u otras afectaciones simbólicas fueron excepcionales.

En conjunto, estos resultados sugieren que la principal consecuencia observable de la ciberviolencia documentada por Ciberadar es el deterioro de la reputación pública de las víctimas, mientras que las afectaciones emocionales, psicológicas y económicas también constituyen impactos relevantes, aunque probablemente subregistrados debido a que muchas de estas consecuencias no son visibles en la información disponible públicamente. En el caso de las juventudes con presencia pública, el daño reputacional puede además debilitar su credibilidad frente a sus comunidades y reducir los márgenes desde los cuales ejercen liderazgo, realizan incidencia o participan en iniciativas de derechos humanos y construcción de paz.

Tabla 17. Consecuencias que tuvieron en las víctimas los casos de ciberviolencia registrados por el equipo de Ciberadar, del 11 de febrero al 4 de junio de 2026

Tipo de consecuencia	Frecuencia	Porcentaje del total
Se desconoce	225	57%
Daño reputacional (afectación de la imagen pública)	110	28%
Daño material (pérdidas económicas)	22	6%
Daño emocional (tristeza, angustia, miedo)	15	4%
Daño sexual (afectación de la integridad sexual)	8	2%



⁹El daño reputacional se documentó cuando las personas que sufrieron la acción violenta lo manifestaron expresamente o cuando la acción involucró la imagen o el nombre de la persona.

¹⁰En estos casos, solamente se documentó el daño emocional cuando la persona que sufrió la acción violenta lo manifestó expresamente.

Tipo de consecuencia	Frecuencia	Porcentaje del total
Daño psicológico (ansiedad, depresión, pánico)	6	2%
Otro	3	1%
Muerte a manos de otra persona	2	1%
Daño simbólico/cultural y de identidad	1	0%
Muerte por suicidio	1	0%
Total	393	100%

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

Caso ilustrativo.

Las consecuencias de la ciberviolencia pueden, en algunos casos, trascender ampliamente el espacio digital. Ciberadar documentó retrospectivamente el caso de María Nohemí Gómez, quien había sido coronada reina de la feria de San Juan Cotzal para el período 2023-2024. Durante 2023 recibió numerosos comentarios ofensivos en redes sociales relacionados con su apariencia física. De acuerdo con la información recopilada por el observatorio, el hostigamiento

masivo estuvo asociado con un proceso que culminó con su suicidio ese mismo año. Aunque se trata de un caso extremo y no permite establecer por sí mismo una relación causal entre una forma específica de agresión digital y el suicidio, este incidente ilustra la gravedad que pueden alcanzar las consecuencias de procesos prolongados de hostigamiento y la necesidad de analizar la ciberviolencia más allá del contenido individual de cada publicación o comentario.

★ Regreso a la teoría: finalidad, duración e intrusión

Los patrones anteriores permiten finalmente regresar a las tres dimensiones que constituyeron el punto de partida conceptual de Ciberadar. La Tabla 18 muestra las distintas categorías que surgen al considerar la duración de los hechos, su finalidad y su grado de intrusión. La mayoría de los casos registrados fueron efímeros: 244 ocurrieron una o dos veces, frente a 97 que se prolongaron tres o más veces. En cuanto

a la finalidad, 242 estuvieron dirigidos a hacer daño a la persona, mientras que 67 buscaron obtener algo de ella o impedir que realizara alguna acción. Finalmente, 273 casos se mantuvieron en el espacio público y fueron clasificados como no intrusivos, frente a 62 que invadieron la esfera privada de la persona.

Tabla 18. Duración, finalidad y grado de intrusión de los casos registrados por el equipo de Ciberadar, del 11 de febrero al 4 de junio de 2026

Duración	Cantidad de casos	Finalidad	Cantidad de casos	Grado de intrusión	Cantidad de casos
Efímera (1 o 2 veces)	244	Hacerle daño a la persona	242	No intrusiva (se mantuvo en el espacio público)	273
Prolongada (3 o más veces)	97	Obtener algo de la persona o impedir que la persona haga algo	67	Intrusiva (invadió la esfera privada de la persona)	62
Se desconoce	33	Se desconoce	65	Se desconoce	39
Total	374	Total	374	Total	374

Caso ilustrativo.

Las tres dimensiones utilizadas por Ciberadar permiten distinguir formas de ciberviolencia que pueden parecer similares pero funcionan mediante lógicas diferentes. Por ejemplo, en febrero de 2026 una persona creó un perfil falso de Instagram utilizando el nombre de Carlos Pérez. Desde la cuenta apócrifa comenzó a seguir a sus amistades y a solicitarles dinero haciéndose pasar por él. La víctima reportó posteriormente el perfil y la plataforma eliminó la cuenta.

Desde el marco analítico de Ciberadar, se trata de una acción utilitaria, porque la suplantación fue utilizada para intentar obtener dinero; intrusiva, porque implicó apropiarse de la identidad digital de la víctima y utilizar sus relaciones personales; y efímera, en la medida en que ocurrió una sola vez y el perfil fue identificado y eliminado en un período relativamente corto. El caso muestra la utilidad de analizar la ciberviolencia no solamente según la conducta observada

—en este caso, suplantación de identidad y fraude— sino también según su finalidad, duración y grado de intrusión.

En conjunto, los hallazgos confirman la utilidad de las dimensiones de finalidad, duración e intrusión para clasificar y comparar formas de ciberviolencia que, en apariencia, pueden ser similares o muy distintas y pueden a la vez tener efectos diversos. Sin embargo, el análisis empírico también muestra los límites de comprender el fenómeno únicamente a partir de estas dimensiones.

La primera ampliación consiste en reconocer quiénes participan en la producción del daño. Una agresión puede tener un blanco individual y, al mismo tiempo, ser producida o amplificada por decenas de usuarios. La dimensión colectiva permite comprender fenómenos como las ciberturbas, las páginas dedicadas a exponer personas y las campañas de desprestigio, en las que el daño surge de la acumulación de múltiples intervenciones.

La segunda ampliación exige incorporar el contexto en el que ocurre la agresión. Los ataques observados reproducen desigualdades relacionadas con género, orientación sexual, pertenencia étnica y posición social, pero también se articulan con conflictos políticos, debates públicos y disputas existentes fuera de Internet. La ciberviolencia aparece así como parte de un continuo entre las relaciones sociales que ocurren dentro y fuera de los espacios digitales.

Finalmente, la teoría debe considerar explícitamente el carácter tecnológicamente dinámico de la ciberviolencia. Las plataformas y herramientas disponibles no constituyen escenarios neutrales donde ocurre la violencia, sino que más bien sus características condicionan la capacidad de producir, transformar, reproducir y amplificar contenidos. La expansión de la inteligencia artificial generativa constituye un ejemplo particularmente claro de cómo una transformación tecnológica puede modificar las posibilidades de causar daño.

Desde esta perspectiva ampliada, la ciberviolencia emerge como un proceso social complejo en el que interactúan actores individuales y colectivos, estructuras históricas de poder y un entorno tecnológico en permanente evolución. Las tres dimensiones originales continúan proporcionando una herramienta para clasificar los casos según cómo ocurre la agresión. Sin embargo, los hallazgos de Ciberadar muestran que, para explicar por qué la ciberviolencia adopta determinadas formas, cómo se amplifica y qué significado adquiere, es necesario considerar también los actores colectivos que intervienen, el contexto social y político en el que ocurre y las capacidades que ofrece un entorno tecnológico en constante transformación. Esta perspectiva amplía el alcance interpretativo de la teoría y ofrece un marco más adecuado para orientar futuras investigaciones, así como el diseño de políticas públicas y estrategias de prevención adaptadas a los desafíos contemporáneos.

