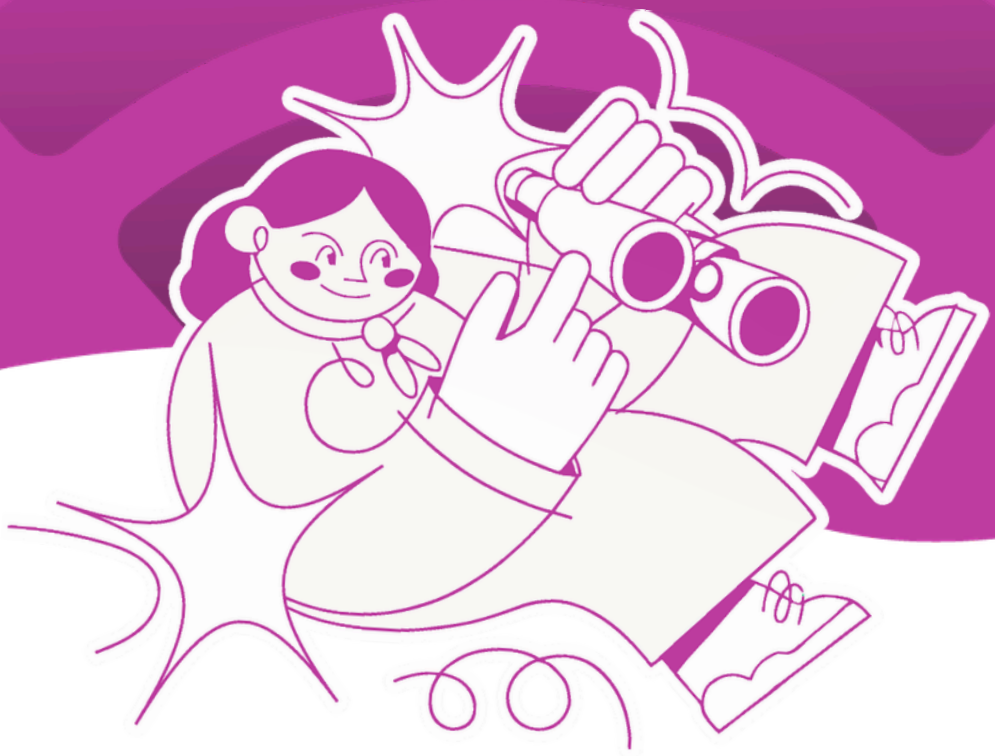
DIÁLOGOS



NOTA METODOLÓGICA

Juventudes por espacios digitales seguros

ciberadar
Juventudes por espacios digitales seguros

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

NOTA METODOLÓGICA
Juventudes por espacios digitales seguros

Ciberadar tiene como objetivo identificar, documentar y analizar casos ilustrativos de ciberviolencia en Guatemala, con énfasis en las experiencias que afectan a juventudes, mujeres, niñez y poblaciones históricamente vulnerabilizadas. El monitoreo busca comprender las formas, dinámicas, actores, plataformas y efectos de la ciberviolencia, así como generar evidencia que sirva como insumo para la discusión de políticas públicas y estrategias de prevención y atención.

El monitoreo se realiza a partir de una metodología mixta con predominio cualitativo, que combina la observación sistemática de plataformas digitales, el registro de casos reportados por terceros y el análisis de los patrones del fenómeno. El alcance temporal del monitoreo comprende cuatro meses de observación (febrero a mayo de 2026), con cortes semanales, y tiene un alcance nacional, cubriendo distintas plataformas digitales utilizadas en Guatemala.

1. Definiciones de variables, categorías o indicadores

Para fines prácticos, en Ciberadar la ciberviolencia se define de la siguiente manera:

Ciberviolencia
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.

Como teoría de partida, planteamos que la ciberviolencia varía según tres dimensiones: su duración, su finalidad y su grado de intrusión.

Tabla 1. **Dimensiones de la ciberviolencia**

Dimensión	Categorías	Definición
Duración: Tiempo durante el cual ocurre el acto de ciberviolencia	Efímera	Los casos efímeros ocurren de manera puntual o breve, como en un comentario en una transmisión en vivo o en el envío de un solo correo electrónico.
	Prolongada	Los casos prolongados en el tiempo ocurren de manera repetida y sostenida, como en las campañas de desprestigio o en el acoso sistemático a una persona o grupo de personas. Para fines prácticos, se considerará que un acto es prolongado en el tiempo si ocurre o ha ocurrido tres o más veces.

