Universidad de San Carlos de Guatemala
Escuela de Trabajo Social
Ciudad Universitaria Z.12
Edificio S 1, Segundo Nivel
Tel.2418-8850 Ext. 107
E-mail: iietsguate1@gmail.com

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Año 2024

Importancia de Trabajo Social para la prevención del Ciberdelito en grupos sociales vulnerables en Guatemala

IIETS"Angela Ayala"

Universidad de San Carlos de Guatemala
Escuela de Trabajo Social
Instituto de Investigaciones "TS Angela Ayala"

IMPORTANCIA DE TRABAJO SOCIAL

PARA LA PREVENCIÓN DEL CIBERDELITO EN GRUPOS SOCIALES VULNERABLES EN GUATEMALA

Daniel Alberto Herrera Letona
Investigador

Universidad de San Carlos de Guatemala
Escuela de Trabajo Social
Instituto de Investigaciones T.S. “Ángela Ayala”

Importancia de Trabajo Social para la Prevención del Ciberdelito en grupos sociales vulnerables en Guatemala

MSc. Daniel Alberto Herrera Letona

Guatemala, noviembre de 2025.

Universidad de San Carlos de Guatemala
Instituto de Investigaciones de la Escuela de Trabajo Social "T. S. Ángela Ayala"
Edificio S-1, 2do. Nivel, Ciudad Universitaria, zona 12. Ciudad de Guatemala.
Tel. PBX- 2418-8850 ext. 107 y 85463
Email: iietsguate1@gmail.com

Tabla de contenido

Introducción

El presente informe de investigación propone una lectura sobre el tema Importancia de Trabajo Social para la Prevención del Ciberdelito en grupos sociales vulnerables en Guatemala. Tomando en cuenta que el Trabajo Social puede formular estrategias de abordaje del tema de la prevención del ciberdelito utilizando sus diferentes metodologías de inmersión en la problemática social de Guatemala.

El objetivo de la investigación es Identificar la importancia del Trabajo Social en la prevención del Ciberdelito en grupos sociales vulnerables utilizando el marco legal e institucional vigente en el ámbito nacional, para el desarrollo de procesos que coadyuven a la prevención del ciberdelito en Guatemala.

El informe integra temas relevantes como: el Ciberespacio, el Ciberdelito, el Trabajo Social y el Ciberdelito en Guatemala, un Análisis Estratégico, entre otros. Con estos temas se pretende comprender de manera general en qué consiste el ciberespacio, cómo se da el ciberdelito, la relación que se puede encontrar entre el Trabajo Social y el Ciberdelito, para finalizar con un análisis de la opinión de actores que trabajan directamente con la atención del ciberdelito en Instituciones como: El Ministerio Público, el Ministerio de Gobernación, la Secretaría contra la Violencia y Explotación Sexual y Trata de Personas –SVET-, la Policía Nacional Civil y un segmento de Trabajadores Sociales.

Se puede referir dentro de los hallazgos más relevantes que el Trabajo Social si puede dar importantes aportes en la prevención del ciberdelito en grupos vulnerables en Guatemala. Esto debido a que sus metodologías, estrategias y modelos de intervención son congruentes para diseñar un Plan Nacional de Prevención del Ciberdelito.

En tal sentido, se invita al lector a realizar las respectivas reflexiones sobre este tema que de manera novedosa surge derivado de los avances de la ciencia, la tecnología y las comunicaciones en un mundo globalizado.

Capítulo I. Planteamiento del problema

El tema del ciberdelito ha cobrado auge a partir que se socializa el uso de internet y las redes sociales. Es en la segunda mitad del siglo XX con la finalización de la segunda guerra mundial y el surgimiento de un mundo bipolar encabezado por las dos potencias hegemónicas mundiales de la época Estados Unidos de América en adelante EUA y la Unión de Repúblicas Socialistas Soviéticas en adelante URSS cuando se inicia un desarrollo acelerado de la ciencia y tecnología.

En efecto a finales de la década de 1950 se inicia una etapa histórica denominada Guerra Fría. Esta época marca la rivalidad que se va desarrollando entre EUA y la URSS y que se caracteriza por la carrera armamentista que se origina entre las dos súper potencias mundiales.

Nada más terminar la II Guerra Mundial, las dos superpotencias, Estados Unidos y la antigua Unión Soviética, dejaron de ser aliadas y se enzarzaron en la llamada guerra fría, que no finaliza hasta la caída del muro de Berlín (9-XI-1989). (Trigo Aranda, 2005. p. 1)

Esta lucha por el poder mundial que emprenden las dos súper potencias mencionadas en párrafo anterior sirve de caldo de cultivo para el vertiginoso avance de la red de redes que se empieza a utilizar en sistemas sofisticados de comunicación que fueron empleados en programas de inteligencia y contra inteligencia que implementaron las dos superpotencias para espiarse mutuamente.

Es en este momento que la tecnología de las comunicaciones sorprende al mundo entero por su velocidad, versatilidad, complejidad y eficiencia en cuanto a la inmediatez que proporcionaba ahorrando significativas medidas de tiempo y espacio, así también recursos materiales como papel, tinta y transporte entre otros.

Según Trigo Aranda (2005) el aparecimiento de los misiles intercontinentales en la época de la guerra fría evidencio la urgencia de que los ordenadores ya existentes se pudieran interconectar entre sí para agilizar la comunicación entre los diferentes comandos militares y de defensa nacional de ambas superpotencias y así dar una respuesta inmediata a cualquier ataque con misiles.

El problema era que existía un nodo central que transmitía información a otros ordenadores dependientes de este nodo y si un misil enemigo destruía el nodo central los

ordenadores dependientes quedaban inutilizados. De esta manera fue como se pensó en convertir a todos los ordenadores en centrales con el propósito que si destruían un ordenador todos los demás seguían transmitiendo.

Así, en 1969 se estableció ARPANET2, la primera red sin nodos centrales, de la que formaban parte cuatro universidades estadounidenses: Universidad de California Los Ángeles (UCLA), Universidad de California Santa Bárbara (UCSB), Universidad de Utah y Stanford Research Institute (SRI). La primera transmisión tuvo lugar el 29 de octubre de 1969, entre UCLA y SRI. (Trigo Aranda, Historia y Evolución de Internet, 2005. p. 2)

Este fue el inicio de la red de redes que posteriormente, de acuerdo con Trigo Aranda (2005), encontró un parteaguas en 1983 cuando el Departamento de Estado de Estados Unidos decide crear su propia red estrictamente confidencial por aspectos de seguridad nacional.

En este tiempo la red de redes no era para nada atractiva para el público general porque no encontraban mayor utilidad con su uso. Fue a inicios de la década de los años 90 que aparecieron buscadores como Google, Yahoo, MSN search, entre otros. Estos ofrecieron a la comunidad virtual la comodidad de encontrar miles de sitios en la red con rapidez y relativa facilidad. Además estos sitios se encontraban ordenados por tema e importancia del documento.

La sistematización de la información de una manera comprensible, la facilidad de acceso y la gratuidad del servicio hizo que los usuarios de internet se multiplicaran rápidamente por millones en todo el mundo. Apareció entonces una dimensión desconocida para la mayoría de habitantes del mundo *el ciberespacio* y con éste surgen una serie de oportunidades para las personas honorables que buscan honradamente información para fines educativos, científicos, informativos, comerciales, financieros, entre otros.

De la misma forma que se expresan las bondades del internet es necesario mencionar el gran riesgo que representa para la seguridad personal, seguridad ciudadana, seguridad nacional, seguridad comercial, seguridad financiera, seguridad pública y en general para la seguridad humana.

El problema se empieza a definir cuando aparecen categorías conceptuales ligadas al ciberespacio tales como cibercrimen, ciberdelincuente, cibercriminal, ciberdelito, ciberseguridad, ciberataque, jaquear, entre otros. Los riesgos y amenazas a la seguridad de las personas,

organizaciones e instituciones se convierten en un problema latente en la cotidianidad de la vida si se observa que el ciberespacio está presente en cualquier lugar que exista un ordenador de escritorio o portátil.

Esto significa que el peligro está presente en todo momento en el trabajo, en el hogar, en la escuela, en la iglesia, en el parque y en todo lugar donde se pueda tener un ordenador con conexión a internet. En esta secuencia de ideas, basta dar una revisión a los medios de comunicación de radio, televisión y prensa escrita para encontrar la diversidad de delitos que se comenten a través de internet que van desde el engaño, el robo de información e identidad, la estafa, la extorción a particulares y a instituciones.

Lo expuesto anteriormente conduce a pensar en qué formas se tienen al alcance para prevenir esta diversidad de amenazas que se presentan en el ciberespacio, encontrando que el Trabajo Social es una profesión idónea para promover la prevención de los ciberdelítos especialmente en grupos sociales que históricamente han sido vulnerados en sus derechos fundamentales.

De esta manera se plantea una serie de preguntas de interrogación con las que se espera generar toda una discusión teórica que conduzca a establecer ¿Cuál es la Importancia del Trabajo Social para la Prevención del Ciberdelito en grupos sociales vulnerables en Guatemala? Por supuesto que estas interrogantes derivaran en una serie de razonamientos y análisis que identificaran los determinantes de la relación Trabajo Social-Ciberdelito.

¿Qué es el ciberespacio?

¿Qué categorías conceptuales se manejan en el ciberespacio?

¿Qué es el ciberdelito?

¿Cuál es el marco jurídico que regula el ciberespacio en Guatemala?

¿Cuál es el marco institucional que vela por la regulación del ciberespacio en Guatemala?

¿Qué relación existe entre Trabajo Social y ciberdelito?

¿Qué procedimientos de Trabajo Social se pueden implementar para la prevención del ciberdelito?

¿Qué importancia tiene el Trabajo Social para la prevención del ciberdelito?

1.1. Delimitación

Ciudad de Guatemala. Año 2023. Instituciones que atienden el ciberdelito en Guatemala. Profesionales de Trabajo Social.

1.2 Objetivos

1.2.1 General:

Identificar la importancia del Trabajo Social en la prevención del Ciberdelito en grupos sociales vulnerables utilizando el marco legal e institucional vigente en el ámbito nacional para el desarrollo de procesos que coadyuven a la prevención del ciberdelito en Guatemala.

1.2.2 Específicos:

Determinar los procesos de Trabajo Social que puedan ser favorables para prevenir el ciberdelito en Guatemala.

Conocer el marco institucional y legal vigente en Guatemala para la prevención y sanción del ciberdelito en todas sus manifestaciones.

Conocer el criterio de los actores directos en el ámbito nacional guatemalteco que intervienen en la prevención del ciberdelito.

Proponer posibles procesos para la integración de esfuerzos entre Trabajo Social y la Institucionalidad que regula el ciberdelito en Guatemala.

1.3 Metodología

En el proceso de la presente investigación se desarrolló una metodología con el enfoque mixto ya que integra estrategias cuantitativas y cualitativas para aprovechar fortalezas de ambos enfoques, asimismo permite triangular hallazgos y enriquecer la interpretación de datos.

En tal sentido se elaboraron instrumentos de investigación consistentes en cinco cuestionarios para ser aplicados a igual número de instituciones públicas encargadas de la atención al ciberdelito en Guatemala.

El universo de estudio es las instituciones públicas del Estado de Guatemala. La muestra es del tipo intencional que se enmarca en el muestreo no probabilístico. Es decir que el investigador seleccionó deliberadamente a cinco instituciones y específicamente a los(as) trabajadores(as) de las Unidades o Dependencias que cumplían ciertos criterios clave para el estudio.

Las instituciones a las que se le aplicó el instrumento son: el Ministerio Público, Ministerio de Gobernación, secretaria para Prevención de Explotación y Trata de personas, Policía Nacional Civil y Trabajadores Sociales.

1.4 Ciberespacio

El ciberespacio es una dimensión que vino a revolucionar el mundo a partir de la segunda mitad del siglo pasado. Los cambios que se han experimentado son increíbles como vertiginosos cambiando increíblemente el campo de las comunicaciones.

(Gibson, 1981) es referido como el escritor que acuñó por primera vez la definición de ciberespacio y la popularizó en 1984 en su obra Neuromante que obtuvo varios premios. Ciberespacio se deriva de la palabra cibernética utilizada por (Wiegner, 1940) para nombrar al estudio de las similitudes entre leyes generales de la comunicación, seres humanos y computadoras.

El ciberespacio es un ámbito artificial que es operado por computadoras, servidores y herramientas tecnológicas. A través de estos mecanismos es posible hacer casi de todo en espacios virtuales. El espació ha sido de mucha utilidad especialmente para las comunicaciones, espacios académicos, de ciencia y de seguridad nacional.

Muchas personas en el mundo entienden los términos ciberespacio e internet como sinónimos, pero hay diferencia entre ambos. Internet se encuentra dentro del ciberespacio que es donde funciona, constituyéndose como una categoría ampliamente menor al ciberespacio.

El ciberespacio es inagotable y se encuentra en cualquier lugar en donde haya un ordenador, por lo que no tiene nacionalidad ni fronteras y existe una gran cantidad de funciones y actividades que aún no se encuentran reguladas por la ley. Esto permitió que aparezcan nuevas amenazas como el robo de identidad, el jaqueo de cuentas bancarias, amenazas a la seguridad

nacional de los Estados, robo de información privada de las personas, entre otras. Estas amenazas mencionadas tienen la figura jurídica de ciberdelito.