5 Conclusiones

La experiencia de Ciberadar muestra, en primer lugar, que la ciberviolencia constituye un fenómeno heterogéneo que difícilmente puede reducirse a una única conducta o categoría. Los casos documentados incluyen desde insultos, discursos discriminatorios y campañas de desprestigio hasta hostigamiento sexual, amenazas, fraudes, suplantaciones de identidad, difusión no consentida de contenidos y accesos no autorizados a información y sistemas digitales. Además, estas modalidades pueden combinarse dentro de un mismo episodio y transformarse a lo largo del tiempo. Esta diversidad confirma la utilidad de abordar la ciberviolencia mediante un marco suficientemente amplio para reconocer diferentes mecanismos de producción del daño y evitar definiciones restringidas exclusivamente al acoso o a los discursos de odio.

La teoría tridimensional desarrollada como punto de partida por Ciberadar proporciona una herramienta útil para ordenar esta diversidad. Analizar las agresiones según su finalidad, duración y grado de intrusión permite distinguir situaciones que pueden compartir una conducta observable pero responder a lógicas diferentes. En los casos documentados predominaron las acciones efímeras, dirigidas a causar daño y desarrolladas en espacios públicos digitales. Sin embargo, también se identificaron acciones prolongadas,

utilitarias e intrusivas que muestran formas diferentes de vulnerabilidad y requieren respuestas distintas. La principal contribución del ejercicio empírico, no obstante, fue mostrar que estas tres dimensiones son necesarias pero no suficientes para explicar plenamente el fenómeno.

Una primera ampliación consiste en reconocer la dimensión colectiva de la ciberviolencia¹¹. Los casos analizados muestran que el modelo de un agresor que actúa contra una víctima individual describe solamente una parte de las dinámicas observadas. Las plataformas digitales permiten que numerosas personas participen en la producción y amplificación del daño mediante comentarios, reacciones, publicaciones, réplicas y creación de nuevos contenidos. Páginas dedicadas a exponer personas, campañas de desprestigio y procesos de hostigamiento colectivo ilustran cómo el daño puede surgir de la acumulación de acciones realizadas incluso por usuarios que no mantienen ninguna coordinación explícita entre sí. Comprender estas dinámicas requiere prestar atención no solamente al iniciador de una agresión, sino también a las comunidades digitales y mecanismos de amplificación que se forman alrededor de ella.

Una segunda conclusión es que la distinción entre violencia digital y violencia fuera de Internet debe entenderse de



¹¹ Keats, *Hate Crimes in Cyberspace*, p. 5.

manera flexible¹². Los casos documentados muestran conexiones constantes entre ambos espacios. Conflictos políticos, desigualdades de género, racismo, transfobia, homofobia, disputas políticas y relaciones interpersonales pueden trasladarse a las plataformas digitales, donde encuentran nuevas posibilidades de expresión y amplificación. A su vez, una agresión iniciada en Internet puede producir consecuencias reputacionales, económicas, emocionales, psicológicas o sociales fuera de las plataformas. Esta continuidad implica que prevenir la ciberviolencia no puede limitarse a modificar comportamientos individuales en redes sociales, sino que requiere considerar también las relaciones de poder, formas de discriminación y conflictos sociales dentro de los cuales adquieren significado las agresiones.

Los patrones relacionados con género, pertenencia étnica y orientación sexual son especialmente ilustrativos. Entre los casos documentados, las características identitarias de las personas fueron utilizadas en repetidas ocasiones como recursos para insultar, desacreditar, sexualizar o excluir. Las agresiones dirigidas contra perfiles femeninos muestran un peso importante de los ataques basados en sexo o género y de la sexualización, mientras que entre los casos con víctimas mayas identificadas el origen étnico adquiere una relevancia particular como motivo de ataque. Los casos que involucran a personas trans y de la diversidad sexual muestran además que distintas formas de discriminación pueden superponerse dentro de una

misma agresión. Estos hallazgos no permiten establecer qué grupos enfrentan una mayor prevalencia de ciberviolencia en Guatemala, pero sí permiten observar los mecanismos mediante los cuales desigualdades y prejuicios existentes pueden reproducirse en los espacios digitales.

En el caso de las juventudes, Ciberadar aporta evidencia sobre algunas de las formas que puede adoptar la violencia digital contra personas de 15 a 29 años. Los casos con información etaria muestran la importancia de las agresiones relacionadas con sexo o género, reputación y apariencia física, así como diferencias entre perfiles femeninos y masculinos. Al mismo tiempo, la elevada proporción de casos en los que no pudo establecerse la edad impide realizar inferencias robustas sobre la distribución etaria de la ciberviolencia. Esta limitación refuerza la necesidad de desarrollar mecanismos de investigación específicamente diseñados para estudiar las experiencias de las juventudes, complementando la observación de espacios públicos digitales con otras metodologías que permitan conocer experiencias que difícilmente pueden identificarse mediante monitoreo abierto.

Una tercera ampliación de la teoría consiste en reconocer que la tecnología no funciona simplemente como el escenario donde ocurre la violencia. Las características de las plataformas influyen en la visibilidad, circulación, persistencia y amplificación de los contenidos, mientras que las transformaciones



¹² Organización de los Estados Americanos, *La violencia de género en línea*.

tecnológicas modifican continuamente las posibilidades disponibles para ejercer daño. La utilización de inteligencia artificial generativa en varios de los casos documentados muestra con particular claridad este proceso. La posibilidad de producir o modificar rápidamente imágenes, audios y otros contenidos permite fabricar representaciones falsas, sexualizadas o degradantes de personas reales y utilizarlas en procesos de difamación, ridiculización o manipulación. Esto sugiere que cualquier marco de análisis de la ciberviolencia deberá conservar suficiente flexibilidad para incorporar tecnologías y modalidades de agresión que todavía se encuentran en proceso de desarrollo.

Los casos de fraude, suplantación y ataques contra sistemas institucionales muestran otra dimensión de esta transformación. La violencia y el daño digital no se limitan a las relaciones interpersonales: pueden dirigirse contra organizaciones e instituciones y afectar indirectamente a grandes cantidades de personas mediante la exposición de información, la vulneración de sistemas o la apropiación de canales oficiales de comunicación. La digitalización creciente de actividades económicas, relaciones sociales y servicios públicos amplía, por tanto, las oportunidades de interacción y los espacios en los cuales pueden producirse distintas formas de daño.

Las consecuencias registradas refuerzan la necesidad de analizar la ciberviolencia más allá del contenido específico de una publicación o mensaje.

El daño reputacional aparece como la consecuencia observable más frecuente dentro del conjunto documentado, pero también se registraron afectaciones económicas, emocionales, psicológicas y sexuales. En una proporción elevada de casos, sin embargo, las consecuencias y las respuestas de las víctimas fueron desconocidas. Esta ausencia de información constituye en sí misma una limitación importante de los métodos basados en la observación de contenidos públicos: no es posible identificar plenamente una agresión sin conocer cómo fue experimentada por la persona afectada o qué ocurrió después de que desapareció de la pantalla. El desarrollo futuro de Ciberadar podría, por ello, complementar el monitoreo digital con mecanismos que permitan comprender mejor las trayectorias y consecuencias de los casos.