Dimensión	Categorías	Definición
Finalidad: Objetivo del acto de ciberviolencia	Utilitaria	Los actos utilitarios son aquellos que ocurren con el fin de obtener algo (ej., información, dinero, favores sexuales) o impedir que una persona o grupo de personas hagan algo (ej., impedir la participación política o cívica), como en una extorsión o mensaje intimidatorio para impedir el ejercicio del voto vía Whatsapp.
	Dirigida	Los actos dirigidos son aquellos que ocurren con el fin de hacerle daño a la persona sin un beneficio personal relacionado, como en un insulto o en el bullying.
Grado de intrusión: Nivel en que se invade la esfera privada de la víctima	No intrusiva	Los actos no intrusivos son aquellos que no invaden la esfera privada de la persona sin su consentimiento y se mantienen en el espacio público, a la vista de todos, como en los comentarios ofensivos en redes sociales.
	Intrusiva	Los actos intrusivos son aquellos que invaden la esfera privada de la persona sin su consentimiento, accediendo y/o publicando información privada que puede ser desde una dirección de correo electrónico o número telefónico, hasta imágenes íntimas e información personal o familiar.

Estas dimensiones permiten desarrollar una tipología de ciberviolencias con la que se puede comprender mejor el fenómeno y diseñar estrategias para abordarla y/o mitigarla. Al combinarlas se crean ocho tipos de ciberviolencia, como se explica en la Tabla 2.

Tabla 2. **Ciberviolencia multidimensional**

	Efímeras	
	No intrusiva	**Intrusiva**
Dirigida	**Efímera dirigida no intrusiva** (ej., insulto o comentario ofensivo en una red pública).	**Efímera dirigida intrusiva** (ej., insulto o comentario ofensivo por medio de mensaje privado en una red social, publicación de fotos íntimas sin el consentimiento de la persona).
Utilitaria	**Efímera utilitaria no intrusiva** (ej., intento de estafa en una red social pública).	**Efímera utilitaria intrusiva** (ej., envío de correo electrónico para obtener información de cuentas bancarias.)

	Prolongadas	
	No intrusiva	**Intrusiva**
Dirigida	**Prolongada dirigida no intrusiva** (ej., acoso o bullying público sostenido en una red social).	**Prolongada dirigida intrusiva** (ej., campaña de intimidación o amenazas por medios privados, robo de identidad).
Utilitaria	**Prolongada utilitaria no intrusiva** (ej., repetidos intentos de estafa en una red social pública).	**Prolongada utilitaria intrusiva** (ej., envío de varios correos electrónicos para obtener información de cuentas bancarias).

Se diseñó un cuestionario digital que está construido sobre la base del Quantitative Discourse Analysis (QDA), una técnica de investigación cualitativa que se utiliza para transformar textos en variables y cifras numéricas. La técnica descompone los textos en "tríadas semánticas" que responden a las preguntas clásicas de quién le hizo qué a quién. A estas les agregamos las preguntas de contexto: por qué medio, cuándo y dónde.

Tabla 3. Tipos de acciones de ciberviolencia y plataformas digitales involucradas

Variables	Categorías
Acciones	• 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 • Otro
Redes sociales monitoreadas	• Facebook • X • Instagram • WhatsApp • TikTok • Zoom • YouTube • Telegram • Roblox • Otro • Se desconoce

A partir de estas variables es posible describir los casos de ciberviolencia, identificar quién sufre este tipo de violencia y quién la ejerce. Es importante señalar que un mismo caso de ciberviolencia puede involucrar distintos tipos de acciones violentas, múltiples plataformas digitales y diferentes tipos de perfiles.

2. Fuentes de datos o información

El equipo de observadores registrará casos ilustrativos de ciberviolencia por medio de fuentes directas e indirectas provenientes de distintos departamentos de Guatemala.

Tabla 4. **Tipos de fuentes directas e indirectas**

Fuentes directas	Fuentes indirectas
Observadas directamente en las publicaciones de redes sociales en grupos públicos, páginas o influencers.	• Publicaciones de medios de comunicación o en notas de prensa. • Observado por terceros que informen a la red de observadores. • Casos registrados en el buzón de la página web de Ciberadar.

Equipo de observadores
Está conformada por un grupo de jóvenes que tiene a su cargo monitorear una lista de redes sociales, "influencers", grupos y medios de comunicación de diferentes departamentos a los que deberá dar seguimiento periódicamente.

