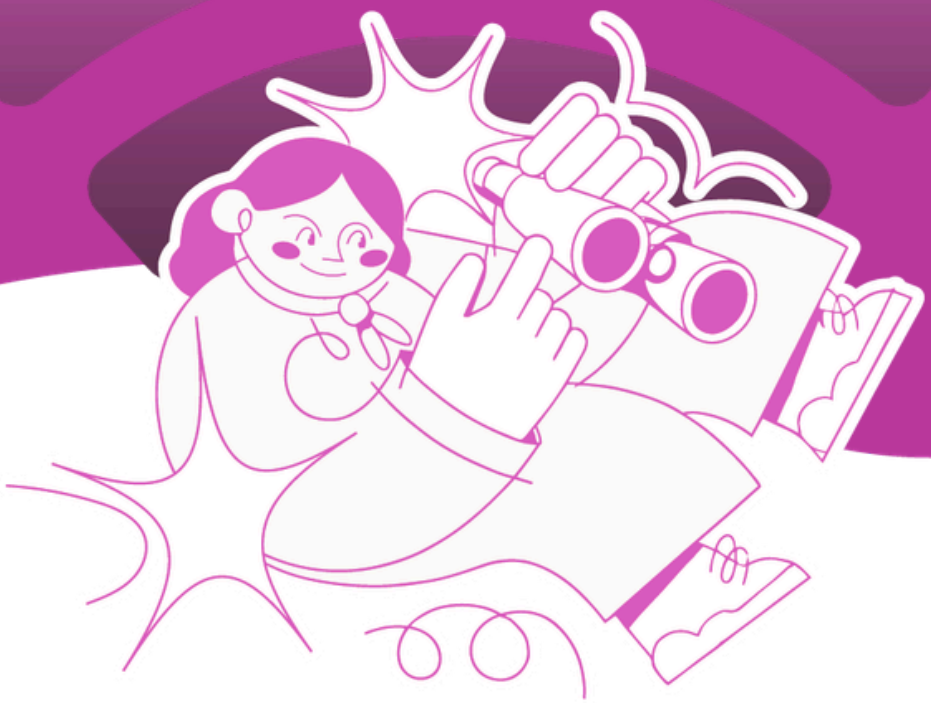
DIÁLOGOS



CUARTO INFORME

1 al 31 de mayo de 2026

Elaborado por Equipo Ciberadar

ciberadar

Juventudes por espacios digitales seguros

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

Créditos

ciberadar
Juventudes por espacios digitales seguros

Autor

Equipo de Ciberadar

Equipo de Diálogos

Walter Corzo, Director Ejecutivo

Daniel Núñez, Director Académico

Gabriela Ayerdi, Coordinadora de Gestión

Karla López, Coordinadora de Investigación

Mayarí Prado, Coordinadora de Comunicación

Diseño: **Pedro Pablo Sánchez**

Edición: **Consejo Editorial Diálogos**

Dirección: 0 calle 16-26 zona 15 colonia El Maestro
Ciudad de Guatemala
Tel: 2369-6418
Correo: info@dialogos.org.gt
www.dialogos.org.gt
@DialogosGuate

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

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

Una iniciativa de:

CIBER CIUDADANOS

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

Resumen ejecutivo

Equipo Ciberadar[1]

Este cuarto informe del Ciberadar presenta los hallazgos del monitoreo de ciberviolencia realizado entre el 1 y el 31 de mayo de 2026 por un equipo de seis observadores distribuidos en distintos departamentos del país y plataformas digitales. Durante este período se documentaron 102 casos de acciones violentas en el espacio virtual, incluyendo ataques verbales y discursos de odio, engaño, fraude y manipulación, vigilancia y acceso no autorizado, difusión no consentida de contenido, amenazas y hostigamiento sexual digital.

Los resultados muestran que los ataques verbales y discursos de odio continúan siendo una de las principales manifestaciones de ciberviolencia registradas. Sin embargo, el informe también evidencia una creciente diversificación de las formas de agresión observadas. Junto a los ataques dirigidos a dañar la reputación, imagen o dignidad de las personas, se identificó una cantidad importante de casos orientados a obtener dinero, información o acceso a sistemas y cuentas digitales. En particular, el engaño, fraude y manipulación, así como la vigilancia, control y acceso no autorizado, representan una proporción significativa de los casos documentados.

Al igual que en los informes anteriores, la mayoría de las víctimas fueron personas individuales, mientras que los victimarios fueron con mayor frecuencia grupos de individuos o actores cuya identidad no pudo determinarse. Estos hallazgos refuerzan la naturaleza predominantemente colectiva de una parte importante de la ciberviolencia observada y el papel que desempeña el anonimato en la amplificación de este tipo de conductas.