Finalmente, los resultados de este informe deben comprenderse de acuerdo con el propósito exploratorio del observatorio. Los 374 casos documentados no constituyen una muestra representativa de la ciberviolencia que ocurre en Guatemala y sus frecuencias no permiten estimar cuántas personas experimentan cada modalidad, qué grupos presentan mayor riesgo ni qué plataformas son intrínsecamente más violentas. Los patrones identificados dependen, entre otros factores, de los espacios observados, la accesibilidad de las interacciones, los criterios de búsqueda y la estrategia de máxima variación utilizada durante el monitoreo, así como de los propios sesgos del equipo de observación. El

aporte de Ciberadar se encuentra, por tanto, en mostrar empíricamente la diversidad de formas que puede adoptar la ciberviolencia, identificar mecanismos y patrones que merecen mayor investigación y desarrollar herramientas conceptuales y metodológicas para estudiarlos sistemáticamente.

A partir de esta experiencia, la ciberviolencia puede conceptualizarse como un proceso social complejo, individual y colectivo, contextual y tecnológicamente dinámico. Las dimensiones de finalidad, duración e intrusión permiten comprender cómo se desarrolla una agresión; la configuración de los actores ayuda a explicar cómo puede producirse y amplificarse; el contexto social y político permite entender por qué determinadas identidades, conflictos o desigualdades se convierten en ejes de agresión; y el entorno tecnológico determina parte de las posibilidades mediante las cuales el daño puede producirse y circular. Esta perspectiva ampliada constituye uno de los principales aportes de Ciberadar y ofrece una base para continuar

desarrollando investigación, prevención y respuestas institucionales frente a un fenómeno que seguirá transformándose junto con las tecnologías y las prácticas sociales que las rodean.

Leídos desde una perspectiva de Juventud, Paz y Seguridad, los hallazgos muestran que la ciberviolencia constituye un riesgo para el bienestar individual de las personas jóvenes. También puede reducir las condiciones necesarias para su participación significativa en la vida pública, al afectar su reputación, seguridad y disposición para expresarse en los espacios digitales. Este riesgo adquiere particular relevancia para quienes ejercen liderazgo, defienden derechos humanos o promueven el diálogo y la convivencia pacífica, pues el hostigamiento y el descrédito pueden operar como mecanismos de silenciamiento y exclusión. Por ello, prevenir y atender las ciberviolencias forma parte de la tarea más amplia de garantizar que las juventudes puedan contribuir de manera segura y efectiva a la construcción de sociedades pacíficas e inclusivas.

6 Recomendaciones



Para las plataformas digitales:

Fortalecer los mecanismos de detección y respuesta frente a discursos de odio, campañas coordinadas de hostigamiento, violencia basada en género facilitada por la tecnología y contenidos manipulados mediante inteligencia artificial, promoviendo procesos más ágiles, transparentes y centrados en la protección de las víctimas.



Para las instituciones del Estado:

Impulsar el fortalecimiento del marco legal y de los protocolos institucionales para la prevención, investigación, atención, sanción y reparación de las ciberviolencias, garantizando un enfoque de derechos humanos, género, interseccionalidad y protección integral de las víctimas.



Para la coordinación interinstitucional:

Consolidar mecanismos permanentes de coordinación entre instituciones públicas, sector educativo, sociedad civil, entre otros, para prevenir las ciberviolencias y promover entornos digitales seguros que favorezcan la participación cívica y política de las juventudes. Desde una perspectiva de Juventud, Paz y Seguridad, estos mecanismos deberían prestar especial atención a la protección y el acompañamiento de jóvenes que promueven los derechos humanos, el diálogo y la convivencia pacífica, evitando que las agresiones digitales restrinjan su liderazgo o incidencia.



Para las juventudes:

Fortalecer las capacidades en Alfabetización Mediática e Informativa (AMI), ciudadanía digital, seguridad digital y pensamiento crítico, dotándolas de herramientas para identificar riesgos, prevenir la desinformación, ejercer una participación segura en el ciberespacio y responder adecuadamente frente a situaciones de violencia digital.



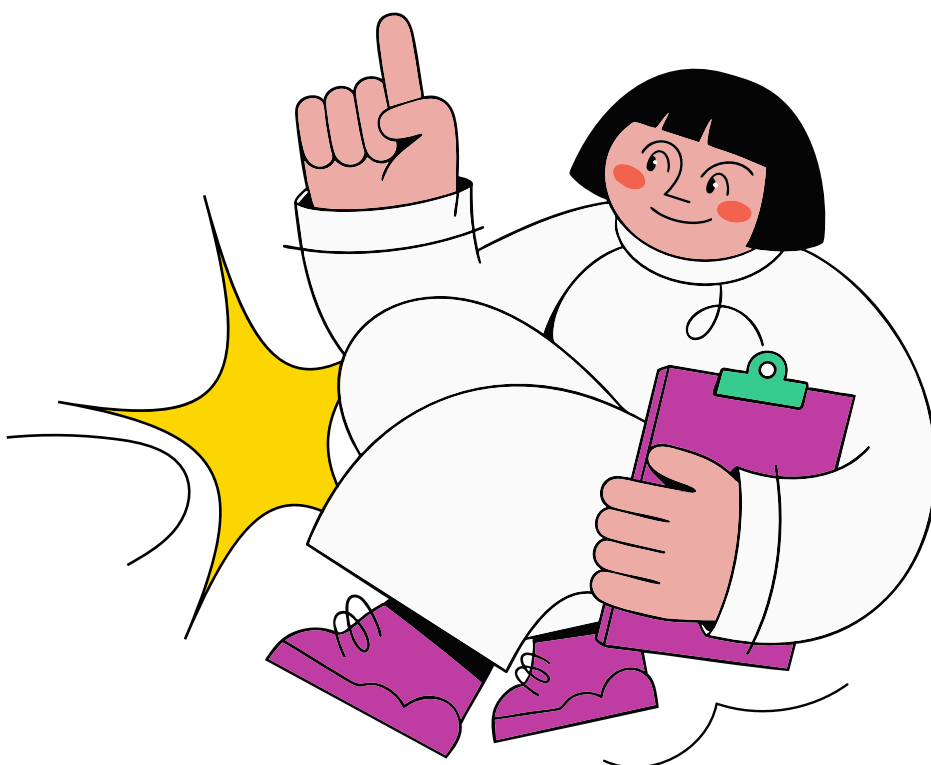
Para futuras investigaciones:

Desarrollar estudios longitudinales y metodologías mixtas que permitan comprender la evolución de la ciberviolencia, profundizar en su relación con la violencia política, la inteligencia artificial y los procesos de construcción de paz, así como analizar sus impactos diferenciados sobre las juventudes y otros grupos en situación de vulnerabilidad.



Para el fortalecimiento de la evidencia:

Consolidar y ampliar el Observatorio Ciberadar como un sistema permanente de monitoreo que incorpore nuevas plataformas digitales, metodologías complementarias y mecanismos de validación de la información, generando evidencia continua para orientar políticas públicas y estrategias de prevención.



7 Anexos

Anexo 1

Tipo de acciones violentas en el espacio digital

Ataques verbales y discurso de odio: Comentarios que incluyen palabras y expresiones ofensivas dirigidos a una persona, grupo o institución/organización, que buscan denigrar sus características personales, conducta o capacidades personales.