Buzón de registro de casos
Es un formulario incrustado en la plataforma digital de Ciberadar, con el fin de que cualquier persona pueda acceder a él y brindar información sobre algún caso de ciberviolencia que haya presenciado o del que se haya enterado por otras personas, con el fin de orientar la identificación de casos de ciberviolencia.

3. Fórmulas o procesamiento de la información

A continuación, se detallan las fórmulas utilizadas para describir cada indicador en la herramienta de visualización en la plataforma de Ciberadar.

Tabla 5. **Descripción de indicadores y fórmulas**

Indicador	Descripción	Fórmula del cálculo
Casos de Ciberviolencia	Distribución y clasificación de casos de ciberviolencia registrados según el año, el medio, el perfil y el tipo de acción.	Número de casos registrados según el año, el medio, el perfil y el tipo de acción.

Indicador	Descripción	Fórmula del cálculo
Quién sufre ciberviolencia / Quién ejerce ciberviolencia	Clasificación de los casos registrados según la cantidad de actores afectados y el perfil del actor.	Número de casos registrados por tipo de actor (individuo, grupo de individuos o entidad/organización) según su perfil específico.
	Distribución porcentual de los casos registrados según el género de la persona afectada.	(Número de casos según género / Total de casos registrados) * 100
	Identificación del departamento desde donde se reportó o registró el caso de ciberviolencia.	Número de casos registrados por departamento.
Ciberviolencia multidimensional	Clasificación de los casos según la duración y finalidad.	Número de casos registrados según la duración y finalidad.
	Clasificación de los casos según el grado de intrusión.	(Número de casos según grado de intrusión / Total de casos registrados) * 100
	Clasificación de los ocho tipos de ciberviolencia.	Número de casos registrados según los ocho tipos de la violencia multidimensional.

4. Limitaciones o notas adicionales

Es importante señalar que el registro de casos en la plataforma Ciberadar o en el buzón de reportes no constituye una denuncia penal, ya que los procesos judiciales únicamente pueden iniciarse a través de las instituciones competentes del Estado, como el Ministerio Público o la Policía Nacional Civil (PNC). El observatorio no tiene como finalidad emprender acciones legales en relación con los casos registrados, sino contribuir a la visibilización del fenómeno y a la generación de evidencia para su análisis y comprensión.

Asimismo, el monitoreo presenta algunas limitaciones metodológicas que deben considerarse al interpretar los resultados:

Tabla 6. **Descripción de limitaciones metodológicas**

Tipo de limitación	Descripción
Representatividad numérica	El monitoreo no tiene como objetivo construir una muestra estadísticamente representativa de la ciberviolencia en Guatemala, sino recopilar casos ilustrativos que permitan comprender mejor las dinámicas y patrones del fenómeno. Por lo tanto, los resultados no pueden generalizarse a toda la población, sino que deben leerse como tendencias y patrones cualitativos.
Representatividad geográfica	Si bien cada observador tiene asignados distintos departamentos del país, el registro de casos depende del monitoreo digital realizado por cada integrante del equipo de observadores, quienes dan seguimiento a determinadas cuentas, perfiles, grupos, páginas e influencers. En consecuencia, la cobertura territorial puede variar y los resultados no reflejan la totalidad de manifestaciones de ciberviolencia en todas las regiones del país.
Limitaciones de cobertura del monitoreo	Los casos documentados dependen de las redes sociales, páginas, influencers y grupos que forman parte del monitoreo. Esto implica que el registro puede no capturar todas las manifestaciones de ciberviolencia presentes en las plataformas digitales, sino únicamente aquellas que ocurren en los espacios observados públicos.
Limitación temporal del monitoreo	La identificación de casos está condicionada por los horarios en los que las y los observadores realizan el monitoreo. Como resultado, algunos incidentes que ocurren fuera de esos períodos pueden no ser registrados.

Tipo de limitación	Descripción
Limitaciones de acceso y seguridad digital	El proceso de observación incorpora criterios de seguridad para proteger al equipo de observadores. En consecuencia, no se accede a ciertos espacios digitales privados o potencialmente riesgosos, lo cual limita la posibilidad de observar algunas manifestaciones de ciberviolencia que podrían ocurrir en dichos entornos.

DIÁLOGOS

ciberadar

Juventudes por espacios digitales seguros