El análisis también muestra que la ciberviolencia reproduce desigualdades y patrones sociales preexistentes. Los perfiles femeninos fueron atacados con mayor frecuencia mediante agresiones relacionadas con el sexo o género, la apariencia física y la actividad profesional, mientras que los perfiles masculinos fueron relativamente más afectados por ataques vinculados con la actividad profesional, la capacidad intelectual, el origen étnico y la orientación sexual. Estos patrones sugieren que las plataformas digitales continúan funcionando como espacios donde se reproducen y amplifican formas de discriminación y exclusión ya presentes en otros ámbitos de la vida social.

El equipo de observación corroboró además la creciente utilización de nuevas tecnologías en la comisión de actos de ciberviolencia. Se documentaron casos de uso de inteligencia artificial para generar contenido engañoso o

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

difamatorio, esquemas de suplantación de identidad y diversas modalidades de fraude digital. Asimismo, se registraron ataques informáticos dirigidos contra instituciones públicas y privadas que comprometieron información sensible de miles de personas, poniendo de manifiesto que la ciberviolencia no afecta únicamente a individuos, sino también a organizaciones y sistemas de interés público.

Finalmente, los hallazgos muestran que predominan los casos efímeros, dirigidos a hacer daño y desarrollados en espacios públicos. No obstante, también se observó una cantidad relevante de casos intrusivos orientados a obtener beneficios materiales o información mediante la invasión de la esfera privada de las víctimas, lo que sugiere una creciente complejidad del fenómeno y la coexistencia de distintas modalidades de ciberviolencia.

Los resultados presentados en este informe deben interpretarse con cautela. Los casos documentados dependen de las redes sociales, páginas, grupos, influencers y medios digitales monitoreados por el equipo de observación, así como de los horarios y capacidades de observación disponibles. Además, por razones de seguridad, el monitoreo no incluye espacios privados o potencialmente riesgosos para las personas observadoras. En consecuencia, los hallazgos no constituyen una muestra representativa de toda la ciberviolencia que ocurre en Guatemala, sino una aproximación exploratoria orientada a identificar patrones, tendencias y manifestaciones relevantes del fenómeno.

Metodología

Este informe se basa en el monitoreo realizado por el equipo de observación de Ciberadar del 1 al 31 de mayo de 2026. La observación fue llevada a cabo por seis jóvenes, distribuidos en distintos horarios, departamentos y redes sociales, como se detalla en la Tabla 1. Además, cada integrante del equipo de Ciberadar fue responsable de monitorear una lista específica de influencers, páginas y grupos dentro de las plataformas asignadas, y medios de comunicación digitales. Esta distribución fue consensuada entre el equipo de Diálogos y el equipo de observación, tomando en cuenta su disponibilidad y conocimiento de las dinámicas departamentales y de las distintas plataformas digitales.

Tabla 1. Distribución de observadores por departamentos y redes sociales

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

En términos analíticos, durante esta cuarta etapa, el equipo de observación se enfocó en documentar distintos casos de ciberviolencia y de conscientemente buscar información sobre casos no incluidos en el informe de la prueba piloto y en el segundo y tercer informes, con el objetivo de visibilizar la diversidad de manifestaciones que ocurren en diferentes plataformas digitales. En particular, el equipo de observación buscó casos que hayan invadido la esfera privada de las personas con el fin de obtener algo de ellas o impedir que realizaran alguna actividad; casos que hayan tenido alguna repercusión grave sobre la víctima o víctimas; y casos que hagan uso de tecnología nueva o inteligencia artificial,

que fue uno de los patrones identificados anteriormente. Cada integrante tuvo a su cargo un máximo de diez casos por semana, y se les indicó priorizar la diversidad de situaciones observadas por encima de su cuantificación. Asimismo, es importante notar que la observación incluyó casos que no necesariamente ocurrieron durante el periodo de monitoreo, sino que se remontan a años anteriores, con el fin de comprender el fenómeno en toda su complejidad y la diversidad de casos existentes.

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

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

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

Hallazgos

Análisis cuantitativo

En total, el equipo de Ciberadar reportó 102 casos de acciones violentas en el espacio virtual entre el 1 y 31 de mayo, como se muestra en la Tabla 2. La mayoría de los casos (n=42, 41%) corresponde a ataques verbales y discursos de odio, pero una cantidad significativa (n=15, 15%) involucró este tipo de acción en combinación con otras formas de agresión. El 44% (n=45) restante son otras acciones violentas que describiremos más adelante.