A través del ciberespacio es posible atacar a los Estados sin necesidad de utilizar una sola arma. Según (Confidencial, 2023) agentes prorrusos realizaron un ciberataque a la Comandancia Central de la Organización del Tratado del Atlántico Norte (OTAN), dejando inoperantes sus servidores informáticos.

De acuerdo con la revista Estrategia y Negocios (2024) en enero de este año las operaciones en la empresa Claro sufrieron ciberataque que afecto sus operaciones e impido dar el servicio a millones de personas.

Con relación al ciberespacio (Gardey, Pérez 2022) señalan que este concepto se deriva del inglés cyberspace y que hace referencia a la dimensión virtual o espació artificial que se desenvuelve por medio de equipos y elementos informáticos que son operados por seres humanos.

(Gardey, Pérez 2022) refieren que el ciberespacio se puede entender como una realidad virtual que no es física, que no puede ser tocado; si no un sistema digital resultado de la interacción de seres humanos y computadoras con sus respectivos programas.

También estos autores refieren que el ciberespacio tiene una derivación del concepto cibernética que en 1940 fue utilizado por Norbert Wierner para nombrar las relaciones entre personas, sistemas de comunicación y computadoras.

La verdad es que el ciberespacio pone al descubierto una nueva realidad que hace aproximadamente 30 años no se conocía. Se pensó en la virtualidad como un tema de futuro al servicio de comunidades científicas y políticas de alta relevancia mundial y a la ciencia ficción, pero no pasó mucho tiempo para que el ciberespacio y la internet se masificaran a tal grado que en la actualidad las personas en todo el mundo se pueden comunicar en todo momento, no importando la ubicación geográfica en que se encuentren.

En tal sentido se ha hecho necesaria la regulación jurídica del ciberespacio, tarea que se ha dificultado debido a las cualidades virtuales que tiene este campo del conocimiento humano. Los delitos al cometerse en una dimensión virtual se hacen difíciles de juzgar. Aunado a esto, existen algunos grupos sociales que exigen la soberanía del ciberespacio argumentando que es una tribuna para la libertad de expresión y de pensamiento.

No obstante, en Guatemala se han promulgado leyes relativas al ciberdelito y se ha creado institucionalidad para perseguir estos ilícitos virtuales. En el ministerio de gobernación existe una unidad encargada del ciberdelito y en el Ministerio Publico una fiscalía especial se hace cargo de este tema. Esto obedece a la cantidad de hechos denunciados en los que personas particulares han visto violentada su seguridad personal. Es en este momento que se tiene conciencia de que el ciberespacio e internet son plataformas para la libertad de expresión y pensamiento, pero que estas libertades deben ser reguladas en aras de la seguridad individual en una sociedad democrática.

En este sentido, legislaciones como la guatemalteca establece a nivel constitucional que el bienestar general prevalece sobre el particular. En este orden se debe tener en cuenta que, si algún hecho es constitutivo de delito, ya sea que ocurra en la presencialidad o en la virtualidad debe de castigarse para salvaguardar la seguridad de los seres humanos en todo el mundo.

Con este marco de referencia es momento de hablar de la seguridad en el ciberespacio y para ello se debe señalar el aparecimiento de un nuevo concepto que se denomina ciberseguridad. (Microsoft, 2015) refiere que ciberseguridad se refiere a un estado de situaciones en que se protegen personas, instituciones, datos, infraestructura de bienes y servicios básicos de las poblaciones para una subsistencia estable.

Tomando como referencia la definición de ciberseguridad propuesta por Microsoft, es pertinente reconocer que el concepto de datos no se limita a simples registros, sino que abarca un conjunto inagotable de información. Esta incluye desde la esfera privada de los individuos hasta datos estratégicos del Estado, pasando por el comercio, la banca, el flujo de capitales, e incluso sistemas de defensa relacionados con armamento nuclear y biológico. La gestión inadecuada o el uso malicioso de dicha información podría generar consecuencias de gran magnitud, al punto de amenazar la estabilidad global y, en un escenario extremo, la propia supervivencia de la humanidad.

Otro tema importante es la infraestructura vital de los diferentes Estados que incluye, como ya se hizo mención en párrafos anteriores, la salud, el agua, energía eléctrica, transportes y actualmente las comunicaciones. Es por esta razón que la ciberseguridad adquiere una importancia muy singular debido a que desde el ciberespacio se pueden realizar una serie de acciones que impliquen atentados a la paz, salud y seguridad mundial.

Con el anterior marco de referencia un tema que no se puede dejar de lado en materia de ciberseguridad y ciberdelito es el marco jurídico para la tutela del bien común en las sociedades democráticas. Para el caso de Guatemala se cuenta con el siguiente marco jurídico.

1.4.1 Marco Jurídico para la regulación del Ciberespacio en Guatemala

En materia de derecho internacional se encuentra la Declaración Universal de Derechos Humanos (Organización de las Naciones Unidas ONU, 1948) adoptada el 10 de diciembre de ese año. En el artículo 12 de esta declaración se establece:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. (ONU, 1948)

Si se analiza detenidamente este artículo, es posible darse cuenta que de manera directa o indirecta según sea su interpretación protege a los seres humanos del mundo contra los abusos que se puedan cometer en el ciberespacio incluido el ciberdelito.

Lo delicado del ciberespacio es que puede estar en todo lugar, es decir que las personas pueden ser atacadas o agredidas desde cualquier espacio, por cualquier persona y sin el mayor control por parte de las autoridades. Uno de los delitos más comunes y más fáciles de cometer es la calumnia, injuria y difamación, que están tipificados en el Código Penal guatemalteco como delitos contra la moral pública. Estos delitos atacan directamente la vida privada, la correspondencia, la honra y reputación de las personas y de acuerdo con este artículo la ley debe proteger a todo ser humano al momento de ser víctima de estos ataques.

En materia de derecho interno guatemalteco se encuentra la ley superior de Guatemala que es la Constitución Política de la República, que no preceptúa nada directamente acerca del ciberespacio y ciberdelito, pero si contiene artículos que protegen aspectos que se encuentran amenazados por el ciberdelito como, por ejemplo:

> Artículo 4. Libertad e igualdad. En Guatemala todos los seres humanos son libres e iguales en dignidad y derechos. El hombre y la mujer, cualquiera que sea su estado civil, tienen iguales oportunidades y responsabilidades. Ninguna persona puede ser sometida a servidumbre ni a otra condición que menoscabe su dignidad. Los seres humanos deben guardar conducta fraternal entre sí. (Organismo Legislativo, 1985. p. 19)

Como puede observarse, este artículo también reconoce la protección de la dignidad de las personas. En ese sentido, al igual que el resto de los artículos de la Constitución, debe ser desarrollado mediante una ley específica que garantice de manera más efectiva dicho derecho. Esto resulta especialmente relevante en el ámbito del ciberespacio, donde la dignidad y la reputación suelen ser vulneradas con frecuencia, en particular a través de la difusión de noticias falsas que afectan la vida privada, familiar o laboral de los individuos.

> Artículo 24.- Inviolabilidad de correspondencia, documentos y libros. La correspondencia de toda persona, sus documentos y libros son inviolables. Sólo podrán revisarse o incautarse, en virtud de resolución firme dictada por juez competente y con las formalidades legales. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna. (Constitución Política de la Republica de Guatemala, 1985. p. 31)

Este artículo tiene relación directa con varios aspectos que son bastante vulnerables en el ciberespacio y cuya agresión debe tenerse como delito. La protección de estos aspectos de la vida privada de las personas debe ser materia de legislación nacional específica y por lo tanto responsabilidad del Organismo Legislativo.

> Artículo 44.- Derechos inherentes a la persona humana. Los derechos y garantías que otorga la Constitución no excluyen otros que, aunque no figuren expresamente en ella, son inherentes a la persona humana.
>
> El interés social prevalece sobre el interés particular. Serán nulas ipso jure las leyes y las disposiciones gubernativas o de cualquier otro orden que disminuyan, restrinjan o tergiversen los derechos que la Constitución garantiza. (CRPG, 1985. p. 47)

El artículo cuarenta y cuatro de la Constitución Política de la República de Guatemala abre la posibilidad de proteger derechos que no se encuentren estipulados en el cuerpo normativo de la Constitución, este es el caso de aspectos humanos como la vida privada, honra, dignidad y reputación que fácilmente pueden ser dañados por actividades practicadas en el ciberespacio como la difamación, calumnia, robo de identidad entre otros.

> Artículo 45.- Acción contra infractores y legitimidad de resistencia. La acción para enjuiciar a los infractores de los derechos humanos es pública y puede ejercerse mediante simple

denuncia, sin caución ni formalidad alguna. Es legítima la resistencia del pueblo para la protección y defensa de los derechos y garantías consignados en la Constitución. (Organismo Legislativo, (CRPG, 1985. p.48)

Este artículo básicamente funciona como cobertura general para garantizar el castigo a los infractores de derechos humanos y se puede interpretar que en esta categoría de infractores están comprendidos los ciberdelincuentes que cometen sus fechorías en el ámbito poco controlado del ciberespacio.

Artículo 46.- "Preeminencia del Derecho Internacional. Se establece el principio general de que, en materia de derechos humanos, los tratados y convenciones aceptados y ratificados por Guatemala, tienen preeminencia sobre el derecho interno". (CRPG, 1985. p.48)

El anterior artículo se cita por considerar que reconoce la preeminencia que tienen los tratados internacionales ratificados por Guatemala en materia de derechos humanos. Este no solo permite que exista legislación internacional vigente en Guatemala en materia de protección de derechos fundamentales, algunos de los cuales pueden ser afectados por el ciberdelito.

Luego de la Constitución Política de la República de Guatemala se encuentra el Código Penal que sufre reformas a dos artículos para ofrecer protección legal a ciertas actividades que se dan en el ciberespacio.

1.4.2. Reformas al Código Penal de Guatemala

A través de decreto legislativo 11-2022 el Congreso de la República de Guatemala reforma el artículo 190 del Código penal para incluir figuras delictivas identificadas con el ciberdelito. A continuación, se describen las reformas planteadas en el decreto en mención.

Artículo 1. Se adiciona el artículo 190 Bis al Decreto Número 17·73 del Congreso de la República, Código Penal, el cual queda así:

Artículo 190 Bis. Seducción de niños, niñas o adolescentes por el uso de las tecnologías de información. Quien, a través de todo tipo o clase de medios tecnológicos, valiéndose o no del anonimato, contacte a cualquier niño, niña o adolescente con el propósito de:

a. Solicitar o recibir material con contenido sexual o pornográfico, propio o de terceras personas, ya sea que incluya o no medios audiovisuales;

b. Tener o facilitar con tercera persona relaciones sexuales;

c. Facilitar la comisión de cualquier otro delito contra la libertad o indemnidad sexual del niño, niña o adolescente contactado.

El responsable de una o varias conductas anteriormente indicadas, será sancionado con prisión de seis (6) a doce (12) años, independientemente que logre su propósito. La pena será aumentada en dos terceras partes, cuando la víctima sea un niño, niña o adolescente con incapacidad cognitiva o volitiva. La pena se impondrá sin perjuicio de las que puedan corresponder por la comisión de otros delitos. (CPRG, 2022. sp.)

Artículo 2. Se adiciona el artículo 190 Ter al Decreto Número 17-73 del Congreso de la República, Código Penal el cual queda así:

> Articulo 190 Ter. Chantaje a niños, niñas o adolescentes mediante el uso de tecnologías de información o medios tecnológicos. Quien, mediante el uso de tecnologías de información o medios tecnológicos valiéndose o no del anonimato, amenace a un niño niña, adolescente o sus representantes legales con difundir material con contenido sexual o pornográfico propios del niño, niña o adolescente, ya sea que el material esté contenido en medios audiovisuales u otros, será sancionado con prisión de seis (6) a doce (12) años. La pena será aumentada en dos terceras partes, cuando la víctima sea un niño, niña o adolescente con incapacidad cognitiva u volitiva. La pena se impondrá sin perjuicio de las que puedan corresponder por la comisión de otros delitos. (CPRG, 2022. s.p.)

Antes de estas reformas, estos delitos no estaban tipificados en la Ley, lo que dificultaba su persecución penal. La nueva legislación busca proteger la libertad e indemnidad sexual de las niñas, niños y adolescentes en Guatemala. Desde el 12 de marzo de 2022, se llevan a cabo procesos penales por estos dos nuevos delitos, y el Ministerio Público está investigando actualmente algunos casos.

Continuando con el tema, es importante que las víctimas conserven las constancias de las conversaciones o mensajes enviados por los agresores, ya que estas pueden ser pruebas fundamentales en un proceso penal.

Se puede dar el caso de que padres o personas tutoras de menores tengan algún grado de responsabilidad en la comisión del delito. En esta situación se debe buscar el apoyo de la

Procuraduría General de la Nación para buscar la protección de los menores con familiares cercanos y realizar los procedimientos y medidas que sean necesarias para alejar a la víctima de su victimario.

Concluyendo con el tema se puede observar que la legislación guatemalteca está sufriendo cambios tendientes a la regulación del ciberespacio y con ello también regular y sancionar el ciberdelito para una mejor protección de los entornos digitales a nivel nacional.