Ataque verbal o insulto **basado en el sexo/género**

Comentarios ofensivos que expresan odio, desprecio o aversión hacia una persona por su sexo, identidad de género o expresión de género, que reproducen estereotipos o prejuicios sobre el rol social de hombres, mujeres o personas con identidades de género diversas

Criterios de identificación

- Insultos dirigidos a mujeres, hombres o personas trans.
- Uso de estereotipos de género.
- Descalificación por el rol de género.

Ejemplo ilustrativo

"Las mujeres no deberían meterse en política."

Ataque verbal o insulto **basado en la apariencia física**

Comentario ofensivo o humillante dirigido a la apariencia física de una persona, incluyendo rasgos corporales, edad, peso, estatura o color de piel.

Criterios de identificación

- Ridiculiza rasgos físicos.
- Uso de comparaciones humillantes.
- Comentarios sobre edad o cuerpo.

Ejemplo ilustrativo

"Qué fea y ridícula se ve."

Ataque verbal o insulto **basado en la capacidad intelectual**

Expresión despectiva que cuestiona o ridiculiza la inteligencia, educación o habilidades cognitivas de una persona.

Criterios de identificación

- Insultos relacionados con inteligencia.
- Cuestiona conocimientos o educación.
- Ridiculiza capacidad mental.

Ejemplo ilustrativo

"Ese tipo es un ignorante."

Ataque verbal o insulto **basado en la orientación sexual**

Comentario ofensivo dirigido a una persona o grupo de personas por su orientación sexual real o percibida, que expresa odio, desprecio o aversión, y que se basa en prejuicios o estereotipos asociados a la diversidad sexual.

Criterios de identificación

- Uso de insultos homofóbicos.
- Descalificación por orientación sexual.
- Ridiculización de diversidad sexual.
- Orientaciones como gay, lesbiana, bisexual entre otras.

Ejemplo ilustrativo

"Ese marica no debería estar aquí."

Ataque verbal o insulto **basado en el origen étnico**

Comentario ofensivo dirigido a una persona o grupo de personas por su origen étnico, real o atribuido, que expresa odio, desprecio o aversión, y que reproduce ideas de inferioridad, estigmatización o discriminación.

Criterios de identificación

- Uso de insultos racistas.
- Ridiculización de cultura y/o idioma.
- Creencias con inferioridad moral, cultural y social.
- Poblaciones indígenas como Mayas, Garífunas, Xincas o Afrodescendientes.

Ejemplo ilustrativo

"Los indígenas son ignorantes."

Ataque verbal o insulto **basado en la posición socioeconómica**

Comentario despectivo que menosprecia a una persona por su nivel de ingresos, ocupación, condición económica o lugar de residencia.

Criterios de identificación

- Insultos relacionados con pobreza, clase social o lugar de residencia.
- Desprecio por el trabajo u ocupación de la persona.
- Estigmatización social.

Ejemplo ilustrativo

"Ese muerto de hambre quiere ser político."

Ataque verbal o insulto **basado en la ideología política**

Expresión ofensiva dirigida a una persona por sus creencias, afiliación o postura política, con el objetivo de desacreditarla o deslegitimar su opinión.

Criterios de identificación

- Insultos asociados a ideologías.
- Descalificación por afiliación política.
- Ridiculización de posturas políticas.

Ejemplo ilustrativo

"Ese comunista corrupto."

Palabras clave

comunista, zurdo, fascista, guerrillero etc.

Ataque verbal o insulto **basado en religión**

Expresión ofensiva o descalificadora dirigida a una persona por su religión, creencias espirituales o por no profesar ninguna religión, sustentada en prejuicios o intolerancia religiosa.

Criterios de identificación

- Ridiculiza creencias religiosas.
- Uso de prejuicios religiosos.
- Ataque a símbolos religiosos.

Ejemplo ilustrativo

"Ese fanático religioso está loco."

Ataque verbal o insulto **basado en nacionalidad/país de origen**

Expresión ofensiva dirigida a una persona por su nacionalidad, país de origen o condición migratoria, utilizando estereotipos o prejuicios asociados a su procedencia.

Criterios de identificación

- Uso de estereotipos nacionales.
- Insultos a migrantes.
- Desprecio por el país de origen.

Ejemplo ilustrativo

"Esos extranjeros vienen a robar."

Ataque verbal o insulto **basado en actividad profesional**

Expresión despectiva que desacredita o menosprecia a una persona por su ocupación, profesión u oficio, con la intención de disminuir su valor o legitimidad.

Criterios de identificación

- Desprestigio de una profesión.
- Uso de insultos asociados al trabajo.
- Ridiculización de ocupaciones.

Ejemplo ilustrativo

"Ese periodista muerto de hambre."

Ataque verbal o insulto **basado en algún tipo de discapacidad**

Comentario ofensivo dirigido a una persona por una discapacidad real o atribuida (visual, auditiva, física, motriz u otra), que expresa desprecio, aversión o burla, y que reproduce ideas de inferioridad, estigmatización o discriminación.

Criterios de identificación

- Uso de términos asociados a discapacidad como insulto.
- Burla o ridiculización de una limitación.
- Atribución de discapacidad de forma ofensiva.
- Asociación con incapacidad o inferioridad.

Ejemplo ilustrativo

"Sos un inválido, no servís para nada."

Difamación

Difusión de información falsa presentada como verdadera que daña la reputación de una persona o comunidad, afectando su honra o credibilidad ante terceros.

Criterios de identificación

- Acusaciones sin evidencia.
- Información falsa sobre conducta moral o legal o acción.
- Daño a la reputación.

Ejemplo ilustrativo

"Dicen que robó dinero público."

Amenazas: Sugerir o insinuar la intención de causar daño a una persona o grupo de personas, con el propósito de intimidar, generar miedo, presionar o condicionar su comportamiento.

Amenaza de **agresiones físicas**

Dar a entender, sugerir o insinuar que se tiene la intención de causar algún daño o lesiones sobre el cuerpo de una persona o grupo de personas.

Criterios de identificación

- Deseos de golpear o herir.
- Incitación a la violencia física.

Ejemplo ilustrativo

"A puro palo te voy a agarrar"

Amenaza de **agresiones sexuales**

Expresiones que dan a entender, sugieren o insinúan que se tiene la intención de realizar actos sexuales, tocamientos u otras conductas de carácter sexual sin el consentimiento de una persona o grupos de personas.

Criterios de identificación

- Uso de lenguaje sexual con intención de amenaza.
- Referencia a actos sexuales sin consentimiento.
- Insinuación de contacto físico sexual.

Ejemplo ilustrativo

"Cuidado que te pueden cxxx"

Amenaza de divulgación de **imágenes/videos/audios de carácter sexual**

Expresiones que dan a entender o sugieren la intención de publicar imágenes, videos o audios íntimos de una persona o grupo de personas sin consentimiento de la persona.

Criterios de identificación

- Amenaza de publicar material íntimo
- Chantaje con contenido sexual.

Ejemplo ilustrativo

"Voy a publicar tus packs."

Amenaza de divulgación de **información/videos/audios con información personal**

Advertencia o intención de hacer pública información privada, datos personales o contenido sensible de una persona sin su autorización, con el propósito de intimidar o perjudicarla.

Criterios de identificación

- Amenaza de publicar dirección, teléfono u otra información.
- Exposición de datos personales o de familiares

Amenaza de **acciones legales**

Advertencia de iniciar procesos judiciales o denuncias formales contra una persona o grupo de personas, utilizada de manera intimidatoria para presionar, silenciar o influir en su comportamiento.