Tabla 2. Tipos de acciones violentas en el espacio virtual reportados por el equipo de Ciberadar, 1 al 31 de mayo de 2026

Tipo de acciones violentas en el espacio virtual	Frecuencia	Porcentaje del total
Ataques verbales y discursos de odio	42	41%
Ataques verbales y discursos de odio + otras formas de ciberviolencia	15	15%
Otras acciones violentas	45	44%
Total	**102**	**100%**

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

La Tabla 3 muestra los tipos de ataques verbales y discursos de odio mencionados en los 42 casos registrados de forma aislada. Dado que un solo caso puede involucrar más de un tipo de ataque, las frecuencias suman más de 42. Como se puede ver, el tipo más frecuente fue el ataque verbal o insulto basado en la capacidad intelectual (n=16, 20%), seguido por los ataques basados en la apariencia física (n=14, 17%), sexo/género (n=12, 15%) y actividad profesional (n=11, 13%). Juntos, estos cuatro tipos de ataques verbales y discursos de odio representan el 65% de todas las menciones.

Tabla 3. Tipos de ataques verbales y discursos de odio en los 42 casos aislados reportados por el equipo de Ciberadar, 1 al 31 de mayo de 2026

Tipo de ataque verbal o discurso de odio	Frecuencia	Porcentaje
Basado en la capacidad intelectual	16	20%
Basado en la apariencia física	14	17%
Basado en el sexo/género	12	15%
Basado en la actividad profesional	11	13%
Basado en el origen étnico	9	11%
Basado en la posición socioeconómica	5	6%
Basado en la orientación sexual	4	5%
Difamación	4	5%
Basado en la ideología política	4	5%
Basado en la nacionalidad/país de origen	3	4%
Total	**82**	**100%**

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

La Tabla 4 muestra los tipos de ataques verbales y discursos de odio mencionados en los 15 casos registrados en combinación con otras formas de agresión. Al igual que en la tabla anterior, un solo caso puede involucrar más de un tipo de acción violenta, por lo que las frecuencias suman más de 15. Como se puede observar, los ataques verbales y discursos de odio estuvieron acompañados por la difusión no consentida de contenido en 8 ocasiones (44% del total), seguido por las amenazas (n=3, 17%) y la vigilancia, control y acceso no autorizado (n=3, 17%).

Tabla 4. Ataques verbales y discursos de odio + tipos de acciones violentas en el espacio virtual en los 15 casos combinados reportados por el equipo de Ciberadar, 1 al 31 de mayo de 2026

Tipo de acciones violentas en el espacio virtual	Frecuencia	Porcentaje del total
Difusión no consentida de contenido	8	44%
Amenazas	3	17%
Vigilancia, control y acceso no autorizado	3	17%
Engaño, fraude y manipulación	2	11%
Hostigamiento sexual digital	2	11%
Total	**18**	**100%**

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

La Tabla 5 muestra las otras acciones violentas reportadas por el equipo de observación. El engaño, fraude y manipulación y la vigilancia, control y acceso no autorizado suman más de la mitad de las menciones (n=41, 66% en conjunto). La difusión no consentida de contenido también fue reportada con frecuencia (n=12, 19%).

Tabla 5. Otras acciones violentas reportadas por el equipo de Ciberadar, 1 al 31 de mayo de 2026

Tipo de acciones violentas en el espacio virtual	Frecuencia	Porcentaje del total
Engaño, fraude y manipulación	25	40%
Vigilancia, control y acceso no autorizado	16	26%
Difusión no consentida de contenido	12	19%
Amenazas	6	10%
Hostigamiento sexual digital	3	5%
Total	**62**	**100%**

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

En cuanto a los patrones entre víctimas y victimarios, destaca que la mayoría de las víctimas (n=52, 51%) fueron personas individuales, mientras que la mayoría de los victimarios (n=45, 44%) fueron grupos de individuos (ver Tabla 6). Esto refuerza el hallazgo de la fase piloto y del segundo y tercer informes de que una parte significativa de la ciberviolencia documentada adopta la forma de violencia colectiva. Al igual que en los informes anteriores, en este caso también se documentaron varios casos (n=34, 33%) en los que se desconoce quién o quiénes fueron los victimarios. Como hemos señalado en repetidas ocasiones, la violencia colectiva en las redes sociales es significativamente facilitada por el anonimato.

Tabla 6. Víctimas y victimarios de ciberviolencia reportados por el equipo de Ciberadar, 1 al 31 de mayo de 2026.

Víctima	Cantidad	Porcentaje del total	Victimarios	Cantidad	Porcentaje del total
Individuo	52	51%	Grupo de individuos	45	44%
Grupo de individuos	37	36%	Individuo	23	23%
Entidad u organización	11	11%	Se desconoce	34	33%
Se desconoce	2	2%	Entidad u organización	0	0%
Total	**102**	**100%**	**Total**	**102**	**100%**

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

La Tabla 7 muestra que los patrones más comunes registrados hasta el momento son los de ciberviolencia ejercida por un grupo de individuos en contra de una persona individual o grupo de individuos (n=22 en ambos casos). También se registraron 16 casos en los que el victimario fue una persona individual en contra de un individuo y 14 en los que se desconoce el victimario y la víctima fue una persona individual.