1.5 Relación Ciberespacio-Internet

Tomando en cuenta lo descrito en el párrafo anterior, es preciso mencionar que después de la segunda guerra mundial Estados Unidos de América y la Unión de Repúblicas Socialistas Soviéticas se enmarcaron en una etapa caracterizada por amenazas, espionaje, carrera armamentista y una serie de eventos que tenían como objetivo extender sus áreas geográficas de influencia política lo más que pudieran. De esta manera se fue desarrollando una red de comunicaciones que cada vez se fue haciendo más compleja y sofisticada.

Esta red de comunicaciones se inició en universidades norteamericanas específicamente en el Estado de California, cuyo fin era la investigación académica y científica. Inmediatamente las instancias de seguridad nacional de Estados Unidos de América se dieron cuenta de la amplia gama de posibilidades que ofrecía esta red y no dudaron en crear su propia red informática de alta seguridad.

Esta red denominada por los expertos *red de redes* se empezó a utilizar para manejar información que denominaron sensible y a la cual tenían acceso solo personal de defensa debidamente autorizado, ya que dicha información contenía resultados de espionaje, sabotajes, atentados, descubrimientos en cuanto al manejo de la energía nuclear, nuevos y sofisticados armamentos entre otros.

Paralelamente a este ejercicio de utilización de la red de redes para el desarrollo de proyectos de defensa y prácticas militares por parte de las dos superpotencias de la época, el mundo entero se fue dando cuenta que la red ofrecía posibilidades casi inagotables para ser utilizada en infinidad de actividades incluso ilícitas. Es así como aparece una nueva amenaza para la humanidad que viene a poner en alto riesgo la seguridad personal en las diferentes regiones del globo terrestre.

Es en este momento que se empieza a hablar de conceptos poco conocidos como hardware, software, humanware, internet, ciberespacio, cibernautas, cibercrimen, ciberdelito, ciberseguridad, entre otros. Por el tema de esta investigación se considera importante tocar de manera sucinta cada uno de estos conceptos debido a que tienen una relación directa o indirecta con el ciberdelito.

Hardware: Conjunto de los componentes que integran la parte material de una computadora. *Software*: Conjunto de programas, instrucciones, datos y reglas informáticas para ejecutar ciertas tareas en una computadora". (Computación, 2017. p. 11)

El concepto de *Humanware* remite directamente al ser humano, en tanto hace referencia al recurso humano que trabaja, opera o interactúa con los dos elementos señalados en el párrafo anterior.

En efecto, los tres elementos mencionados anteriormente resultan indispensables para el funcionamiento de la red de redes (internet). Dentro de cada uno de ellos se distinguen múltiples componentes: en el ámbito material o hardware se incluyen las computadoras personales, portátiles, tabletas, teléfonos móviles, entre otros dispositivos; en el plano intangible o software se encuentran numerosos programas y aplicaciones que permiten operar el equipo físico; finalmente, en lo que respecta al humanware, intervienen diversas personas que interactúan con el hardware y el software con fines de investigación, desarrollo científico, actividades académicas, deporte, entretenimiento, comunicación, espionaje, entre otros.

En relación a la definición de internet, la Real Academia Española define "Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación". (Española, 2020)

Resulta muy fácil darse cuenta de la interacción entre hardware, software y humanware de la cual resulta una inagotable fuente de actividades, acciones, relaciones y comportamientos humanos que ha venido a establecer un complejo escenario virtual que es susceptible de ser utilizado de manera legal y socialmente aceptado o de manera ilegal que definitivamente no es aceptado por la sociedad.

No se puede dejar de mencionar la relación que tiene el ciberespacio respecto del internet, ya que es en esta red que se desarrolla esa dimensión ciberespacial que parece ser tan infinita como

el universo mismo. Si bien es cierto que el ciberespacio es una categoría más amplia que el internet, también es cierto que el ciberespacio necesita del internet para desarrollarse.

A partir de la segunda mitad del siglo pasado y las primeras dos décadas del siglo XX, la tecnología ha sido una de las fuerzas más importantes en la transformación de la sociedad, y el ciberespacio es uno de los fenómenos que ha surgido como detonante de este vertiginoso cambio en las comunicaciones, en la ciencia, la academia, el entretenimiento, entre otros.

Como ya se ha mencionado con anterioridad el ciberespacio es un espacio virtual donde se desarrollan actividades económicas, sociales, culturales, entre otras. Su principal característica es que está integrado por una serie de redes digitales donde se generan y circulan grandes cantidades de información.

A diferencia de otras infraestructuras digitales, internet se constituye la red más importante y utilizada dentro del ciberespacio. Sin embargo, no es la única: también lo integran otras plataformas digitales como el correo electrónico, las redes sociales o los juegos en línea, que amplían y diversifican las formas de interacción en este espacio virtual.

Una de las similitudes más destacables entre el ciberespacio e internet es que ambos han revolucionado la comunicación e interacción humana. Gracias al ciberespacio, las personas pueden comunicarse a través de diversas plataformas y dispositivos, como la mensajería instantánea o la videoconferencia. Igualmente, internet ha permitido una conexión global y la difusión de información de manera instantánea, así como la creación de comunidades virtuales donde personas con intereses similares pueden interactuar e intercambiar información.

No obstante, existen diferencias entre ciberespacio e internet. El ciberespacio es un espacio abstracto que se genera por la conexión de diferentes redes digitales, mientras que internet es una red de comunicación global donde es posible acceder a información y recursos que se encuentran en diferentes lugares del mundo. Además, el ciberespacio implica una conexión entre personas, donde se generan relaciones sociales y culturales, mientras que internet se enfoca en la tecnología y la comunicación.

Para una mayor y mejor comprensión del tema hay que insistir en cuanto a la relación entre ciberespacio e internet. En este sentido, es importante señalar que internet es la principal herramienta para acceder al ciberespacio, pero el ciberespacio no se reduce a internet.

El ciberespacio es un concepto que ha ido evolucionando con la incorporación de nuevas redes digitales y tecnologías de la información. Asimismo, el ciberespacio y la internet son dos conceptos interconectados que se retroalimentan mutuamente, pues el desarrollo de nuevas tecnologías y herramientas digitales está estrechamente relacionado con la evolución del ciberespacio.

En conclusión, el ciberespacio e internet son dos conceptos que han revolucionado la manera en que las personas se relacionan y acceden a la información. Aunque el ciberespacio se integra por diferentes redes digitales, internet es su principal herramienta y la que ha permitido un acceso global e instantáneo a los recursos y la información que se encuentran en él.

A medida que avanza la tecnología, el ciberespacio seguirá evolucionando y transformando la sociedad. Expresándolo de manera figurada el mundo se hará cada vez más pequeño debido a que las personas con acceso a un ordenador digital tendrán un innumerable cúmulo de posibilidades para interactuar en entornos digitales en cualquier parte del mundo.

1.6 Impacto del ciberespacio en la sociedad

El tema del ciberespacio ha marcado una influencia revolucionaria en el mundo del siglo XXI. En el escenario mundial actual la libertad de la información y el acceso a la misma se ha popularizado que casi cualquier persona puede ingresar a diversos entornos digitales.

El aparecimiento del ciberespacio y de redes virtuales ha impactado a las sociedades de los diferentes Estados del mundo en sus relaciones internacionales, en la política, en el intercambio comercial, en la ciencia, la cultura, el deporte, las comunicaciones y el transporte, entre otros.

No obstante, esta nueva realidad mundial requiere de nuevas estrategias para hacer frente a los desafíos que plantea el mundo de la virtualidad para que la humanidad continúe avanzando dentro de los parámetros de la paz, fraternidad, democracia y derechos humanos que son los postulados esenciales que plantea el máximo organismo mundial representado en la Organización de las Naciones Unidas ONU.

Uno de los principales impactos del ciberespacio en la sociedad humana es su potencial para el manejo de información. En la actualidad se puede acceder en pocos segundos a información de diverso tipo con solo buscarla en una red virtual.

El avance de la tecnología de las comunicaciones y de motores de búsqueda ha facilitado la ubicación de información específica y certera. La tecnología también ha hecho posible la creación de redes globales; las personas de diferentes partes del mundo pueden conectarse instantáneamente gracias al ciberespacio.

La ciencia, la educación, la medicina, las artes, los deportes y la comunicación, han tenido una expansión como nunca en la historia de la humanidad. El conocimiento humano se ha vuelto tan vertiginoso que los avances suceden en intervalos de tiempo cada vez más cortos.

Otro impacto del ciberespacio en la sociedad es su papel en la economía. La globalización ha creado nuevas oportunidades para los negocios y ha revolucionado la forma en que las empresas operan. Los mercados globales se han hecho más accesibles a través del ciberespacio, lo que ha puesto en igualdad de condiciones a pequeñas empresas con grandes corporaciones. En algunos casos, han surgido los negocios que operan exclusivamente en línea, lo que ha llevado a la creación de empleos y a la innovación en el ámbito empresarial.

No obstante, esta explosión tecnológica encuentra limitaciones en cuanto a quienes tiene acceso a ella. Esto significa que, aunque la información está más cerca no todos tienen las condiciones necesarias para acceder a estos entornos virtuales. Esta situación limita la capacidad para conectarse a la red de redes y aprovechar las oportunidades que el ciberespacio ofrece. También hay que señalar que la creciente dependencia de la tecnología podría conducir a una gran brecha digital entre grupos sociales y por ende a la exclusión social.

Hay que marcar que uno de los grandes beneficios del ciberespacio es la generación de una cultura de la inmediatez en la que las personas se han acostumbrado a resultados inmediatos y efectivos para los diferentes fines que se proponen. Ciertamente esta cultura que se está generando choca con la cultura de la paciencia y constancia en la búsqueda de información que es a la que se practicaba con anterioridad.

De manera paralela, es posible que se estén perdiendo prácticas de comunicación interpersonal en la familia, el trabajo y la escuela, lo que propicia el individualismo y una progresiva abstracción social. Esta situación se relaciona con el uso constante de teléfonos móviles, tabletas y ordenadores, fenómeno que se observa en diversos contextos cotidianos como reuniones

familiares, espacios laborales, aulas, parques o cafeterías. Como consecuencia, se reduce en cierto grado la convivencia familiar y social que solía practicarse en el pasado.

En términos generales no cabe la menor duda que el ciberespacio ha tenido un impacto muy fuerte en la sociedad con sus beneficios, pero también con sus amenazas o riesgos. Uno de los temas de mayor beneficio es el desarrollo y constante actualización de la tecnología de las comunicaciones con lo que se ha logrado un inmediato acceso a la información beneficiando a millones de personas en todo el mundo.

No obstante, no hay que olvidar los desafíos como la calidad educativa, cobertura educativa, la exclusión, entre otros. Desafíos en los que hay que trabajar fuerte para lograr un mundo integrado al ciberespacio sin que ningún grupo social sea excluido.

1.7 Grupos Vulnerables

Son segmentos de población que se encuentran en situación de desventaja, lo que los expone a situación de discriminación, exclusión y vulneración de sus derechos humanos.

1.7.1 Mujeres Indígenas

"En Guatemala, las mujeres indígenas enfrentan altos niveles de discriminación y exclusión social. Un informe de la Comisión Internacional de Juristas señaló que las mujeres indígenas son las más afectadas por la pobreza, la violencia y la discriminación" (Comisión Internacional de Juristas [CIJ], 2019)

En Guatemala, la población indígena representa alrededor del 43.6% del país, y las mujeres indígenas han sido históricamente marginadas y discriminadas debido a su género, raza y condición socioeconómica. Estas mujeres enfrentan múltiples desafíos y obstáculos para acceder a sus derechos y necesidades básicas, lo que limita seriamente sus oportunidades de desarrollo y bienestar.

En términos de educación, muchas mujeres indígenas no tienen acceso a la educación primaria o secundaria, y mucho menos a la educación superior. Esto se debe a una combinación de factores, como la exclusión lingüística, la pobreza y la discriminación cultural hacia las mujeres, lo que significa que a menudo se les asigna un papel secundario en la sociedad. La falta de

educación perpetúa el ciclo de pobreza, ya que las mujeres indígenas pueden tener menos oportunidades de trabajo y menos capacidad para salir de la pobreza.

Además del acceso limitado a la educación, las mujeres indígenas también enfrentan problemas de salud. La falta de servicios de salud accesibles y adecuados, especialmente en las áreas rurales donde vive la mayoría de la población indígena, significa que estas mujeres tienen más probabilidades de sufrir enfermedades y enfermedades relacionadas con la pobreza, como la desnutrición y la mala salud reproductiva.

En cuanto a la violencia de género, las mujeres indígenas son particularmente vulnerables debido a su condición de género y cultura. Muchas mujeres indígenas son víctimas de abuso físico y sexual, y a menudo no tienen acceso a recursos legales o de otro tipo para abordar estos problemas. Además, la discriminación cultural y racial significa que a menudo se les niega justicia y protección por parte de las autoridades.

En resumen, las mujeres indígenas en Guatemala enfrentan enormes desafíos y exclusiones en términos de educación, salud y derechos de género. Se necesita un esfuerzo concertado y sostenido, tanto a nivel local como internacional, para apoyar y empoderar a estas mujeres y abordar las desigualdades y violaciones de derechos que enfrentan.