Criterios de identificación

- Amenazas de denuncias.
- Uso intimidatorio de procesos legales.

Amenazas **contra la vida de la persona**

Dar a entender o sugerir que se tiene la intención de causar la muerte de una persona o grupo de personas.

Criterios de identificación

- Deseos de muerte.
- Amenazas directas de intención de matar

Hostigamiento sexual digital: Envío de mensajes, comentarios o contenidos de carácter sexual no solicitados, dirigidos a una persona.

Envío de mensajes con **insinuaciones sexuales**

Envío de mensajes, comentarios o solicitudes con connotación sexual no solicitada.

Criterios de identificación

- Comentarios sexuales no deseados.
- Insinuaciones o propuestas sexuales.

Ejemplo ilustrativo

"Me gusta tu cuerpo."

Envío de mensajes **con imágenes/videos de genitales o partes íntimas**

Envío de imágenes/videos en distintos formatos con partes íntimas o genitales sin consentimiento de la persona receptora.

Criterios de identificación

- Envío de fotos íntimas no solicitadas.
- Contenido sexual explícito.

Ejemplo ilustrativo

Envío de fotografía de genitales en un mensaje.

Engaño, fraude y manipulación: uso de información falsa, engañosa o manipulada para inducir a error a una persona o grupo, con el propósito de obtener un beneficio indebido, influir en su comportamiento o causar perjuicio.

Envío de mensajes con **contenido engañoso**

Envío de mensajes o contenido que contienen información falsa, manipulada o distorsionada como si fuera verídica, con el objetivo de confundir, desinformar o influir en la percepción o conducta de la persona receptora

Criterios de identificación

- Información falsa.
- Manipulación de texto, imágenes o mensajes.

Ejemplo ilustrativo

Publicación que difunde información falsa sobre un hecho político

Estafa

Acción mediante la cual una persona obtiene un beneficio económico o material a través del engaño, induciendo a otra persona o grupo de personas con información falsa o manipulada.

Criterios de identificación

- Solicitud de dinero con información falsa.
- Promesas engañosas de beneficios económicos.

Ejemplo ilustrativo

Mensaje que solicita una transferencia de dinero haciéndose pasar por una institución o persona conocida.

Vigilancia, control y acceso no autorizado: Conductas que implican el monitoreo, control, obtención o uso no autorizado de información, cuentas o contenidos de una persona, con el fin de vigilarla, suplantarla, manipularla o causarle perjuicio.

Vigilancia cibernética

Monitoreo, seguimiento u observación constante de la actividad digital de una persona sin su consentimiento, con el fin de controlar, recopilar información o invadir su privacidad. También puede dar a entender que se vigila o realiza proposiciones insistentemente con el fin de causar miedo y angustia emocional a una persona.

Criterios de identificación

- Seguimiento reiterado de la actividad digital.
- Mensajes que indican vigilancia o control.
- Referencias a la ubicación o actividades de la persona.

Robo de información personal (número de identificación, cuentas bancarias o datos de tarjeta de crédito, teléfono, dirección, etc.)

Obtención, acceso o uso no autorizado de datos personales sensibles con el propósito de cometer fraude, suplantación o causar perjuicio.

Criterios de identificación

- Acceso a datos privados.
- Uso de información personal.

Robo de imágenes personales

Obtención, copia o uso no autorizado de fotografías o imágenes privadas de una persona, vulnerando su derecho a la intimidad.

Criterios de identificación

- Copia de imágenes privadas.
- Uso de fotos sin consentimiento.

Ejemplo ilustrativo

Publicar fotos privadas sin consentimiento

Suplantación de identidad digital (hacerse pasar por otra persona)

Creación o utilización de perfiles, cuentas o comunicaciones digitales haciéndose pasar por otra persona sin su consentimiento, con el fin de engañar o perjudicar.

Criterios de identificación

- Perfil falso.
- Uso del nombre o imagen de otra persona.

Ejemplo ilustrativo

Crear una cuenta falsa con el nombre o información de otra persona.

Robo de identidad digital (controlar cuentas digitales de otra persona)

Acceso y control no autorizado de las cuentas digitales de una persona o institución (como redes sociales o correo electrónico), asumiendo su identidad para realizar acciones en su nombre.

Criterios de identificación

- Acceso a cuentas ajenas.
- Uso de perfiles sin permiso.

Ejemplo ilustrativo

Manejar la cuenta de Facebook de otra persona sin su permiso

Difusión no consentida de contenido: Conductas que implican la publicación, distribución o circulación de contenido (imágenes, videos, audios o información) de una persona sin su consentimiento

Difusión de imágenes / videos / audios con información personal

Publicar, compartir o distribuir contenido audiovisual que contenga datos personales o información privada de una persona sin su consentimiento.

Criterios de identificación

- Exposición de información privada.
- Difusión de datos personales.

Difusión de imágenes / videos / audios de índole sexual sin consentimiento (packs)

Publicar, compartir o distribuir contenido íntimo o sexual de una persona sin su autorización, independientemente de cómo se haya obtenido.

Criterios de identificación

- Compartir packs o material sexual.
- Difusión de contenido íntimo.

Difusión de imágenes / videos / audios personales modificadas por medio de IA

Publicar, compartir o distribuir contenido audiovisual que ha sido alterado o manipulado mediante herramientas de inteligencia artificial para modificar, distorsionar o fabricar situaciones relacionadas con una persona, sin su consentimiento

Criterios de identificación

- Uso de deepfakes.
- Manipulación digital de imágenes.

Ejemplo ilustrativo:

Video falso generado con IA.

Difusión de imágenes / videos / audios de índole sexual modificadas por medio de IA

Publicar, compartir o distribuir contenido íntimo o sexual generado o alterado mediante inteligencia artificial (por ejemplo, montajes o “deepfakes”) que involucra a una persona sin su consentimiento.

Criterios de identificación

- Deepfakes sexuales.
- Imágenes sexuales falsas.

Ejemplo ilustrativo:

Imagen sexual falsa creada con IA.

Anexo 2

Formulario equipo Ciberadar

Versión compacta del instrumento. El asterisco () identifica preguntas obligatorias; las instrucciones de salto se conservan dentro de las opciones.*

A. Identificación y descripción del caso

1. Código de observador *

[Respuesta abierta]

2. Describa el caso de ciberviolencia * Responda: quién le hizo qué a quién, por qué medio, cuándo y dónde.

[Respuesta abierta]

B. Caracterización de quien ejerció la ciberviolencia

3. ¿Quién ejerció la ciberviolencia? *

Opciones: Se desconoce Ir a la pregunta 35 • Individuo Ir a la pregunta 5 • Grupo de individuos Ir a la pregunta 4 • Entidad u organización Ir a la pregunta 9

4. Tamaño del grupo que ejerció la violencia *

Opciones: Se desconoce • Entre 2 y 10 personas • De 11 a 20 personas • De 21 a 30 personas • De 31 a 40 personas • De 41 a 50 personas • Más de 50 personas

5. Género de quien ejerció la violencia *

Opciones: Se desconoce • Masculino • Femenino • Transgénero • Otros:

6. Edad de quien ejerció la violencia *

Opciones: Se desconoce • 10 a 14 años • 15 a 19 años • 20 a 24 años • 25 a 29 años • 30 a 34 años • 35 a 39 años • 40 a 44 años • 45 a 49 años • 50 o más

7. Pueblo de origen de quien ejerció la violencia *

Opciones: Se desconoce • Maya • Garífuna • Xinka • Afrodescendiente/Creole/Fromestizo • Ladino/ mestizo • Extranjero

8. Orientación sexual de quien ejerció la ciberviolencia *

Opciones: Se desconoce • Lesbiana • Gay • Bisexual • Heterosexual • Otros:

9. Ubicación del individuo que ejerció la ciberviolencia *

En caso de que el individuo no se encuentre en Guatemala, puedes marcar "otros" y especificar el país.