Tabla 7. Casos según tipo de víctima y victimario registrados por el equipo de Ciberadar, 1 al 31 de mayo de 2026

Víctima / Victimario				
	Grupo de individuos	Individuo	Se desconoce	Total general
Individuo	22	16	14	**52**
Grupo de individuos	22	6	9	**37**
Entidad u organización	1	1	9	**11**
Se desconoce	0	0	2	**2**
Total general	45	23	34	**102**

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

Respecto al género de las víctimas y los victimarios, la Tabla 8 muestra que en 33 de los 102 casos (32%), las víctimas fueron perfiles femeninos, mientras que en 28 de los 102 casos (27%), fueron perfiles masculinos. En 21% de los casos (n=21) se desconoce el género de la víctima. En cuanto a los victimarios, en la mayoría de los casos (n=48, 47%) no fue posible determinar el género, mientras que en 27 casos (26%) se identificó que se trataba de personas masculinas. En 21 casos (21%) los victimarios involucraron a perfiles tanto masculinos como femeninos.

Tabla 8. Género de las víctimas y victimarios en los casos registrados por el equipo de Ciberadar, 1 al 31 de mayo de 2026

Género de la víctima	Frecuencia	Porcentaje del total	Género del victimario	Frecuencia	Porcentaje del total
Femenino	33	32%	Se desconoce	48	47%
Masculino	28	27%	Masculino	27	26%
Se desconoce	21	21%	Masculino, Femenino	21	21%
Masculino, Femenino	20	20%	Femenino	6	6%
Total	**102**	**100%**	**Total**	**102**	**100%**

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

En el tercer informe, un patrón emergente en los casos analizados sugirió que la ciberviolencia adopta formas diferenciadas según el género de las personas afectadas. En esta ocasión, como se muestra en la Tabla 9, los ataques verbales y/o discursos de odio muestran el mismo patrón. En el caso de los perfiles femeninos, predominan claramente los ataques vinculados al sexo/género (n=13, 25%), la actividad profesional (n=8, 15%), la apariencia física (n=7, 14%) y la capacidad intelectual (n=6, 12%), que juntos suman más del 65%. Esto evidencia una tendencia relativa a deslegitimar más a estos perfiles a partir de atributos asociados con el género y la apariencia.

Por el contrario, en los perfiles masculinos, destacan relativamente más los ataques relacionados con la actividad profesional (n=5, 13%), la capacidad intelectual (n=5, 13%), la apariencia física (n=4, 10%) y el origen étnico (n=4, 10%), orientados relativamente más a cuestionar aspectos de capacidad, origen e identidad social. Como señalamos en el tercer informe, estos hallazgos sugieren que la ciberviolencia reproduce patrones de desigualdad y normas de género preexistentes en la sociedad guatemalteca, utilizando distintos repertorios de agresión dependiendo del género de la víctima. Sin embargo, en esta ocasión, es necesario notar que los ataques basados en la actividad profesional, apariencia física y capacidad intelectual fueron mencionados para ambos géneros.

La Tabla 9 resume estos hallazgos. Las frecuencias y los porcentajes corresponden a menciones y solo a los casos en los que las víctimas fueron individuos, por lo que el total no suma 102.

Tabla 9. Tipo de ataque por género de la víctima en los casos registrados por el equipo de Ciberadar, 1 al 31 de mayo de 2026

Tipo de ataque verbal o discurso de odio	Femenino n (%)	Masculino n (%)
Basado en sexo/género	13 (25%)	1 (3%)
Basado en actividad profesional	8 (15%)	5 (13%)
Basado en apariencia física	7 (14%)	4 (10%)
Basado en la capacidad intelectual	6 (12%)	5 (13%)
Difamación	4 (8%)	3 (8%)
Basado en la ideología política	2 (4%)	2 (5%)
Basado en el origen étnico	0 (0.0%)	4 (10%)
Basado en la orientación sexual	0 (0.0%)	3 (8%)
Basado en la nacionalidad/país de origen	1 (2%)	1 (3%)
Basado en la posición socioeconómica	1 (2%)	1 (3%)
Basado en relaciones interpersonales	1 (2%)	0 (0.0%)
No aplica	9 (17%)	11 (28%)
Total	**52 (100%)**	**40 (100%)**

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

En cuanto a las edades de las víctimas de los casos de ciberviolencia registrados, la Tabla 10 muestra que más de una cuarta parte (n=21, 21% en conjunto) ocurrió en contra de jóvenes entre los 15 y 29 años, mientras que en 9 casos (9%) las víctimas tenían 50 años o más. En más de la mitad de los casos (n=62, 61%) se desconoce la edad de la víctima.