1.7.2 Personas con Discapacidad

Las personas con discapacidad en Guatemala también enfrentan problemas de exclusión social y económica. Según un informe de la Comisión Económica para América Latina y el Caribe, la mayoría de las personas con discapacidad en Guatemala vive en la pobreza y enfrenta barreras para el acceso a la educación y el empleo (CEPAL, 2019)

En el Estado de Guatemala, las personas con discapacidad enfrentan múltiples barreras y desafíos para acceder a sus derechos y necesidades básicas. La discriminación, la falta de acceso a los servicios y la falta de oportunidades de empleo son solo algunos de los desafíos que enfrentan diariamente.

En términos de educación, las personas con discapacidad tienen acceso limitado a instituciones educativas y, cuando lo logran, a menudo enfrentan barreras lingüísticas y de accesibilidad debido a la falta de recursos tales como intérpretes de lenguaje de señas y tecnologías

asistidas. La discriminación también limita el acceso a oportunidades de empleo, lo que perpetúa el ciclo de pobreza y exclusión de la sociedad.

La falta de accesibilidad a los servicios también es un problema importante. Muchas personas con discapacidad en Guatemala enfrentan obstáculos para acceder a servicios básicos, como atención médica y transporte público. Esto se debe a la falta de infraestructura y equipamiento adaptado para personas con discapacidad.

Además, la falta de apoyo y políticas gubernamentales efectivas también es un problema importante en la lucha por los derechos de las personas con discapacidad en Guatemala. A pesar de algunas iniciativas recientes, aún hay mucho por hacer para garantizar que las personas con discapacidad tengan acceso a oportunidades equitativas en todas las áreas de la vida.

En síntesis, las personas con discapacidad en Guatemala enfrentan múltiples desafíos para acceder a sus derechos y necesidades básicas. La discriminación, la falta de accesibilidad y la falta de políticas gubernamentales efectivas son solo algunos de los desafíos que enfrentan diariamente. Se necesita un esfuerzo concertado y sostenido por parte de la sociedad civil y el gobierno para abordar estas barreras y garantizar que las personas con discapacidad tengan igualdad de oportunidades y acceso a servicios y recursos clave.

1.7.3. Niños y Niñas

Los niños y niñas en Guatemala también enfrentan altos niveles de pobreza y exclusión social. Según UNICEF, “(…) más de la mitad de los niños y niñas en Guatemala viven en la pobreza, y muchos están expuestos a la violencia y el abuso" (UNICEF, 2020).

La situación de la niñez en Guatemala puede describirse como precaria y vulnerable. Las desigualdades socioeconómicas, la falta de acceso a servicios básicos y la discriminación son solo algunos de los desafíos a los que se enfrentan los niños y niñas guatemaltecos.

En términos de educación, muchos niños y niñas en Guatemala tienen acceso limitado a la educación primaria y secundaria. Debido a la pobreza y la discriminación cultural, a menudo se espera que las niñas cuiden de los hermanos menores y realicen tareas domésticas en lugar de asistir a la escuela. Además, la falta de financiación y de recursos educativos adecuados para las zonas rurales donde vive la mayoría de la población guatemalteca dificulta el acceso y mantienen altas tasas de analfabetismo.

La salud infantil es otro tema crítico. Las tasas de mortalidad infantil y materna son alarmantemente altas en Guatemala, causadas por la falta de acceso a servicios de atención médica y el acceso a agua potable. Además, muchos niños y niñas sufren de problemas de salud relacionados con la desnutrición, que también están relacionados con la pobreza.

La violencia es otra preocupación para los niños y niñas guatemaltecos. La violencia se produce en forma de abuso infantil, la explotación laboral infantil y la violencia sexual. Además, en el contexto de la violencia generalizada en el país, los niños y niñas a menudo son testigos de la violencia y pueden sufrir trastornos de estrés postraumático.

En conclusión, los niños y niñas en Guatemala enfrentan graves desafíos en múltiples áreas de la vida, como la educación, la salud y la seguridad. Es crucial que el gobierno, las organizaciones no gubernamentales y la sociedad en su conjunto trabajen juntos para abordar estas barreras y garantizar que tengan acceso a una educación de calidad, atención médica y seguridad para prosperar y desarrollarse.

1.7.4 Pueblos Indígenas

La población indígena es otro grupo vulnerable que también enfrentan altos niveles de discriminación y exclusión social en Guatemala. En un informe de Amnistía Internacional se señala que las comunidades indígenas en Guatemala están expuestas a la violencia y la discriminación por parte de las autoridades y otros grupos. (Amnistia Internacional, 2019)

La población indígena en el Estado de Guatemala representa cerca del 60% de la población total, y es un grupo racial y culturalmente diverso que abarca más de 20 grupos étnicos diferentes. A pesar de constituir la mayoría de la población, la población indígena ha sido históricamente discriminada y marginada en todos los aspectos de la vida en Guatemala.

Uno de los mayores problemas que enfrenta la población indígena es la falta de acceso y representación política. Las instituciones políticas del país están dominadas por una pequeña élite de la población criolla, y las políticas y decisiones gubernamentales a menudo ignoran las necesidades y perspectivas de la población indígena.

Otro problema importante que debería mencionarse es el acceso limitado a la educación y la salud. La mayoría de los miembros de la población indígena vive en zonas rurales y tiene acceso limitado a servicios básicos de atención médica y educación de calidad, especialmente en áreas

remotas y aisladas. Además, la falta de educación y salubridad son factores significativos que contribuyen a la proporción de mal nutrición infantil entre la población indígena.

La discriminación cultural y la exclusión lingüística también son problemas crónicos que enfrenta la población indígena en Guatemala. La discriminación cultural afecta los derechos y libertades de los miembros de esta población, afectando su identidad, su integridad física, su idioma y su religión.

Concluyendo, la situación de la población indígena en Guatemala es precaria y preocupante. La exclusión política, la falta de acceso a servicios básicos de educación y salud de calidad y la discriminación cultural y lingüística son problemas importantes que enfrentan los miembros de esta población. Es esencial que el gobierno, la sociedad y las organizaciones internacionales trabajen juntas para abordar estos desafíos y para garantizar que la población indígena tenga acceso igualitario a los derechos, recursos y servicios básicos que necesitan para vivir dignamente.

1.7.5. Personas en Situación de Calle

Las personas en situación de calle también son un grupo vulnerable en Guatemala. Según el Comité Internacional de la Cruz Roja, las personas en situación de calle en Guatemala enfrentan problemas de salud, seguridad y acceso a la vivienda y los servicios básicos (Comite Internacional de la Cruz Roja, 2018).

Las personas en situación de calle en Guatemala son un problema social que afecta especialmente a las zonas urbanas. Los motivos por los que las personas viven en la calle son diversos; algunos de ellos se han quedado sin hogar por situaciones de desempleo, marginación, pobreza extrema, falta de capacitación y drogadicción. Las personas en situaciones de calle en Guatemala enfrentan múltiples desafíos diarios, ya que estas situaciones afectan seriamente su calidad de vida.

Uno de los principales problemas que enfrentan estas personas es el acceso limitado a servicios básicos, como alimento, agua potable y atención médica. Muchos residentes sin hogar en Guatemala carecen de acceso a servicios de salud básicos y a atención social y médica. Además, la mayoría de ellos vive en condiciones precarias, lo que aumenta su vulnerabilidad a enfermedades y otros problemas de salud.

La falta de integración social también es otra problemática grave para las personas en situación de calle en Guatemala. La marginación social, la discriminación y la estigmatización son problemas crónicos que dificultan que estas personas puedan encontrar trabajo y medios de subsistencia, lo que a su vez los fuerte a continuar viviendo en la calle.

La violencia y la delincuencia son otros riesgos graves a los que se enfrentan las personas sin hogar en Guatemala. Muchos residentes en situación de calle son víctimas de robos, violencia y agresiones, y algunos también han sufrido abusos por parte de la policía.

En síntesis, las personas en situación de calle en Guatemala enfrentan múltiples desafíos que afectan de manera directa su calidad de vida y bienestar. Esto resulta indispensable que el Estado y las organizaciones no gubernamentales trabajen de forma articulada para garantizarles acceso a servicios básicos, atención médica, apoyo social y oportunidades de inserción laboral. Por encima de todo, se debe procurar que cuenten con un espacio digno, estable y seguro al que puedan llamar hogar.

1.7.6. Personas Adultas Mayores

Las personas adultas mayores también son un grupo vulnerable en Guatemala, especialmente en términos de acceso a la atención médica y la pensión. Según el (Fondo Monetario Internacional, 2018) solo el 14 % de las personas en edad de pensión en Guatemala recibe pensión, y menos del 20 % de la fuerza laboral activa aporta al sistema de pensiones, lo que sugiere que un porcentaje significativo de personas mayores depende finalmente del apoyo familiar para sobrevivir.

En Guatemala, las personas adultas mayores enfrentan múltiples desafíos y obstáculos que afectan su calidad de vida y bienestar. La mayoría de estas personas vive en zonas rurales y tienen acceso limitado a servicios básicos de salud y nutrición.

Una de las mayores problemáticas para las personas adultas mayores es la falta de acceso a atención médica y servicios de salud de calidad. Muchas personas mayores que viven en áreas rurales tienen dificultades para acceder a atención médica y algunos ni siquiera pueden permitirse el acceso a servicios médicos básicos. Además, muchas personas mayores en Guatemala tienen enfermedades crónicas como diabetes, hipertensión y enfermedades cardíacas, por lo que necesitan acceso a servicios médicos y medicamentos específicos para estas condiciones.

La pobreza es también otro obstáculo que afecta a la calidad de vida de las personas adultas mayores en Guatemala. Muchas de estas personas viven en condiciones de pobreza extrema y carecen de acceso a servicios básicos, como alimentación y vivienda adecuada. Además, la mayoría de ellos se ha jubilado y también enfrentan problemas financieros para satisfacer sus necesidades básicas, lo que aumenta su vulnerabilidad a sufrir inseguridad alimentaria y falta de acceso a productos de primera necesidad.

La discriminación y la exclusión social son también factores que afectan a las personas mayores en Guatemala. A menudo, estas personas enfrentan aislamiento social y están marginadas de las actividades sociales y comunitarias. La discriminación también está presente en el mercado de trabajo, donde las personas mayores tienen menos oportunidades de empleo y se ven afectadas por la discriminación de edad.

Por último, las personas adultas mayores en Guatemala enfrentan una serie de desafíos y obstáculos que afectan su calidad de vida y bienestar. Es importante que el gobierno, la sociedad y las organizaciones internacionales trabajen juntos para abordar estos problemas y garantizar que estas personas tengan acceso a servicios básicos, atención médica de calidad, servicios de apoyo y protección social. También se necesita una toma de conciencia y sensibilización sobre los derechos de las personas mayores, y debe promoverse respeto cultural y social para ellos, reduciendo así la exclusión y discriminación hacia ellos en la sociedad guatemalteca.

1.7.7 Personas Desplazadas

Según el Alto Comisionado de las Naciones Unidas para los Refugiados (ACNUR), al finalizar 2024 había 180 276 personas desplazadas dentro de Guatemala (ACNUR, 2024)

Las personas desplazadas por el conflicto armado en Guatemala representan una de las situaciones más difíciles que ha enfrentado el país. Durante la década de 1980, los guerrilleros y las fuerzas gubernamentales lucharon una guerra civil que duró más de treinta años, y en la que numerosas comunidades fueron desplazadas de sus hogares.

La mayoría de estas personas desplazadas, son indígenas de áreas rurales del país y fueron forzadas a abandonar sus hogares debido a la violencia y la inseguridad que enfrentaban en sus comunidades. A menudo, las personas desplazadas se han visto obligadas a huir a regiones remotas

del país, a menudo en la selva, donde se encuentran con grandes dificultades para acceder a alimentos, agua potable, atención médica y otros recursos básicos.

A pesar de que la guerra civil concluyó hace muchos años, existe todavía una considerable cantidad de personas desplazadas que todavía no han podido regresar a sus hogares. El problema se ha agravado debido al aumento del crimen organizado, la violencia, los conflictos de tierras y otros problemas sociales que han impedido el regreso de estas personas.

Las personas desplazadas en Guatemala se enfrentan a una variedad de dificultades causadas por la falta de acceso a recursos y servicios básicos. Las condiciones de vida en los campamentos son extremadamente difíciles y muchas personas sufren de problemas de salud como infecciones respiratorias, enfermedades diarreicas y malnutrición. El acceso a servicios de educación, servicios médicos y protección social sigue siendo una cuestión de preocupación, lo que aumenta la vulnerabilidad de las personas desplazadas.

La realidad social guatemalteca evidencia que las personas desplazadas por el conflicto armado en Guatemala continúan enfrentando situaciones difíciles marcadas por la exclusión social, la discriminación, la falta de acceso a servicios básicos, la falta de protección y apoyo social, lo que limita sus posibilidades de desarrollo. Es esencial que las autoridades continúen trabajando juntas para abordar estos problemas mediante la creación de políticas para reubicar a las personas desplazadas y garantizando que tengan acceso a servicios básicos y protección social, para reducir de esta forma la problemática de las personas desplazadas por el conflicto armado en Guatemala.