Opciones: Se desconoce Ir a la pregunta 33 • Guatemala Ir a la pregunta 10 • Otros:

10. Departamento en donde se encontraba la persona que ejerció la ciberviolencia *

Opciones: Se desconoce • Guatemala Ir a la pregunta 11 • El Progreso Ir a la pregunta 12 • Sacatepéquez Ir a la pregunta 13 • Chimaltenango Ir a la pregunta 14 • Escuintla Ir a la pregunta 15 • Santa Rosa Ir a la pregunta 16 • Sololá Ir a la pregunta 17 • Totonicapán Ir a la pregunta 18 • Quetzaltenango Ir a la pregunta 19 • Suchitepéquez Ir a la pregunta 20 • Retalhuleu Ir a la pregunta 21 • San Marcos Ir a la pregunta 22 • Huehuetenango Ir a la pregunta 23 • Quiché Ir a la pregunta 24 • Baja Verapaz Ir a la pregunta 25 • Alta Verapaz Ir a la pregunta 26 • Petén Ir a la pregunta 27 • Izabal Ir a la pregunta 28 • Zacapa Ir a la pregunta 29 • Chiquimula Ir a la pregunta 30 • Jalapa Ir a la pregunta 31 • Jutiapa Ir a la pregunta 32 • Ir a la pregunta 33

C. Ubicación municipal (preguntas condicionales 11-32 y 43-64)

Las preguntas 11-32 registran el municipio de quien ejerció la ciberviolencia y las preguntas 43-64 registran el municipio de quien la sufrió. En ambos casos se utiliza el mismo catálogo departamental:

Departamento	Victimario	Víctima	Opciones de municipio
Guatemala	P. 11	P. 43	Se desconoce • Guatemala • Santa Catarina Pinula • San José Pinula • San José del Golfo • Palencia • Chimaltán • San Pedro Ayampuc • Mixco • San Pedro Sacatepéquez • San Juan Sacatepéquez • San Raymundo • Chuarrancho • Fraijanes • Amatitlán • Villa Nueva • Villa Canales • Petapa
El Progreso	P. 12	P. 44	Se desconoce • Guastatoya • Morazán • San Agustín Acasaguastlán • San Cristóbal Acasaguastlán • El Jicaro • Sansare • Sanarate

Departamento	Victimario	Víctima	Opciones de municipio
Sacatepéquez	P. 13	P. 45	Se desconoce • Antigua Guatemala • Jocotenango • Pastores • Sumpango • Santo Domingo Xenacoj • Santiago Sacatepéquez • San Bartolomé Milpas Altas • San Lucas Sacatepéquez • Santa Lucía Milpas Altas • Magdalena Milpas Altas • Santa María de Jesús • Ciudad Vieja • San Miguel Dueñas • San Juan Alotenango • San Antonio Aguas Calientes • Santa Catarina Barahona
Chimaltenango	P. 14	P. 46	Se desconoce • Chimaltenango • San José Poaquil • San Martín Jilotepeque • Comalapa • Santa Apolonia • Tecpán Guatemala • Patzún • San Miguel Pochuta • Patzicía • Santa Cruz Balanyá • Acatenango • San Pedro Yepocapa • San Andrés Itzapa • Parramos • Zaragoza • El Tejar
Escuintla	P. 15	P. 47	Se desconoce • Escuintla • Santa Lucía Cotzumalguapa • La Democracia • Siqinalá • Masagua • Tiquisate • La Gomera • Guanagazapa • San José • Itzapa • Palín • San Vicente Pacaya • Nueva Concepción • Sipacate
Santa Rosa	P. 16	P. 48	Se desconoce • Cuilapa • Barberena • Santa Rosa de Lima • Casillas • San Rafael Las Flores • Oratorio • San Juan Tecuaco • Chiquimulilla • Taxisco • Santa María Ixhuatán • Guazacapán • Santa Cruz Naranjo • Pueblo Nuevo Viñas • Nueva Santa Rosa
Sololá	P. 17	P. 49	Se desconoce • Sololá • San José Chacayá • Santa María Visitación • Santa Lucía Utatlán • Nahualá • Santa Catarina Ixtahuacán • Santa Clara La Laguna • Concepción • San Andrés Semetabaj • Panajachel • Santa Catarina Palopó • San Antonio Palopó • San Lucas Tolimán • Santa Cruz La Laguna • San Pablo La Laguna • San Marcos La Laguna • San Juan La Laguna • San Pedro La Laguna • Santiago Atitlán
Totonicapán	P. 18	P. 50	Se desconoce • Totonicapán • San Cristóbal Totonicapán • San Francisco El Alto • San Andrés Xecul • Momostenango • Santa María Chiquimula • Santa Lucía La Reforma • San Bartolo Aguas Calientes
Quetzaltenango	P. 19	P. 51	Se desconoce • Quetzaltenango • Salcajá • Olinstepeque • San Carlos Sija • Sibilia • Cabricán • Cajolá • San Miguel Sigüilá • San Juan Ostuncalco • San Mateo • Concepción Chiquirichapa • San Martín Sacatepéquez • Almolonga • Cantel • Huitán • Zunil • Colomba • San Francisco La Unión • El Palmar • Coatepeque • Génova • Flores Costa Cuca • La Esperanza • Palestina de Los Altos
Suchitepéquez	P. 20	P. 52	Se desconoce • Mazatenango • Cuyotenango • San Francisco Zapotitlán • San Bernardino • San José el Ídolo • Santo Domingo Suchitepéquez • San Lorenzo • Samayac • San Pablo Jocopilas • San Antonio Suchitepéquez • San Miguel Panán • San Gabriel • Chicacao • Patulul • Santa Bárbara • San Juan Bautista • Santo Tomas la Unión • Zunilito • Pueblo Nuevo • Río Bravo • San José La Máquina
Retalhuleu	P. 21	P. 53	Se desconoce • Retalhuleu • San Sebastián • Santa Cruz Muluá • San Martín Zapotitlán • San Felipe • San Andrés Villa Seca • Champerico • Nuevo San Carlos • El Asintal
San Marcos	P. 22	P. 54	Se desconoce • San Marcos • San Pedro Sacatepéquez • San Antonio Sacatepéquez • Comitancillo • San Miguel Ixtahuacán • Concepción Tutuapa • Tacaná • Sibinal • Tajumulco • Tejutla • San Rafael Pie de la Cuesta • Nuevo Progreso • El Tumbador • San José el Rodeo • Malacatán • Catarina • Ayutla • Ocos • San Pablo • El Quetzal • La Reforma • Pajapita • Ixchiguan • San José Ojetenam • San Cristóbal Cucho • Sipacapa • Esquipulas Palo Gordo • Río Blanco • San Lorenzo • La Blanca
Huehuetenango	P. 23	P. 55	Se desconoce • Huehuetenango • Chiantla • Malacatancito • Cuilco • Nentón • San Pedro Necta • Jacaltenango • San Pedro Soloma • San Ildefonso Ixtahuacán • Santa Bárbara • La Libertad • La Democracia • San Miguel Acatán • San Rafael La Independencia • Todos Santos Cuchumatán • San Juan Atitán • Santa Eulalia • San Mateo Ixtatán • Colotenango • San Sebastián Huehuetenango • Tectitán • Concepción Huista • San Juan Ixcay • San Antonio Huista • San Sebastián Coatán • Barrillas • Aguacatán • San Rafael Petzal • San Gaspar Ixchil • Santiago Chimaltenango • Santa Ana Huista • Unión Cantinil • Petatán
Quiché	P. 24	P. 56	Se desconoce • Santa Cruz del Quiché • Chiché • Chinique • Zacualpa • Chajul • Chichicastenango • Patzité • San Antonio Ilotenango • San Pedro Jocopilas • Cunén • San Juan Cotzal • Joyabaj • Santa María Nebaj • San Andrés Sajcabajá • San Miguel Uspantán • Sacapulas • San Bartolomé Jocotenango • Canillá • Chicamán • Ixcán • Pachalum
Baja Verapaz	P. 25	P. 57	Se desconoce • Salamá • San Miguel Chicaj • Rabinal • Cubulco • Granados • El Chol • San Jerónimo • Purulhá