Tabla 10. **Rangos de edad de las víctimas de los casos de ciberviolencia registrados por el equipo de Ciberadar, 1 al 31 de mayo de 2026**

Rango de edad	Frecuencia	Porcentaje del total
10 a 14 años	2	2%
15 a 19 años	6	6%
20 a 24 años	9	9%
25 a 29 años	6	6%
30 a 34 años	2	2%
35 a 39 años	2	2%
40 a 44 años	1	1%
45 a 49 años	3	3%
50 o más años	9	9%
Se desconoce	62	61%
Total	**102**	**100%**

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

En relación con los medios utilizados, la mayoría de los casos documentados por el equipo de Ciberadar ocurrieron en Facebook (n=49, 58%), seguido por Whatsapp (n=17, 20%), Otro (n=12, 14%) e Instagram (n=6, 7%). La Tabla 11 resume las menciones de los medios.

Tabla 11. Medios utilizados en los casos de ciberviolencia registrados por el equipo de Ciberadar, 1 al 31 de mayo de 2026

Medio	Frecuencia	Porcentaje
Facebook	49	56%
Whatsapp	17	19%
Otro	12	14%
Instagram	6	7%
Tik Tok	2	2%
Telegram	1	1%
X	1	1%
Total	**88**	**100%**

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

Análisis cualitativo

En su tercer informe, el equipo de Ciberadar confirmó los patrones identificados en análisis previos: la naturaleza predominantemente colectiva de la ciberviolencia, su facilitación por el anonimato que ofrecen las plataformas digitales y su capacidad para amplificar tanto las dinámicas del contexto político nacional como las estructuras históricas de desigualdad presentes en la sociedad guatemalteca. Asimismo, identificó algunas formas de ciberviolencia que hacen uso de tecnología nueva para irrumpir en la vida privada de las personas, en particular, inteligencia artificial o el uso de sistemas de mensajería directa utilizada para engañar a usuarios, entrometerse en su vida privada y/o obtener algo de ellos.

En esta ocasión, el equipo de observación corroboró todos estos patrones y documentó varios casos de uso de tecnología con los fines señalados arriba. Algunos ejemplos:

> *El 15 de abril de 2026, la página de Facebook Noticias de Impacto Guatemala difundió al público una noticia aparentemente falsa sobre la supuesta captura de una extorsionista llamada "la reina", mediante una publicación acompañada de una imagen generada con inteligencia artificial en la que se muestra a una mujer con el rostro difuminado; esta información no fue encontrada en medios oficiales, lo que indica que se trató de desinformación utilizada para atraer interacciones principalmente del público masculino a través de contenido visual sugestivo, con el fin de aumentar vistas y comentarios dentro de la plataforma.*

Desde el 1 de abril de 2026, en Facebook, la página Quetzal Shute ha publicado de forma continua una serie de imágenes generadas con inteligencia artificial en las que representa a funcionarios y figuras políticas de Guatemala como animales, acompañados de nombres "científicos" y descripciones satíricas sobre su comportamiento. Las publicaciones utilizan ilustraciones y textos para asociar características de los animales con rasgos atribuidos a las personas representadas, con un enfoque de burla y crítica.

La banda "Los Lauren Paleck" cometió un caso de ciberviolencia mediante la suplantación de identidad en la plataforma Messenger, donde los integrantes fingían ser familiares cercanos de las víctimas para solicitar transferencias de dinero de manera urgente. El caso salió a la luz el 7 de enero de 2026, luego de que una persona transfiriera más de medio millón de quetzales creyendo que ayudaba a un pariente. Las autoridades realizaron operativos simultáneos en Retalhuleu, Zacapa y la ciudad capital, logrando la captura de seis integrantes de la estructura criminal, según reportó el medio La Hora.

Además de estos casos, en esta ocasión, el equipo de Ciberadar documentó también varios casos de acceso no autorizado, vulneración de sistemas y ataques informáticos dirigidos tanto a instituciones públicas como privadas. Estos incidentes evidencian que la ciberviolencia puede trascender las agresiones entre individuos en redes sociales y llegar a afectar el funcionamiento de organizaciones que prestan servicios esenciales o administran información sensible.

Las implicaciones de estos ataques son significativas: pueden comprometer datos personales, afectar la continuidad de servicios, generar pérdidas económicas y erosionar la confianza ciudadana en las instituciones. Asimismo, ponen de relieve la creciente importancia de fortalecer las capacidades de ciberseguridad del país, desarrollar protocolos de respuesta ante incidentes y promover una cultura de protección digital que reduzca la vulnerabilidad de organizaciones y personas frente a amenazas cada vez más sofisticadas.