1.7.8 Población Rural

La población rural o la Guatemala profunda como también se le ha denominado también enfrentan problemas de pobreza y acceso limitado a servicios básicos como la educación y la atención médica. Según la Comisión Económica para América Latina y el Caribe, "…la población rural en Guatemala enfrenta desafíos en términos de acceso a la educación, la atención médica y la infraestructura básica" (CEPAL, 2019)

La población rural en Guatemala experimenta una situación socioeconómica desigual en comparación con la población urbana, lo que se traduce en una mayor pobreza y exclusión social. El país tiene una población rural significativa que representa el 38% de toda la población del país.

Una de las mayores problemáticas radica en la falta de acceso a servicios básicos de educación, salud, agua potable y saneamiento. La mayoría de la población rural en Guatemala vive en condiciones precarias, lo que implica una limitación para adecuado acceso a la atención médica y educación necesaria para un desarrollo completo.

La población rural también se enfrenta a limitaciones financieras, a menudo se les asignan trabajos mal remunerados o informales, por lo que enfrentan desempleo o subempleo. Además, la falta de acceso a recursos financieros significa que la población rural enfrenta dificultades para invertir en sus tierras y explotar los recursos de la región.

El acceso limitado a servicios de transporte y comunicación también es un impedimento enfrentado por la población rural. La falta de carreteras adecuadas hace que el ingreso y comercio de personas que viven en estas regiones sea difícil y a menudo caro, limitando así su capacidad para comercializar y vender productos de la zona. Además, la falta de electricidad y otros servicios de comunicación significa que el acceso a servicios de telecomunicaciones y de conexión a internet es limitado.

Otras problemáticas enfrentadas por la población rural incluyen la discriminación, el acaparamiento de tierras y la violencia. La discriminación y exclusión por cuestiones de género, raza y etnia se pueden observar con frecuencia en zonas rurales, lo que implica limitaciones en el acceso a recursos y servicios. El acaparamiento de tierras es una problemática significativa, que limita la capacidad de la población rural para acceder a tierras y explotarlas. Además, la violencia también afecta a la población rural, ya sea como resultado de la actividad criminal o por el conflicto generado por la construcción de territorios hidroeléctricos.

En este marco de referencia se puede inferir que la situación socioeconómica de la población rural en Guatemala revela una alta exclusión social, generando a menudo pobreza e inestabilidad. Es fundamental abordar estos problemas para que la población rural pueda acceder a servicios básicos, oportunidades laborales, inversiones en tierra y bienes de capital, y así mejorar su calidad de vida y bienestar.

Capitulo II. El ciberdelito

2.1 Definición del Ciberdelito

Por su parte el ciberdelito es una figura delictiva que aparece casi de forma simultánea con la dimensión virtual del ciberespacio. Ambos conceptos eran desconocidos por la población mundial hasta la segunda mitad del siglo XX en que apareció internet en plena etapa histórica de guerra fría como instrumento de manejo de información secreta también llamada sensible por las dos superpotencias que emergieron después de la segunda guerra mundial Estados Unidos de América en adelante EUA y la Unión de Repúblicas Socialistas Soviéticas en adelante URSS.

Existen definiciones de diferentes autores y fuentes, por ejemplo:

> El ciberdelito se refiere a la conducta delictiva que se lleva a cabo por medio de una red informática, y que puede incluir desde el acceso ilegal a sistemas y datos, hasta la difusión de virus informáticos y el robo de información personal y financiera de los usuarios (Rodríguez, 2016. p. 29)

En la definición anterior de ciberdelito se puede intuir que es necesario contar con el apoyo de recursos técnicos de comunicación como una red informática para cometer un ciberdelito y que éste puede afectar a Instituciones gubernamentales, no gubernamentales, Organizaciones y personas particulares.

Otra definición importante es: "El ciberdelito se define como el delito que se comete mediante el uso de tecnologías de la información y las comunicaciones y que afecta a la confidencialidad, integridad o disponibilidad de los datos almacenados en sistemas informáticos" (Conseyu de la Xusticia d´Asturies, 2019. p.17)

Se puede observar que la definición anterior hace énfasis en las tecnologías de la información y comunicación como elementos importantes para cometer un ciberdelito. Es decir, toda vez una acción cometida al margen de la ley utilizando técnicas informáticas en el ciberespacio se convierte en la figura delictiva de ciberdelito.

Para culminar con una última definición del ciberdelito se puede referir: “El ciberdelito se caracteriza por el uso de la tecnología y las redes de comunicación para la comisión de actos delictivos como el robo, fraude, difamación, extorsión, acoso, entre otros" (Santos & Bertozzi, 2018, p. 24)

En ésta última definición también se observa la mención del uso de tecnología y redes de comunicación con lo que es posible inferir que para la comisión de un ciberdelito la condición sine qua non es la utilización de tecnología de la información y comunicación.

2.2 Los tipos de ciberdelito

Como se ha mencionado en acápites anteriores con el surgimiento del ciberespacio se dan avances que representan grandes oportunidades para el desarrollo de la tecnología de las comunicaciones, pero también aparecen amenazas como el ciberdelito. Dentro de algunos de los delitos cibernéticos más comunes en Guatemala se incluyen:

2.2.1. Extorsión a través de llamadas telefónicas o medios digitales

La extorsión por medios digitales es una forma de delito que ha emergido con la expansión de la tecnología y el internet. Este tipo de extorsión, también conocida como extorsión en línea, implica el uso de herramientas digitales para amenazar, chantajear o coaccionar a una persona para obtener un beneficio económico o de otro tipo. En Guatemala, la legislación ha tenido que adaptarse para enfrentar estos nuevos retos y proporcionar protección a las víctimas de este delito.

Este delito cometido por medios digitales se refiere a cualquier acto de coerción o chantaje que se realiza a través de plataformas digitales. Este tipo de extorsión puede tomar varias formas, como amenazas de difusión de información privada, suplantación de identidad, o el uso de malware para obtener información sensible.

Según (Martínez, 2022) "la extorsión digital es una modalidad de delito en la que el agresor utiliza tecnologías de la información para amenazar o chantajear a la víctima con el fin de obtener un beneficio económico o personal". El fácil acceso y el anonimato que ofrecen los medios digitales han facilitado el crecimiento de este tipo de delitos. Diversos grupos sociales se sienten desprotegidos ante esta amenaza dentro de estos grupos se encuentran los denominados grupos vulnerables quienes tienen un mayor grado de riesgo por su condición de vulnerabilidad.

En Guatemala, la protección legal contra la extorsión digital ha sido un desafío debido a la evolución rápida de la tecnología y la adaptación lenta de las leyes. No obstante, el país ha tomado medidas significativas para abordar este problema. Ya existen oficinas encargadas específicamente del tema del ciberdelito en Instituciones como el Ministerio de Gobernación, el Ministerio Público y la Secretaría contra la Violencia Sexual, Explotación y Trata de Personas.

La Ley de Delitos Informáticos y Tecnológicos, aprobada en 2017, es uno de los instrumentos clave para enfrentar los delitos cibernéticos, incluida la extorsión digital. Esta ley define y penaliza diversos tipos de delitos informáticos, estableciendo marcos legales para la persecución y sanción de estos actos (García, 2019, p. 78)

Esta ley tipifica el acceso no autorizado a sistemas informáticos y la utilización indebida de datos como delitos, lo que proporciona una base para abordar casos de extorsión en línea. Esto representa un avance para la persecución penal de este tipo de acciones ilegales cometidas desde plataformas digitales.

Además, el Código Penal de Guatemala ha sido modificado para incluir delitos relacionados con el uso indebido de tecnología. En particular, el artículo 292-B del Código Penal establece sanciones para aquellos que cometen chantajes o extorsiones utilizando medios electrónicos (Rivas, 2021, p. 112) Esto incluye penas de prisión y multas que varían dependiendo de la gravedad del delito. En este punto lo que hace falta es una mayor difusión a nivel nacional de la existencia de estas leyes.

A pesar de estos avances legales, la implementación y aplicación efectiva de las leyes contra la extorsión digital en Guatemala enfrenta varios desafíos. La falta de recursos especializados y la capacitación insuficiente para las fuerzas de seguridad y el poder judicial pueden limitar la capacidad para investigar y procesar estos delitos de manera eficaz (Méndez, 2023, p. 66)

En este sentido hay que explorar estrategias como la cooperación internacional y el fortalecimiento de las capacidades locales con el propósito de mejorar la respuesta del sistema legal a la extorsión por medios digitales.

La extorsión por medios digitales representa un reto significativo en la era moderna, con implicaciones serias para la privacidad y la seguridad de las personas. En Guatemala, la legislación ha hecho avances para enfrentar este problema a través de leyes específicas y modificaciones al Código Penal. Sin embargo, la efectividad de estas medidas depende de la adecuada implementación y el fortalecimiento de las capacidades legales y técnicas para combatir la extorsión digital.

A medida que la tecnología continúa avanzando, es crucial que las leyes y políticas evolucionen para proteger a las víctimas y asegurar que los responsables sean llevados ante la justicia.

2.2.2. Seducción y chantaje sexual por medios digitales

El avance de las tecnologías digitales de la comunicación ha transformado múltiples aspectos de las relaciones sociales, incluyendo las dinámicas de poder y control en las relaciones íntimas. En la actualidad la seducción y el chantaje sexual se manifiestan también a través de medios digitales, utilizando mecanismos sofisticados que tienen implicaciones legales y psicológicas.

La proliferación de plataformas digitales ha facilitado nuevas formas de interacción, pero también ha dado lugar a prácticas problemáticas como la seducción y el chantaje sexual. La seducción digital implica la manipulación emocional y sexual a través de medios electrónicos, mientras que el chantaje sexual se refiere a la amenaza de divulgar material íntimo con el objetivo de coaccionar a la víctima. Ambos fenómenos han sido objeto de estudio en campos como la psicología, la criminología y el derecho.

La seducción digital se refiere al uso de plataformas como redes sociales, aplicaciones de mensajería y sitios web para fomentar la atracción sexual. De acuerdo con Papageorgiou et al. (2020), la seducción digital puede implicar la creación de perfiles falsos y la manipulación de la información personal para atraer y engañar a la víctima (p. 175). Este tipo de interacción a menudo explota la vulnerabilidad emocional de las personas y puede tener consecuencias duraderas en su bienestar psicológico.

Por otro lado, la seducción digital puede estar ligada a prácticas como el grooming, que se define como el proceso de establecer una relación de confianza con una persona para explotarla posteriormente (Wolak, Mitchell, & Finkelhor, 2012, p.220) Los perpetradores utilizan técnicas manipulativas para ganarse la confianza de la víctima antes de intentar explotarla sexualmente.

El chantaje sexual, también conocido como "sextortion", implica la amenaza de divulgar material sexual comprometedor a cambio de favores sexuales o dinero (Kroft & Hout, 2019, p. 98) Esta práctica se ha convertido en un problema creciente debido a la facilidad con la que se puede compartir información en línea. De acuerdo con (Garza, (2021)), el chantaje sexual digital puede

tener efectos devastadores en las víctimas, incluyendo depresión, ansiedad y pérdida de autoestima (p. 142).

Los perpetradores de chantaje sexual suelen aprovechar la confianza que la víctima ha depositado en ellos, a menudo estableciendo una relación íntima que se utiliza como base para la amenaza. La investigación de (Klein et al., 2023) indica que el chantaje sexual digital a menudo se lleva a cabo mediante la manipulación de imágenes y videos privados que han sido obtenidos sin el consentimiento de la víctima (p. 67).

Estos abusos descritos anteriormente tienen implicaciones que van desde lo legal hasta los efectos psicológicos que causan. El chantaje sexual y la seducción digital presentan desafíos significativos. Las leyes sobre delitos informáticos y protección de datos varían ampliamente entre las distintas jurisdicciones de los Estados, lo que puede complicar la persecución de estos crímenes. Según (Martínez, 2022) aunque muchos países han comenzado a legislar contra el chantaje sexual digital, la aplicación de estas leyes a menudo enfrenta obstáculos debido a la naturaleza transnacional del ciberespacio (p. 115).

Psicológicamente, las víctimas de seducción y chantaje sexual digital a menudo experimentan un trauma considerable. La investigación de (Smith y Thomas, 2021) destaca que las consecuencias emocionales de estos actos pueden ser graves y duraderas, afectando la salud mental y el bienestar general de las personas involucradas (p. 89).

En definitiva, la seducción y el chantaje sexual a través de medios digitales representan fenómenos complejos que requieren una atención interdisciplinaria por parte de autoridades nacionales e internacionales. Las respuestas institucionales y legales deben evolucionar para abordar adecuadamente estos problemas, y es de suma importancia que se ofrezca apoyo integral a las víctimas. La investigación en este tema juega un papel importantísimo y debe ser permanente el desarrollo de estrategias efectivas para la prevención y la intervención para mitigar el impacto de estos delitos.

2.2.3. Robo de datos financieros, fraude y extorsión digital

En la era digital que se está viviendo en todo el mundo, el robo de datos financieros, el fraude y la extorsión digital han emergido como amenazas significativas que afectan tanto a individuos como a organizaciones.