Departamento	Victimario	Víctima	Opciones de municipio
Alta Verapaz	P. 26	P. 58	Se desconoce • Cobán • Santa Cruz Verapaz • San Cristóbal Verapaz • Tactic • Tamahú • Tucurú • Panzós • Senahú • San Pedro Carchá • San Juan Chamelco • Lanquín • Cahabón • Chisec • Chahal • Fray Bartolomé de Las Casas • Santa Catarina La Tinta • Raxruhá
Petén	P. 27	P. 59	Se desconoce • Flores • San José • San Benito • San Andrés • La Libertad • San Francisco • Santa Ana • Dolores • San Luis • Sayaxché • Melchor de Mencos • Poptún • Las Cruces • El Chal
Izabal	P. 28	P. 60	Se desconoce • Puerto Barrios • Livingston • El Estor • Morales • Los Amates
Zacapa	P. 29	P. 61	Se desconoce • Zacapa • Estandueta • Río Hondo • Gualán • Teculután • Usumatlán • Cabañas • San Diego • La Unión • Huité • San Jorge
Chiquimula	P. 30	P. 62	Se desconoce • Chiquimula • San José La Arada • San Juan Ermita • Jocotán • Camotán • Olopa • Esquipulas • Concepción las Minas • Quezaltepeque • San Jacinto • Ipala
Jalapa	P. 31	P. 63	Se desconoce • Jalapa • San Pedro Pinula • San Luis Jilotepeque • San Manuel Chaparrón • San Carlos Alzatate • Monjas • Mataquescuintla
Jutiapa	P. 32	P. 64	Se desconoce • Jutiapa • El Progreso • Santa Catarina Mita • Agua Blanca • Asunción Mita • Yupiltepeque • Atescatempa • Jerez • El Adelanto • Zapotitlán • Comapa • Jalpatagua • Conguaco • Moyuta • Pasaco • San José Acatempa • Quesada

D. Caracterización de la víctima y relación con el victimario

33. Tipo de individuo o individuos que ejercieron la violencia (puedes seleccionar más de uno) *

Opciones: Particular(es) • Actor(es) político(s) o partidario(s) • Funcionario(s) público(s) • Activista(s) o defensor(es) de derechos • Lideresa(s) o líder(es) comunitario(s) • Periodista(s) o trabajador(es) de medios • Creador(es) de contenido / influencer(s) • Empresa privada • Organización social (ONG, sindicato, colectivo, etc.) • Institución pública • Partido político • Medio de comunicación • Se desconoce • Otros:

34. Alguna otra característica importante del individuo que ejerció la ciberviolencia Detallar características del individuo o grupo de personas, como por ejemplo si pertenece a una organización juvenil, partido político o institución.

[Respuesta abierta]

35. ¿Quién sufrió la violencia? *

Opciones: Individuo Ir a la pregunta 37 • Grupo de individuos Ir a la pregunta 36 • Entidad u organización Ir a la pregunta 41 • Se desconoce Ir a la pregunta 68

36. Tamaño del grupo que sufrió la violencia *

Opciones: Entre 2 y 10 personas • De 11 a 20 personas • De 21 a 30 personas • De 31 a 40 personas • De 41 a 50 personas • Más de 50 personas • Se desconoce • Ir a la pregunta 37

37. Género de quien sufrió la violencia *

Opciones: Masculino • Femenino • Transgénero • Otro • Se desconoce

38. Edad de quien sufrió la violencia (en años) *

Opciones: 0 a 4 años • 5 a 9 años • 10 a 14 años • 15 a 19 años • 20 a 24 años • 25 a 29 años • 30 a 34 años • 35 a 39 años • 40 a 44 años • 45 a 49 años • 50 o más años • Se desconoce

39. Pueblo de origen de quien sufrió la violencia *

Opciones: Maya • Garífuna • Xinka • Afrodescendiente/creole/afromestizo • Ladino/ Mestizo • Extranjero • Se desconoce

40. Orientación sexual de quien sufrió la ciberviolencia *

Opciones: Lesbiana • Gay • Bisexual • Heterosexual • Se desconoce • Otros:

41. Ubicación del individuo o grupo que sufrió la ciberviolencia *

En caso de que el individuo no se encuentre en Guatemala, puedes marcar "otros" y especificar el país.

Opciones: Guatemala Ir a la pregunta 42 • Se desconoce Ir a la pregunta 65 • Otros:

42. Departamento en donde se encontraba la persona que sufrió la ciberviolencia *

Opciones: Se desconoce Ir a la pregunta 65 • Guatemala Ir a la pregunta 43 • El Progreso Ir a la pregunta 44 • Sacatepéquez Ir a la pregunta 45 • Chimaltenango Ir a la pregunta 46 • Escuintla Ir a la pregunta 47 • Santa Rosa Ir a la pregunta 48 • Sololá Ir a la pregunta 49 • Totonicapán Ir a la pregunta 50 • Quetzaltenango Ir a la pregunta 51 • Suchitepéquez Ir a la pregunta 52 • Retalhuleu Ir a la pregunta 53 • San Marcos Ir a la pregunta 54 • Huehuetenango Ir a la pregunta 55 • Quiché Ir a la pregunta 56 • Baja Verapaz Ir a la pregunta 57 • Alta Verapaz Ir a la pregunta 58 • Petén Ir a la pregunta 59 • Izabal Ir a la pregunta 60 • Zacapa Ir a la pregunta 61 • Chiquimula Ir a la pregunta 62 • Jalapa Ir a la pregunta 63 • Jutiapa Ir a la pregunta 64

65. Tipo de individuo o individuos que sufrió la violencia (puedes seleccionar más de uno) *

Opciones: Particular(es) • Actor(es) político(s) o partidario(s) • Funcionario(s) público(s) • Activista(s) o defensor(es) de derechos • Periodista(s) o trabajador(es) de medios • Creador(es) de contenido / influencer(s) • Empresa privada • Organización social (ONG, sindicato, colectivo, etc.) • Institución pública • Partido político • Medio de comunicación • Se desconoce • Lideresa(s) o líder(es) comunitario(s) • Otros:

66. Alguna otra característica importante del individuo o grupo que sufrió la ciberviolencia

[Respuesta abierta]

67. ¿Qué tipo de relación existía o existe entre la víctima y el victimario?