Algunos ejemplos de los casos recopilados:

El 7 de abril de 2026, el hacker identificado como "Gordon Freeman" realizó un ciberataque contra la Dirección General de Control de Armas y Municiones (Digecam) en Guatemala mediante la saturación e intrusión de su sistema web, vulnerando y extrayendo información de aproximadamente 18 mil usuarios, incluyendo registros de armas de personas individuales, empresas y entidades públicas; el ataque inició alrededor de las 3:00 horas y duró cerca de 13 horas, mientras las autoridades señalaron que la información obtenida era pública y no sensible, aunque expertos advirtieron que la correlación de datos como nombres, identificadores y licencias de armas podría representar un riesgo para la seguridad y privacidad de los afectados.

El 27 de abril de 2026, el hacker identificado como "Gordon Freeman" realizó un ciberataque contra el portal Tu Empleo del Ministerio de Trabajo y Previsión Social (Mintrab) en Guatemala mediante el acceso no autorizado a una API antigua y vulnerable, lo que permitió la extracción de más de 200 mil registros y alrededor de 40 GB de información confidencial, incluidos currículums, números de DPI, contactos, direcciones, historiales académicos, laborales y salariales de los usuarios; el ataque fue facilitado por fallas de seguridad en los servidores, como el uso de protocolos obsoletos TLS 1.0 y TLS 1.1 y la ausencia de medidas básicas de protección digital, tras lo cual el atacante habría exigido el pago de bitcoin a cambio de no vender la información sustraída.

El 27 de abril de 2026, el hacker identificado como "MrGoblinciano" realizó ataques cibernéticos contra la Universidad de San Carlos de Guatemala (Usac) y la Universidad Rafael Landívar (URL) en Guatemala mediante la vulneración de sus sistemas informáticos, lo que provocó la exposición y filtración de información financiera, nóminas, números de CUI y datos bancarios vinculados al Sistema Integrado de Información Financiera (SIIF) de la Usac, así como la filtración de 84 mil 620 fotografías y datos personales de estudiantes y docentes de la URL; aunque ambas universidades confirmaron los incidentes y activaron protocolos de seguridad, indicaron que no existía evidencia de alteración masiva o sistemática de datos sensibles.

En Guatemala, el hacker identificado como "NemorisHacking", presuntamente vinculado al grupo "JXLLTEAM" y al alias "KeyBreaker", realizó ataques cibernéticos contra los portales de la Procuraduría General de la Nación (PGN) y la Superintendencia de Telecomunicaciones (SIT) mediante la vulneración y exposición de credenciales de acceso administrativo, ataques de fuerza bruta, posible uso de programas de robo de información y desfiguración de sitios web, operando a través de canales de Telegram y foros externos; el objetivo habría sido comprometer nombres de usuario y contraseñas de sistemas estatales

El 1 de mayo de 2026, el hacker identificado como "MrGoblinciano" realizó un presunto ciberataque contra el Tribunal Supremo Electoral (TSE) en Guatemala mediante la vulneración del portal de firma electrónica firmaelectronica.tse.org.gt, lo que habría permitido la filtración y distribución gratuita de 2 mil 136 imágenes JPG de firmas electrónicas de empleados autorizados para validar documentos oficiales; ante el riesgo de falsificación documental y vulneración del padrón electoral y otros datos sensibles, el TSE suspendió temporalmente su sitio web www.tse.org.gt, activó un Plan de Respuesta y Contención ante Amenazas de Seguridad Informática y comenzó investigaciones técnicas para prevenir accesos no autorizados y reforzar la seguridad institucional.

El equipo de Ciberadar también documentó las acciones que tomaron las víctimas para lidiar con la ciberviolencia. En general, como se puede observar en la Tabla 12, al igual que en el informe anterior, en la mayoría de los casos no se sabe qué hicieron las víctimas (n=53, 51%) o no tomaron ninguna acción (n=19, 18%). Sin embargo, en una proporción importante las víctimas publicaron una aclaración en su cuenta personal o institucional (n=17, 16%) o respondieron públicamente a la persona sin agredirla (n=7, 7%). Como se ha mencionado antes, esta tabla resume las menciones, y dado que un solo caso puede involucrar más de una acción, las frecuencias suman más de 102.