Se propone a continuación las definiciones de estos conceptos, también se describe de manera sucinta la situación actual en términos de incidencia y prevalencia, y las implicaciones que conllevan para las víctimas y para el sistema financiero global. Se abordan los mecanismos de ataque, las respuestas institucionales y las estrategias de mitigación.

En lo que respecta al robo de datos financieros se refiere al acceso no autorizado a información económica sensible, como números de tarjetas de crédito, cuentas bancarias y datos de transacciones. Según (Anderson et al., 2019) este tipo de robo generalmente implica la infiltración en sistemas de seguridad para obtener información que puede ser utilizada para realizar transacciones fraudulentas o para venderla en mercados clandestinos (p. 57).

Durante las primeras dos décadas del presente siglo este tipo de ciberdelito a proliferado a nivel global poniendo en riesgo la seguridad industrial, comercial y los mercados financieros. Diversas empresas y firmas nacionales e internacionales han tenido que ocupar una parte de su presupuesto para invertirlo en ciberseguridad para evitar ser víctimas de este ciberdelito.

En el tema del fraude digital este se define como la manipulación o falsificación de datos electrónicos con el objetivo de obtener beneficios ilícitos. Esto incluye, pero no se limita a, técnicas como el phishing, donde los delincuentes engañan a las víctimas para que proporcionen información confidencial a través de comunicaciones falsas (Carter & Hughes, 2020, p. 112) El fraude digital puede manifestarse en diversas formas, como estafas en línea, fraudes en e-commerce y suplantación de identidad.

Esto quiere decir que cualquier actividad realizada desde plataformas digitales que tenga como fin el engaño, difundir información falsa, difundir información confidencial o manipular ilícitamente la buena fe de las personas, Organizaciones o Empresas se considera como fraude digital.

Ahora bien, la extorsión digital, también conocida como ransomware, implica la utilización de malware para cifrar los datos de la víctima y exigir un rescate para su liberación (Lechner & Schuler, 2021, p. 89). Este tipo de ataque suele dirigirse tanto a individuos como a organizaciones, y puede tener un impacto devastador en la operatividad y la seguridad de los datos de las víctimas.

En la actualidad el panorama del robo de datos financieros, el fraude y la extorsión digital ha evolucionado significativamente en la última década. Según el Informe de Amenazas

Cibernéticas de 2023 de la firma de seguridad informática Symantec, "…el robo de datos financieros ha aumentado un 30% en los últimos dos años, con técnicas de phishing y malware avanzadas que se han vuelto más sofisticadas" (Symantec, 2023, p. 42)

En lo que se refiere al fraude digital, el Centro de Quejas de Delitos en Internet (IC3) reporta un incremento del 25% en los casos de fraude en línea en 2023, con un costo total para las víctimas estimado en más de 3.5 mil millones de dólares (IC3, 2023, p. 74).

Se debe tener presente que las tácticas y modalidades de fraude están en constante evolución, cada vez se tornan más sutiles y casi imperceptibles a la mirada de las personas que son sorprendidas en su buena fe aprovechando las vulnerabilidades que aparecen en las nuevas tecnologías y plataformas.

La extorsión digital también ha mostrado un aumento alarmante. El reporte de Ciberseguridad Global 2023 de McAfee revela que "…los ataques de ransomware crecieron un 40% en el último año, con un impacto económico global de aproximadamente 20 mil millones de dólares" (McAfee, 2023, p.56)

Como es de esperarse los ataques en mención se han vuelto más agresivos a medida que avanza la tecnología, también hay que referir que los demandantes exigen rescates cada vez mayores y utilizan técnicas de doble extorsión que implican la amenaza de divulgar los datos robados.

Por supuesto este tipo de ciberdelitos tiene sus implicaciones que son profundas y abarcan varios campos, a saber: En el campo económico el impacto de estos ciberdelitos es bastante considerable.

Los costos directos incluyen las pérdidas financieras por transacciones fraudulentas y el pago de rescates en el caso de ransomware. Además, los costos indirectos pueden ser aún mayores, incluyendo gastos en recuperación de datos, mejora de la seguridad y daños a la reputación (Smith, 2022, p. 135)

Las pérdidas financieras pueden llegar a significar cantidades millonarias dinero, lo que puede llevar a una entidad bancaria, financiera o comercial a la banca rota y con ello arrastrar a miles o millones de personas a la inseguridad personal en el caso de robo de bancos de datos, cuentas bancarias, o información de mercados de inversión como bolsas de valores.

Otra implicación importante se da en la esfera de la vida privada de las personas. Las víctimas de robo de datos financieros y fraude digital suelen enfrentar graves violaciones de privacidad.

"La exposición de información confidencial puede llevar a la suplantación de identidad y a un uso indebido de datos personales" (Harris & Wlker, 2021, p. 78)

Es evidente que un ciberataque que tenga como consecuencia la pérdida de privacidad puede tener efectos duraderos en la confianza de los consumidores y en la seguridad personal promoviendo un ambiente de inestabilidad institucional, social y a nivel familiar de las víctimas.

Ante estos escenarios de amenazas desde la virtualidad las instituciones financieras y los organismos de seguridad están respondiendo a estas amenazas con medidas como la implementación de tecnologías de detección de fraudes y la promoción de educación sobre ciberseguridad. Sin embargo, la rapidez con la que evolucionan las amenazas digitales plantea un desafío continuo para mantener la eficacia de estas medidas (Johnson, 2023, p. 94)

El robo de datos financieros, el fraude y la extorsión digital representan una amenaza creciente en el entorno digital actual. Las implicaciones económicas y personales son significativas, y las respuestas institucionales deben adaptarse constantemente para abordar estos desafíos.

La prevención y la educación son esenciales para mitigar el impacto de estos delitos y proteger tanto a individuos como a organizaciones en un mundo cada vez más digitalizado.

2.2.4 Venta de información personal o corporativa

Otro tipo de actividad ilícita cometida desde la virtualidad es la venta de información personal o corporativa es un tema cada vez más relevante en una sociedad en la que la privacidad se ve constantemente amenazada. Según la definición de la Comisión Federal de Comercio de los Estados Unidos (FTC, por sus siglas en inglés), la venta de información personal se refiere a "la transferencia de datos personales identificables por parte de una empresa u organización a otra empresa u organización a cambio de dinero u otra consideración". (FTC, s.f.)

En un mundo en el que la información es considerada un activo valioso para las empresas, la venta de información personal se ha convertido en una práctica cada vez más común. Desde los datos personales de los consumidores, hasta los secretos comerciales de una empresa, la información se está convirtiendo en una mercancía que se puede comprar y vender en el mercado.

Esta práctica no solo pone en peligro la privacidad de las personas, sino que también puede tener graves consecuencias para la seguridad de las empresas. Según un informe de la consultora Gartner, "la venta de información corporativa es una de las principales causas de filtraciones de datos en las empresas". (Gartner, 2017) Además, los efectos de la venta de información personal y corporativa pueden ser aún más preocupantes cuando se analizan desde una perspectiva social. De acuerdo con una investigación realizada por la American Civil Liberties Union (ACLU), (…) la venta de información personal puede perpetuar la discriminación y el prejuicio en una sociedad. Cuando la información personal de las personas se vende sin consentimiento, se les niega el control sobre su propia información, lo que puede llevar a la discriminación en áreas como la vivienda, el empleo y la educación". (ACLU, s.f).

En este orden de ideas, es preciso subrayar que la venta de información personal y corporativa se realiza en un marco jurídico complicado, en el que los límites de la seguridad personal, privacidad y la protección de datos son cada vez más difusos.

De acuerdo con Daniel Solove, profesor de derecho en la Universidad de George Washington, "la venta de información personal es un reflejo de la complejidad de la ley de privacidad, que ha evolucionado a lo largo de los años y ha tenido dificultades para mantenerse al día con la tecnología y las prácticas comerciales (Solove, 2013 s.n.)

En estos tiempos de vertiginosos avances en la tecnología de las comunicaciones se debe tener siempre presente que la venta de información personal y corporativa se ha convertido en un tema controvertido que pone en peligro la privacidad de las personas y la seguridad de las empresas.

Asimismo, esta práctica también puede perpetuar la discriminación y el prejuicio en la sociedad. En un marco legal cada vez más complejo, es necesario seguir analizando y debatiendo sobre esta cuestión para encontrar soluciones justas y equitativas que respeten la privacidad y los derechos de las personas.

2.2.5. Violencia digital y acoso sexual

Los dos últimos tipos de ciberdelitos que se describirán en esta investigación son la violencia digital y el acoso sexual. El primero es un tema que se ha extendido de ambientes presenciales como el hogar y el trabajo a plataformas virtuales en donde ha proliferado con mucha facilidad en esta era de la tecnología y las comunicaciones digitales avanzadas. En cuanto al acoso

sexual por medios digitales ha tenido implicaciones de tanto impacto y espectro que incluso se ha filtrado a lo más íntimo de los hogares, centros de estudio y de trabajo.

Algunas definiciones respaldadas por fuentes confiables permiten visualizar de mejor manera estos ilícitos de la violencia digital y el acoso sexual, es por ello que se presentan a continuación.

En primer lugar, se presenta una definición lata sensu de violencia digital para lo cual se hace referencia del autor (Marina, 2020, p. 45) según el cual este tipo de violencia digital se comete cuanto se utilizan plataformas digitales para realizar agresiones psicológicas que pueden tener implicaciones físicas a las víctimas, generalmente se utilizan ordenadores y la internet.

Este autor hace énfasis en el carácter multifacético de la violencia digital, debido a que se manifiesta de diferentes formas, estilos, niveles de gravedad, intensidad causando diferentes niveles de impacto, daños y efectos.

En el contexto de género hablando de la violencia Digital hay autores como (Guerrero, 2019, p. 77) que aborda la violencia digital definiéndola como todo hecho de violencia de género llevado a cabo a través de medios digitales, incluyendo el engaño, el acoso, las amenazas, y la divulgación no autorizada de información íntima.

Esta definición enfatiza cómo las dinámicas de poder y control se manifiestan en el entorno digital, afectando particularmente a las mujeres en lo que se refiere a violencia de género. En este tema hay millones de mujeres en Guatemala, en América Latina y en el mundo entero que son víctimas de este flagelo. No obstante, la violencia digital de género también encuentra campo fértil en otros grupos sociales vulnerables como niñez, población indígena, grupo LGTBI+, tercera edad, entre otros.

En Guatemala, la violencia contra la mujer es el delito denunciado número uno con 52.447 denuncias en 2022, 197 por día y 532 feminicidios; sin embargo, solo se resolvió el 20 por ciento de las denuncias de VRG presentadas ese año. Los hombres son los principales perpetradores de la violencia de género en Guatemala. La evidencia indica que las causas fundamentales de la violencia de género se pueden reducir a dos cosas: la desigualdad de género y los aspectos violentos, dañinos y controladores de las masculinidades que son el resultado de los desequilibrios de poder patriarcales. (USAID, 2004, parr.2)

De acuerdo con (Guerrero, 2919, p. 112) otro campo en el que se puede identificar violencia digital es la educación manifestándose como conductas hostiles realizadas a través de plataformas digitales que afectan el bienestar emocional y psicológico de las/os estudiantes, tales como el ciberacoso y el bullying en línea.

Esta definición resalta el impacto de la violencia digital en el ambiente escolar y educativo manifestándose como una amenaza a la dignidad humana, la intimidad y la vida privada de los(as) estudiantes.

La violencia digital en el ámbito escolar en Guatemala se ha convertido en una preocupación que cada día va en aumento, dado el surgimiento del uso de tecnologías digitales por parte de estudiantes, docentes y familias.

Hablando específicamente de Guatemala, la tecnología digital ha comenzado a jugar un rol importante en la educación, con la implementación de plataformas educativas en línea, redes sociales para la comunicación escolar, y el uso de dispositivos electrónicos en el aula. Sin embargo, esta integración también ha traído desafíos, especialmente en términos de violencia digital.

Existen diferentes tipos de violencia digital en el ámbito escolar entre los más relevantes se encuentran el Ciberacoso. En este tema se identifica que los(as) estudiantes pueden ser acosados, humillados o amenazados a través de mensajes en redes sociales, aplicaciones de mensajería y plataformas de comunicación en línea. El ciberacoso puede ser persistente y difícil de controlar, afectando la autoestima y el rendimiento académico de las víctimas. En Guatemala el problema se ha agudizado tanto que ya se lamentan pérdidas de vidas humanas por suicido debido a este tipo de violencia digital.

Otro tipo de violencia digital en el ámbito escolar es la exclusión digital llamada también marginación digital que ocurre cuando algunos estudiantes son deliberadamente excluidos de grupos en línea, foros o actividades escolares digitales, lo que puede generar sentimientos de aislamiento y afectar la dinámica social en el entorno escolar; influyendo además en el rendimiento académico de las víctimas.

Un tema que se ha agudizado en los últimos tiempos es difusión de contenidos Inapropiados. En efecto la distribución de imágenes o mensajes ofensivos, amenazas, y rumores puede ocurrir a través de las plataformas digitales utilizadas en el ámbito escolar. Esto puede tener

un impacto negativo en el ambiente escolar y en la relación entre estudiantes, alcanzando incluso el ambiente familiar.