Opciones: Ninguna • Afectiva/Íntima (parejas, ex parejas) • Familiar/De parentesco (padres, hermanos, tíos, primos, cuñados) • Social de trabajo (compañeros o ex compañeros de trabajo, jefes, empleados, clientes) • Institucional/Política (miembros de partidos políticos, funcionarios públicos, activistas) • Exclusivamente digital (seguidores o haters recurrentes, miembros de comunidad digital, influencers) • Se desconoce • Otros:

E. Acciones, finalidad y medios del incidente

68. ¿Qué acciones de violencias involucró el incidente? *

Opciones: Ataques verbales y discursos de odio • Amenazas • Hostigamiento sexual digital • Engaño, fraude y manipulación • Vigilancia, control y acceso no autorizado • Difusión no consentida de contenido • Se desconoce • Otros:

69. Especifique el tipo de ataque verbal y/o discurso de odio

Opciones: No aplica • Ataque verbal o insulto basado en el sexo/género • Ataque verbal o insulto basado en la apariencia física • Ataque verbal o insulto basado en la capacidad intelectual • Ataque verbal o insulto basado en la orientación sexual • Ataque verbal o insulto basado en el origen étnico • Ataque verbal o insulto basado en la posición socio económica • Ataque verbal o insulto basado en la ideología política • Ataque verbal o insulto basado en religión • Ataque verbal o insulto basado en nacionalidad/país de origen • Ataque verbal o insulto basado en actividad profesional • Ataque verbal o insulto basado en algún tipo de discapacidad (visual, auditiva, física o motriz)) • Difamación • Se desconoce • Otros:

70. Especifique el tipo de amenaza

Opciones: No aplica • Amenaza de agresiones físicas • Amenaza de agresiones sexuales • Amenaza de divulgación de imágenes/videos /audios de carácter sexual • Amenaza de divulgación de información/videos/audios con información personal • Amenaza de acciones legales • Amenaza contra la vida de la persona • Amenaza de pérdida de empleo o perjuicio laboral/ económico • Se desconoce

71. Especifique el tipo de hostigamiento sexual digital

Opciones: No aplica • Envío de mensajes con insinuaciones sexuales • Envío de mensajes con imágenes/videos de genitales o partes íntimas • Se desconoce

72. Especifique el tipo de engaño, fraude y/o manipulación

Opciones: No aplica • Envío de mensajes con contenido engañoso • Estafa • Se desconoce

73. Especifique el tipo de vigilancia, control y/o acceso no autorizado

Opciones: No aplica • Vigilancia cibernética • Robo de información personal (número de identificación, cuentas bancarias o datos de tarjeta de crédito, teléfono, dirección, etc.) • Robo de imágenes personales • Suplantación de identidad digital (hacerse pasar por otra persona) • Robo de identidad digital (controlar cuentas digitales de otra persona) • Se desconoce

74. Especifique el tipo de difusión no consentida de contenido

Opciones: No aplica • Difusión de imágenes/videos/audios con información personal • Difusión de imágenes/videos/audios de índole sexual sin consentimiento (packs) • Difusión de imágenes/videos/audios personales modificados por medio de IA • Difusión de imágenes/videos/audios de índole sexual modificados por medio de IA • Se desconoce

75. ¿Cuál fue la duración del caso de ciberviolencia?

Opciones: Ocurrió una o dos veces • Ocurrió tres o más veces • Se desconoce

76. ¿Cuál fue la finalidad del caso de ciberviolencia?

Opciones: Hacerle daño a la persona Ir a la pregunta 78 • Obtener algo (información, dinero, favores sexuales, bienes materiales) de la persona o impedir que la persona haga algo • Se desconoce Ir a la pregunta 78

77. ¿Qué se quiere obtener o impedir?

Opciones: Se desconoce • Obtener información personal • Obtener dinero • Obtener favores sexuales • Obtener bienes materiales • Impedir la participación cívica • Impedir la participación política • Impedir que la persona denunciara • Impedir el ejercicio profesional o laboral • Otros:

78. ¿Cuál fue el grado de intrusión del caso de ciberviolencia?

Opciones: Ocurrió o se mantuvo en un espacio público, a la vista de todos • Invadió los espacios personales o la vida privada de la persona sin su consentimiento (la persona recibió un correo electrónico o un mensaje directo en su teléfono o redes sociales, se publicaron fotografías íntimas o información personal o familiar de la persona) • Se desconoce

79. ¿Qué medio se usó para ejercer la violencia?

Opciones: Facebook • X • Instagram • WhatsApp • Tik Tok • Zoom • Snapchat • YouTube • Telegram • Signal • Roblox (videojuego) • Free fire (videojuego) • Bumble (Citas) • Grindr (Citas) • Tinder (Citas) • Otro • Se desconoce

80. El perfil desde donde se realizó la agresión era:

Opciones: No aplica • Se desconoce • Perfil con nombre real de la persona • Perfil con seudónimo (alias) • Perfil anónimo (sin identidad clara o solo con el usuario) • Página • Grupo • Cuenta institucional

F. Fecha, respuesta y consecuencias

81. ¿En qué año ocurrió el caso de ciberviolencia? (conteste solo si lo sabe)

Opciones: 2010 • 2011 • 2012 • 2013 • 2014 • 2015 • 2016 • 2017 • 2018 • 2019 • 2020 • 2021 • 2022 • 2023 • 2024 • 2025 • 2026 • 2027 • 2028

82. ¿En qué mes y día ocurrió el caso de ciberviolencia? (conteste solo si lo sabe)
Ejemplo: 7 de enero

[Respuesta abierta]

83. ¿Qué acciones tomó la víctima para lidiar con el caso de ciberviolencia?

Opciones: Ninguna • Respondió públicamente a la persona sin agredirla • Publico una aclaración en su cuenta personal o institucional • Cerró la cuenta • Bloqueo o reporto la cuenta • Agredió a la persona en línea o en persona • Tomó acciones legales contra la persona • Se desconoce • Otros:

84. ¿Qué consecuencias tuvo el caso de ciberviolencia en la vida de la víctima?

Seleccione esta opción únicamente si la persona afectada manifestó explícitamente esta consecuencia.

Opciones: Daño material (pérdidas económicas) • Daño reputacional (afectación de imagen pública) • Daño emocional (tristeza, angustia, miedo) • Daño psicológico (ansiedad, depresión, pánico) • Daño sexual (afectación de la integridad sexual) • Daño físico (lesiones corporales) • Muerte por suicidio (suicidio consumado) • Muerte a manos de otra persona • *Se desconoce

* Otros

G. Fuentes, evidencias y observaciones

85. Fuente

Opciones: Tú sufriste la agresión • Tú lo presenciaste directamente en una red social o plataforma digital • A tí te lo dijo la víctima • A tí te lo dijo una tercera persona • Tú lo leíste en un medio digital o escrito • Otro

86. ¿Qué evidencia tiene para verificar el incidente?

Opciones: Link a un reporte en Internet • Captura de pantalla o fotografía • Captura de video • Captura de audio • No está verificado.

87. Pegue el link del reporte en internet

[Respuesta abierta]

88. Suba la captura de pantalla o fotografía (<10MB)

[Carga de archivo]

89. Suba el video (<10MB)

[Carga de archivo]

90. Suba el audio (<10MB)

[Carga de archivo]

91. Comentarios adicionales

[Respuesta abierta]

DIÁLOGOS