Tabla 12. Acciones que tomaron las víctimas para lidiar con la ciberviolencia en los casos registrados por el equipo de Ciberadar, 1 al 31 de mayo de 2026

Acción	Frecuencia	Porcentaje
Se desconoce	53	50%
Ninguna	19	18%
Publicó una aclaración en su cuenta personal o institucional	17	16%
Respondió públicamente a la persona sin agredirla	7	7%
Tomó acciones legales contra la persona	4	4%
Bloqueó o reportó la cuenta	2	2%
Eliminó la publicación	1	1%
Se retiró del grupo de WhatsApp y bloqueó los números	1	1%
Envió un video con la conversación a la página Boletín Monjas	1	1%
Cerró la cuenta	1	1%
Agredió a la persona en línea o en persona	1	1%
Total	**107**	**100%**

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

En cuanto a las consecuencias que tuvieron los actos de ciberviolencia, la Tabla 13 muestra que en más de la mitad de los casos (n=64, 62%) se desconoce qué ocurrió, pero en un porcentaje significativo (n=29, 28%) las personas experimentaron daño reputacional, material o emocional. La tabla resume las menciones, por lo que las frecuencias suman más de 102.

Tabla 13. **Consecuencias que tuvieron en las víctimas los casos de ciberviolencia registrados por el equipo de Ciberadar, 1 al 31 de mayo de 2026**

Tipo de consecuencia	Frecuencia	Porcentaje
Se desconoce	64	62%
Daño reputacional (afectación de imagen pública)	29	28%
Daño material (pérdidas económicas)	6	6%
Daño emocional (tristeza, angustia, miedo)	4	4%
Total	**103**	**100%**

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

La Tabla 14 muestra las distintas categorías de ciberviolencia que surgen después de combinar las tres dimensiones de cada hecho: duración (efímeras o prolongadas), grado de intrusión (intrusiva y no intrusiva) y finalidad (hacer daño o tratar de obtener algo/impedir que la persona haga algo). Como se puede observar, y al igual que en los informes anteriores, la mayoría de los casos ocurrieron de manera efímera, buscaron hacerle daño a la persona o grupo de personas, y se mantuvieron en el espacio público.

Tabla 14. **Duración, finalidad y grado de intrusión de los casos registrados por el equipo de Ciberadar, 1 al 31 de mayo de 2026**

Duración	Cantidad de casos	Finalidad	Cantidad de casos	Grado de intrusión	Cantidad de casos
Efímera (1 o 2 veces)	72	Hacerle daño a la persona	60	No intrusiva (se mantuvo en el espacio público)	65
Prolongada (3 o más veces)	27	Obtener algo de la persona o impedir que la persona haga algo	33	Intrusiva (invadió la esfera privada de la persona	28
Se desconoce	3	Se desconoce	9	Se desconoce	9
Total	**102**	**Total**	**102**	**Total**	**102**

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

La Tabla 15 resume las frecuencias para las distintas categorías que surgen después de combinar las tres dimensiones de los casos en los que se lograron documentar todas ellas. Al igual que en el informe anterior, el tipo predominante es el dirigido no intrusivo tanto para los casos efímeros como para los prolongados. En otras palabras, la mayoría de los casos registrados han sido ataques que buscaron hacerle daño directamente a una persona o grupo de personas en el espacio público. Sin embargo, en esta ocasión, el equipo de Ciberadar también registró una cantidad relevante de casos utilitarios intrusivos efímeros (n=16, 16%), lo cual está ligado a los ataques a las instituciones públicas y privadas mencionados anteriormente.

Tabla 15. Tipos de ciberviolencia registrados por el equipo de Ciberadar según tipología basada en la duración, finalidad y grado de intrusión, 1 al 31 de mayo 2026

Efímeras	Cantidad de casos	Porcentaje del total
Dirigida no intrusiva	35	34%
Dirigida intrusiva	3	3%
Utilitaria no intrusiva	4	4%
Utilitaria intrusiva	16	16%
Prolongadas	**Cantidad de casos**	**Porcentaje del total**
Dirigida no intrusiva	18	18%
Dirigida intrusiva	0	0%
Utilitaria no intrusiva	0	0%
Utilitaria intrusiva	3	3%
Se desconoce	23	23%
Total	**102**	**100%**

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

Como hemos mencionado en otros informes, es relevante destacar que los resultados de este informe deben interpretarse con cautela, ya que están condicionados por un sesgo y limitación de reporte inherentes al proceso de observación. En particular, los casos documentados dependen de las redes sociales, influencers, páginas y grupos que el equipo de observación monitorea, así como de los horarios en que realiza este monitoreo. Asimismo, la observación está sujeta a limitaciones derivadas de consideraciones de seguridad, como la decisión de no ingresar a grupos privados o espacios digitales potencialmente riesgosos para el equipo.