Como ya se ha señalado en párrafos anteriores la Violencia de Género en el ámbito digital es otro problema tenaz. En algunos casos, las niñas y mujeres jóvenes pueden enfrentar violencia de género en línea, que incluye acoso sexual y la difusión no consensuada de imágenes íntimas. Esto refleja y perpetúa las desigualdades de género presentes en la sociedad guatemalteca.

Basta con acudir a los medios de comunicación nacionales para encontrar casos como los del Colegio Continental Americano (2024) en el que alumnas fueron agredidas por sus compañeros de clase poniendo sus rostros en cuerpos desnudos de otras mujeres y publicándolos en una plataforma digital. Sin lugar a duda estos son ilícitos graves que dañan la dignidad, honra y reputación de las víctimas que posiblemente nunca se recuperen al cien por ciento del daño psicológico que les causaron.

Existen factores que contribuyen a la comisión de este tipo de ilícitos en los ámbitos digitales como la falta de educación digital. Muchos estudiantes, padres y docentes carecen de la educación adecuada sobre el uso seguro y responsable de la tecnología. Esto está dando como resultado la falta de conciencia sobre las consecuencias del comportamiento digital y denota la falta de estrategias para prevenir y abordar la violencia digital no solo en ámbitos escolares sino a nivel general.

Otro factor determinante es la Insuficiente capacitación para docentes en referencia a la ética para el uso de espacios virtuales. En efecto el incremento de casos puede encontrar una de sus causas en el hecho que los(as) docentes pueden no estar suficientemente capacitados para reconocer y manejar situaciones de violencia digital. La capacitación en manejo de conflictos digitales y en herramientas de regulación es esencial para que puedan apoyar a los estudiantes de manera efectiva.

La falta de procedimientos de supervisión adecuada de las interacciones digitales entre estudiantes puede permitir que el acoso y otras formas de violencia digital pasen desapercibidos o no sean tratados de manera oportuna.

Impacto en los Estudiantes

Uno de los impactos difíciles de detectar es el psicológico. Los estudiantes que son víctimas de violencia digital pueden experimentar estrés, ansiedad, depresión, y baja autoestima, lo que

puede afectar su rendimiento académico y su bienestar general hasta conducirlos a decisiones extremas como el suicidio.

En lo social la violencia digital puede afectar la dinámica social dentro del entorno escolar, creando divisiones y conflictos entre estudiantes y dificultando la formación de relaciones positivas y de apoyo. También en el ámbito familiar se ve afectada la integración, la seguridad personal y la dignidad de sus diferentes integrantes. Citar algún caso de algún departamento de psicología.

En el campo académico los estudiantes víctimas de violencia digital pueden ver afectado su rendimiento académico debido a la distracción, la falta de concentración y el impacto emocional que sufren.

La violencia digital en el ámbito escolar en Guatemala es un problema que requiere atención y acción concertada e inmediata. La educación, la capacitación, la implementación de políticas adecuadas y el apoyo a los estudiantes son esenciales para crear un entorno escolar seguro y positivo. Abordar estos problemas de manera integral puede ayudar a proteger a los estudiantes y a fomentar un uso saludable y constructivo de la tecnología en el entorno educativo.

Aspectos Legales de la Violencia Digital

De acuerdo con destaca la dimensión legal de la violencia digital al definirla como "acciones digitales que constituyen delitos bajo la legislación vigente, tales como el acoso en línea, el robo de identidad, y la difusión de contenido ilícito" (Bermúdez, 2018, p. 60) Esta definición aclara cómo la violencia digital puede ser abordada desde una perspectiva jurídica.

Es más, existe la urgente necesidad esta violencia ya que cada día se hace más fácil e inmediata la forma de delinquir defraudar la buena fe de las personas. Si los delitos que se cometen de forma presencial son sancionados de forma tardía los que se cometen en el ciberespacio pueden tardar aún más.

Otra definición interesante es "(…) es el uso de plataformas digitales para causar daño psicológico, emocional o físico a una persona, donde el impacto negativo en el bienestar mental del individuo puede ser profundo y duradero" (Rodríguez, p.98)

Esta definición pone énfasis en el efecto duradero de la violencia digital sobre la salud mental de las víctimas que puede durar hasta el final de su vida.

Estas definiciones ofrecen una visión integral de la violencia digital desde diferentes perspectivas y contextos, proporcionando una base sólida para su estudio y comprensión en el ámbito académico.

Acoso sexual

El acoso sexual digital es un tema relevante en la era de la tecnología y las comunicaciones. Permíteme proporcionarte información sobre este fenómeno, junto con algunas citas APA para respaldar lo que compartiremos.

Definición del acoso sexual digital

El acoso sexual digital se refiere a comportamientos no deseados de naturaleza sexual que ocurren en línea. Estos pueden incluir:

Sexting no consensuado

Enviar mensajes, fotos o videos sexualmente explícitos sin el consentimiento de la persona.

Ciberacoso sexual

Utilizar redes sociales, correos electrónicos u otras plataformas digitales para acosar sexualmente a alguien.

Online grooming

Este término se refiere específicamente al abuso sexual a través de internet, donde los agresores manipulan y establecen una relación con menores con fines sexuales.

Análisis actual

En España, el ciberacoso afecta especialmente a los menores. El país se encuentra en séptimo lugar en el ranking mundial de niños de 13 años que han recibido amenazas o insultos a través de WhatsApp o redes sociales.

Además, se ha desarrollado una Escala de acoso sexual e interacción social de contenido sexual en el ámbito universitario (EASIS-U). Esta escala evalúa comportamientos de chantaje sexual, acoso sexual verbal y físico, así como interacción social de contenido sexual en el contexto académico.

2.3. Prevención del ciberdelito

El ciberdelito ha emergido como una amenaza significativa en el siglo XXI, impulsado por el crecimiento exponencial de las tecnologías digitales y la conectividad global. Estos delitos no solo comprometen la seguridad de individuos y organizaciones, sino que también pueden tener efectos perjudiciales a nivel social y económico.

Combatir el ciberdelito requiere una estrategia integral que combine prevención, detección, respuesta y educación. Este escrito explora las características del ciberdelito y propone enfoques efectivos para su mitigación, respaldado por referencias académicas y de expertos en la materia.

2.3.1. Características del Ciberdelito

Formas del ciberdelito

Acceso No Autorizado a Sistemas

Involucra la intrusión en sistemas informáticos para robar o manipular datos (Clarke, 2018).

Fraude Electrónico

Incluye el phishing, el fraude con tarjetas de crédito y el robo de identidad (Ponemon Institute, 2021).

Ciberacoso

Acoso o intimidación a través de plataformas digitales, con efectos negativos en la salud mental de las víctimas (Smith et al., 2022).

Ataques a Infraestructuras Críticas: Involucra la interrupción o sabotaje de servicios esenciales como la energía o las comunicaciones (Davis & Shneier, 2023).

Espionaje Cibernético: Obtención de información confidencial o clasificada a través de medios digitales (Rouse, 2022).

Estrategias para Combatir el Ciberdelito

La prevención es el primer paso para combatir el ciberdelito. La educación de los usuarios sobre prácticas seguras en línea puede reducir significativamente el riesgo de ataques.

Los programas de formación deben incluir la identificación de correos electrónicos de phishing, la creación de contraseñas seguras y la protección de información personal (Reddy et al, 2022). Además, las campañas de concienciación pública pueden ayudar a sensibilizar a la población sobre los peligros y las mejores prácticas de seguridad en línea.

Implementación de Tecnologías de Seguridad Avanzadas

"La adopción de tecnologías avanzadas es crucial para proteger los sistemas contra ataques. Esto incluye el uso de software antivirus actualizado, firewalls, y sistemas de detección y prevención de intrusiones" (Cunningham & Kent, 2021) "La implementación de tecnologías de autenticación multifactorial también puede mejorar significativamente la seguridad de las cuentas y sistemas sensibles" (Kirkpatrick, 2020)

Estos autores señalan la importancia de tomar medidas que tomen en cuenta múltiples factores, procesos y elementos. Sería bueno que el gobierno realice proyectos con cooperación internacional para la adquisición de equipo y programas que busquen soluciones para una mejor regulación del uso de redes digitales.

En este sentido se puede acudir a la cooperación sur-sur y no solo a la norte-sur porque podría haber mayor identificación entre países con características que se pueden identificar entre sí.

Desarrollo de Políticas y Legislaciones Efectivas

Las leyes y regulaciones deben evolucionar para abordar las nuevas amenazas cibernéticas. La creación de marcos legales específicos para el ciberdelito, como la Ley de Protección de Información Personal en Línea para Niños (COPPA) y el Reglamento General de Protección de Datos (GDPR), son ejemplos de cómo las políticas pueden proteger la privacidad y la seguridad en línea (Solove & Schwartz, 2021)

Además, la cooperación internacional en la formulación de leyes y tratados es esencial para abordar el ciberdelito transnacional (Harris, 2022)

En este aspecto se debe recordar que una de las posibilidades para que una política sea efectiva es que permita la participación de diferentes sectores de la sociedad, así como expertos en el campo en el que se va a desarrollar la política.

Respuesta y Recuperación ante Incidentes

La capacidad de respuesta rápida a incidentes cibernéticos es crucial para minimizar el daño y recuperar la normalidad operativa. Las organizaciones deben desarrollar planes de respuesta a incidentes que incluyan la identificación y contención del ataque, la recuperación de datos y la comunicación con las partes afectadas (Kopp et al, 2022)

"La colaboración con equipos de respuesta a emergencias cibernéticas, como los equipos de respuesta a incidentes informáticos (CSIRT), puede mejorar la eficacia en la gestión de incidentes" (NIST, 2021)

El ciberdelito representa una amenaza creciente en el mundo digital, con consecuencias potencialmente graves para la seguridad individual y organizacional. Combatirlo requiere una estrategia multifacética que combine educación, tecnología, legislación y una respuesta eficiente ante incidentes. A medida que las tecnologías evolucionan, también deben hacerlo las estrategias para protegernos contra estos delitos, asegurando que el ciberespacio sea un entorno seguro y confiable para todos.

2.4 Marco jurídico nacional e internacional para la prevención del ciberdelito

La creciente digitalización de la sociedad ha traído consigo el aumento de ciberdelitos, que representan un desafío significativo para los sistemas legales tanto nacionales como internacionales. La prevención y combate de estos delitos requieren un marco jurídico robusto y actualizado que contemple las peculiaridades del entorno digital. Este ensayo examina el marco jurídico nacional e internacional para la prevención del ciberdelito, destacando los esfuerzos realizados para armonizar las legislaciones y la importancia de la cooperación internacional.

2.4.1 Marco Jurídico Internacional

A nivel internacional, la comunidad global ha desarrollado diversos instrumentos legales para enfrentar el ciberdelito. Uno de los documentos más relevantes es el Convenio de Budapest sobre Ciberdelincuencia, adoptado en 2001 por el Consejo de Europa. Este convenio es el primer tratado internacional diseñado para abordar los delitos cometidos a través de Internet y otras redes informáticas (Council of Europe, 2001, p.5) Su objetivo principal es facilitar la cooperación internacional y la armonización de leyes nacionales, estableciendo normas mínimas para la criminalización de ciertos actos de ciberdelincuencia.

"El Convenio de Budapest cubre una variedad de delitos, incluidos el acceso no autorizado a sistemas informáticos, la interferencia en sistemas y datos, y el contenido ilegal" (Council of Europe, 2001, p.5) Asimismo, promueve medidas de cooperación y asistencia mutua entre las partes contratantes, lo que resulta esencial para enfrentar el ciberdelito que trasciende fronteras.

Otro instrumento clave es la Resolución de la ONU sobre la Ciberdelincuencia y la Seguridad de la Información, que subraya la necesidad de una estrategia integral para la lucha contra el ciberdelito y promueve la cooperación internacional (United Nations, 2013, p. 12) Esta resolución destaca la importancia de compartir información y mejores prácticas entre los países para mejorar la respuesta global ante las amenazas cibernéticas.

2.4.2 Marco Jurídico Nacional

En el ámbito nacional, muchos países han implementado leyes específicas para abordar el ciberdelito. En Estados Unidos, la Ley de Fraude y Abuso en Computadoras (Computer Fraud and Abuse Act, CFAA) es una de las legislaciones más relevantes. Esta ley penaliza el acceso no autorizado a sistemas informáticos y el daño a datos (United States Code, 2023, p. 3) Aunque el CFAA ha sido fundamental en la lucha contra el ciberdelito en EE.UU., también ha sido objeto de críticas por su amplitud y la necesidad de reformas para adaptarse a la evolución de las tecnologías.

En la Unión Europea, el Reglamento General de Protección de Datos (GDPR) es fundamental para la protección de datos personales en el contexto digital. Aunque su enfoque principal es la privacidad y protección de datos, el GDPR también tiene implicaciones significativas para la prevención del ciberdelito al imponer obligaciones estrictas sobre el manejo de datos y la notificación de brechas de seguridad (European Union, 2016, p. 15)

En América Latina, países como México han adoptado la Ley de Delitos Informáticos, que aborda delitos cibernéticos específicos y establece mecanismos para la cooperación con otras naciones (Gobierno de México, 2019, p. 22) Sin embargo, la implementación efectiva y la actualización continua de estas leyes siguen siendo un desafío.