Conclusiones

Los hallazgos de este cuarto informe confirman varios de los patrones identificados en las fases anteriores del Ciberadar. La ciberviolencia observada continúa caracterizándose por una fuerte dimensión colectiva, facilitada por el anonimato y por las dinámicas de interacción propias de las plataformas digitales. Una proporción importante de los casos registrados involucró grupos de individuos actuando contra personas individuales u otros grupos, lo que sugiere que las agresiones digitales suelen trascender los conflictos estrictamente interpersonales para adquirir características de acción colectiva.

Los ataques verbales y discursos de odio siguen ocupando un lugar central dentro de las formas de violencia observadas. Sin embargo, el informe muestra que la ciberviolencia en Guatemala no puede reducirse a este tipo de manifestaciones. El peso que adquieren el engaño, fraude y manipulación, la vigilancia y acceso no autorizado a información, así como la difusión no consentida de contenido, refleja una diversificación creciente de las estrategias utilizadas para dañar, controlar o explotar a las víctimas.

Los casos documentados sugieren además que la ciberviolencia continúa reproduciendo desigualdades y normas sociales preexistentes. Los repertorios de agresión empleados contra perfiles femeninos y masculinos muestran diferencias significativas que reflejan patrones más amplios de discriminación y desigualdad presentes en la sociedad guatemalteca. Al mismo tiempo, varios tipos de ataques aparecen de forma recurrente en ambos grupos, lo que evidencia que ciertas formas de deslegitimación y descrédito afectan transversalmente a distintos perfiles.

Otro hallazgo relevante es la creciente importancia de la dimensión tecnológica del fenómeno. El uso de inteligencia artificial para generar contenido engañoso o satírico, la suplantación de identidad con fines económicos y los ataques informáticos contra instituciones públicas y privadas muestran que la ciberviolencia evoluciona constantemente y adopta nuevas modalidades conforme se transforman las tecnologías disponibles. En este sentido, los casos registrados evidencian que las fronteras entre ciberviolencia, fraude digital, desinformación y ciberseguridad son cada vez más difusas.

La tipología utilizada por el Ciberadar muestra que la forma predominante de ciberviolencia documentada sigue siendo aquella que busca dañar a una persona o grupo de personas en espacios públicos digitales. No obstante, también se identificó una presencia significativa de casos utilitarios intrusivos, orientados a obtener dinero, información u otros beneficios mediante la invasión de la esfera privada de las víctimas. Este hallazgo sugiere que, junto a la agresión simbólica y reputacional, formas de ciberviolencia vinculadas con incentivos materiales y económicos también tienen relevancia.

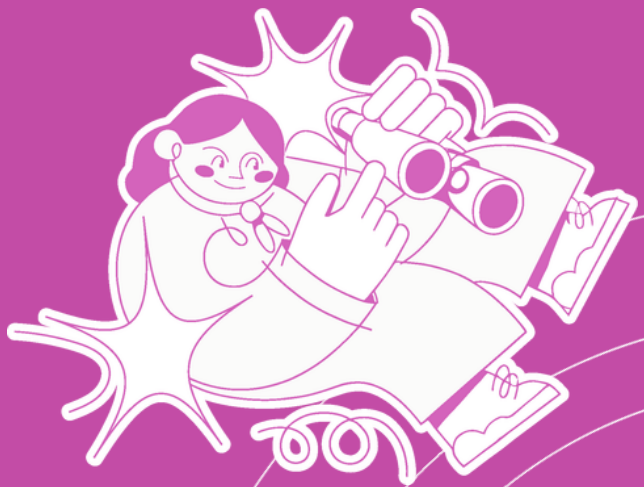
Finalmente, el informe pone de relieve la necesidad de fortalecer las capacidades de prevención, documentación y respuesta frente a la ciberviolencia. La elevada proporción de casos en los que se desconoce qué acciones tomaron las víctimas o cuáles fueron las consecuencias concretas de las agresiones evidencia la necesidad de desarrollar mejores mecanismos de acompañamiento, denuncia y seguimiento, así como estrategias de alfabetización digital y fortalecimiento de la ciberseguridad tanto para personas como para instituciones.

Es importante señalar que estas conclusiones deben interpretarse con cautela. Los casos registrados reflejan únicamente aquellos que fueron identificados por el equipo de observación dentro de las plataformas, grupos, páginas y espacios digitales monitoreados durante el período de estudio. Asimismo, la observación está condicionada por limitaciones operativas y de seguridad que restringen el acceso a determinados espacios digitales. Por ello, los resultados no deben entenderse como una medición exhaustiva o representativa de toda la ciberviolencia que ocurre en Guatemala, sino como evidencia exploratoria que permite identificar tendencias, patrones emergentes y áreas prioritarias para futuras investigaciones.

DIÁLOGOS

ciberadar

Juventudes por espacios digitales seguros



CIBER CIUDADANOS

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