2.4.3 Desafíos y Perspectivas Futuras

A pesar de los avances en la legislación internacional y nacional, la prevención del ciberdelito enfrenta varios desafíos. La rápida evolución de la tecnología a menudo supera la

capacidad de los marcos legales para adaptarse, lo que puede dejar lagunas en la protección jurídica (Higgins, 2022, p. 30)

"También, la cooperación internacional es crucial, pero a menudo complicada por diferencias en las leyes y procedimientos entre países" (Smith, 2021, p. 45)

Para abordar estos desafíos, es esencial fomentar la cooperación y el intercambio de información entre las jurisdicciones, así como actualizar periódicamente las leyes para reflejar los desarrollos tecnológicos. La capacitación permanente de los profesionales en el ámbito de la ciberseguridad y la implementación de mejores prácticas también juegan un papel vital en la prevención del ciberdelito

El marco jurídico para la prevención del ciberdelito, tanto a nivel nacional como internacional, ha avanzado significativamente, pero aún enfrenta varios desafíos. Instrumentos internacionales como el Convenio de Budapest y resoluciones de la ONU (2004) han establecido una base sólida para la cooperación y armonización de leyes.

A nivel nacional, las legislaciones específicas y regulaciones como el GDPR han contribuido a la protección en el entorno digital. Sin embargo, es crucial seguir adaptando y fortaleciendo estos marcos legales para enfrentar la evolución constante de las amenazas cibernéticas.

Capítulo III. El Trabajo Social y el Ciberdelito en Guatemala

En vista de la importancia y lo determinante que son los temas que se han venido tratando acerca del ciberespacio se deben buscar estrategias para la prevención de riesgos que como el ciberdelito pueden afectar a las personas incluso dentro de su mismo hogar ya que como se señaló en párrafos anteriores el ciberespacio está en todas partes en donde se encuentre un ordenador informático.

Es así como se ubica al Trabajo Social como una estrategia profesional de singular importancia en la promoción y defensa de los derechos de las personas y comunidades que puedan ser transgredidos desde esta nueva dimensión que representa el ciberespacio.

Interpretando a diferentes autores que definen el Trabajo Social se pueden notar acercamientos en el trabajo comunitario que se debe realizar para la consecución del bien común que incluye propiciar un ambiente libre de amenazas a la seguridad humana que comprende por supuesto amenazas como el ciberdelito.

De esta forma se puede ir identificando posibles espacios en los que se pueda vincular el tema de prevención del ciberdelito. Dentro de los autores destacados se encuentran:

(Richmond, 1922, s.n.) Quien indica que el conjunto de métodos que desarrollan la personalidad reajustando consciente e individualmente a la persona a su medio social. El logro de esta adaptación exige al trabajador social al menos la compresión de ambas cosas, la persona y el medio, ello implica el uso de técnicas adecuadas para poder producir un cambio en esa situación. También dice que implica una política en esa forma de actuar: el apoyo como método de educación y hacer partícipe en esos cambios a la persona implicada.

En la anterior definición es posible encontrar espacios para inducir el conocimiento y prevención del ciberdelito cuando la autora Richmond menciona métodos para desarrollar la personalidad y así reajustar de forma consciente a la persona a su medio social. Acá se debe de inferir que el medio social se encuentra infiltrado por nuevas realidades emergentes dentro de las cuales se encuentra el ciberespacio y por ende el ciberdelito entonces, resulta congruente hacer la deducción que el Trabajo Social resulta estratégico para la prevención del ciberdelito.

En el primer Congreso Panamericano de Servicio Social de 1957 se destaca la definición siguiente:

> Profesión basada en el reconocimiento de la dignidad del ser humano y de su capacidad de superación, que mediante los procedimientos propios ayuda a los individuos, grupos y comunidades a valerse por sí mismos y lograr su desarrollo integral, especialmente en las situaciones sociales en que necesitan ayuda ajena para poder atender sus necesidades y desarrollar sus potencialidades. (Congreso, Panamericano de Trabajo Social, 1957, s.n.)

Esta definición del autor Aguilar Idañez también es susceptible de interpretar que cuenta con espacios temáticos que se pueden relacionar con el ciberdelito ya que el autor habla de dignidad humana, atención de necesidades y desarrollo de potencialidades. Estos tres últimos temas tienen que ver con el ciberdelito si se toma en cuenta que éste atenta contra la dignidad humana, asimismo, la prevención de amenazas es una de las necesidades que necesitan especial atención en los diferentes grupos sociales y por último el desarrollo de potencialidades puede comprender la generación de capacidades para defenderse frente al ciberdelito.

En el año 1959 la Organización de las Naciones Unidas define el Trabajo Social de la siguiente manera:

> El servicio social es una actividad organizada cuyo objetivo es contribuir a una adaptación mutua entre las personas y su medio social, ésta adaptación mutua entre las personas y su medio social, esta adaptación se logra mediante el empleo de técnicas y métodos destinados a que los individuos, grupos o comunidades puedan satisfacer sus necesidades y resolver sus problemas de adaptación a un tipo de sociedad que se haya en proceso de evolución, así como por medio de una acción cooperativa para mejorar las condiciones económicas y sociales. (Naciones Unidas, 1959, s.n.)

Definitivamente la definición que presenta la Organización de Naciones Unidas también contiene elementos teóricos que vinculan la prevención de amenazas como el ciberdelito con el Trabajo Social. Al mencionar la premisa contribuir a la adaptación mutua entre las personas y su medio social se puede inferir que esta adaptación incluye temas novedosos como el ciberespacio y ciberdelito.

También menciona técnicas y métodos para resolver problemas de adaptación a una sociedad en constante evolución como en la que actualmente viven las comunidades. Este último

enunciado se encuadra de buena manera en la línea de resolver la amenaza del ciberdelito por medio de métodos y técnicas de prevención.

3.1. Relación del Trabajo Social con el Ciberdelito

Después de analizar varias definiciones de Trabajo Social de diferentes autores y organizaciones es posible darse cuenta de la vinculación teórica y práctica que tiene esta disciplina social con diferentes campos del conocimiento humano.

De esta forma el Trabajo Social se convierte o puede convertirse en actor clave en temas como: derechos humanos, resolución de conflictos, discriminación, violencia contra la mujer, desarrollo humano, formulación, gerencia y evaluación de proyectos sociales, equipos multidisciplinarios en temas sociales, atención a privados de libertad, reinserción social de menores en conflictos con la ley, gestión de cooperación internacional para el desarrollo social, adopción, prevención del ciberdelito, entre otros.

La función del Trabajo Social es multifacética, holística, multifuncional, teórica, práctica y no riñe con las demás ciencias sociales. Esto hace que la disciplina se pueda adaptar a una serie de situaciones, temas, factores y realidades del campo social, tratando de promover el bienestar general en una sociedad democrática.

Por ello es posible afirmar su versatilidad de actuación que la convierte en una herramienta profesional de singular importancia para la mediación en tantos problemas que aquejan a la sociedad guatemalteca.

En este marco de referencia se puede encontrar un nicho de actuación del Trabajo Social para la Prevención del Ciberdelito en grupos sociales vulnerables en Guatemala. Hay que tener presente que hasta finales del siglo pasado no se había masificado el acceso a las redes sociales. Hace un par de décadas la mayoría de personas en el mundo no sabía qué significaban temas como: el ciberespacio, internet, cibernauta, redes sociales, cibercrimen, entre otros.

En la actualidad la mayoría de la población mundial encuentra un punto de encuentro en internet no importando en qué lugar del mundo se encuentre. Hoy por hoy una buena parte de la población mundial pasa su día conectado en el ciberespacio.

Esta es una nueva realidad mundial que jamás se pensó que fuera a dominar a los seres humanos. Por ejemplo, en varios países del primer mundo los servicios básicos son controlados

por inteligencia artificial. Diferentes universidades del planeta ya gestionan el conocimiento por medio de inteligencia artificial. Sistemas de armamentos nucleares de las superpotencias son controlados por inteligencia artificial. Restaurantes, bibliotecas, parques de diversión, sistemas de transporte aéreo y ferroviario utilizan programas computarizados para el desarrollo de sus actividades.

Esto hace que no solo la regulación de estas nuevas realidades sino más importante aún el pleno conocimiento de éstas no sea promovido en las poblaciones de todo el mundo, pero especialmente en poblaciones de países en vías de desarrollo como Guatemala en donde hay fuertes segmentos de la población viviendo en pobreza y extrema pobreza y que no tienen acceso a la educación menos al conocimiento de estos nuevos temas.

Lo delicado de esta situación es que es una realidad que la mayoría de la gente que vive en pobreza tiene acceso a un celular y por lo tanto acceso al ciberespacio en donde se ve expuesta a muchos riesgos de engaños y estafas entre otros. Es en este momento en donde se encuentra un rol preponderante del Trabajo Social mediando en las poblaciones para prevenirlos del ciberdelito y promover las formas que hay de combatirlo.

Esta nueva realidad si no se empieza gestionar socialmente de forma inmediata dentro de muy pocos años será una de las mayores amenazas del mundo porque una población que no conoce la realidad en que vive está expuesta a sufrir las consecuencias que van desde vivir engañada hasta sufrir disminuciones o pérdidas en sus derechos más elementales.

En la era digital que se está viviendo, los ciberdelitos se han convertido en una amenaza creciente que afecta a individuos, comunidades y organizaciones a nivel global. El trabajo social, como una disciplina enfocada en el bienestar social y la protección de los derechos humanos, tiene un papel crucial en la prevención y atención de las víctimas de estos delitos. En este acápite se analiza la intersección entre el trabajo social y el ciberdelito, explorando cómo los profesionales del trabajo social pueden colaborar en la prevención de estos delitos y en el apoyo a las personas afectadas. Asimismo, se examina la importancia de una formación interdisciplinaria que prepare a los trabajadores sociales para enfrentar los retos del ciberespacio.

Ahondando un poco más en este tema se puede observar que el ciberdelito abarca una amplia gama de actividades delictivas que se cometen a través de tecnologías digitales, incluyendo

fraudes, ciberacoso, suplantación de identidad y la distribución de material ilegal (Europol, 2021) Estas formas de delito pueden tener efectos devastadores en las víctimas, que van desde el daño emocional hasta el impacto financiero y la vulneración de la privacidad. Para los trabajadores sociales, este fenómeno plantea nuevos desafíos, ya que las personas afectadas por los ciberdelitos pueden necesitar asistencia en múltiples niveles: emocional, legal y social.

Como ya se ha mencionado el Trabajo Social se centra en la intervención y la promoción del bienestar de los individuos y comunidades vulnerables. En este sentido, los profesionales del Trabajo Social tienen la capacidad de intervenir tanto en la prevención como en la atención de las víctimas de ciberdelítos (Álvarez & Hernández, 2020) Desde una perspectiva preventiva, los trabajadores sociales pueden participar en programas educativos que fomenten el uso responsable de las tecnologías y la concientización sobre los riesgos del ciberespacio.

A nivel de intervención directa, los trabajadores sociales pueden apoyar a las víctimas de ciberdelitos proporcionando acompañamiento emocional y ayudándolas a acceder a servicios legales y psicológicos. También es fundamental su papel en la defensa de los derechos digitales, ayudando a las personas a recuperar el control de sus vidas tras un incidente cibernético (García & López, 2019, s.n.)

Para abordar eficazmente los ciberdelitos desde el trabajo social, es necesario adoptar un enfoque interdisciplinario. Los profesionales del trabajo social deben colaborar con expertos en ciberseguridad, abogados especializados en delitos digitales y psicólogos para ofrecer una respuesta integral a las víctimas (Sanchez & Rodríguez, 2021) Esta cooperación permite desarrollar estrategias más efectivas para prevenir los ciberdelitos y ofrecer a las víctimas el apoyo que necesitan para superar el impacto de estas actividades delictivas.

Además, la formación continua en el uso de tecnologías digitales y el entendimiento de los entornos virtuales es esencial para que los trabajadores sociales puedan desempeñar su papel de manera eficaz. El constante desarrollo de nuevas tecnologías y formas de ciberdelito requiere que los profesionales del Trabajo Social se mantengan actualizados sobre las amenazas y las mejores prácticas de intervención.

En síntesis, se puede inferir que el trabajo social juega un papel fundamental en la lucha contra el ciberdelito, tanto en términos de prevención como de atención a las víctimas. A través de

una formación interdisciplinaria y la colaboración con otros profesionales, los trabajadores sociales pueden ayudar a mitigar los efectos negativos de los ciberdelitos y proteger los derechos de las personas vulnerables en el ciberespacio.

El desafío que representa el ciberdelito requiere que los profesionales del trabajo social se adapten a las nuevas realidades digitales para continuar promoviendo el bienestar y la justicia social en un mundo cada vez más interconectado.

No hay que olvidar que el ciberdelito en Guatemala es un tema relevante que ha experimentado un aumento inesperado en los últimos años. “En el año 2021, las denuncias por ciberdelítos ante la Policía Nacional Civil pasaron de 6 500 casos en 2020 a 9 100 en 2021, lo que representa un incremento del 40 %” (Barreno Castillo, 2022, p. 1). En los primeros ocho meses de 2022 se registraron 3 500 denuncias de delitos a través de redes sociales, un aumento del 27 % respecto al mismo periodo de 2021 (Solórzano, 2022, p. 1)

No obstante haber hecho ya mención en esta parte del trabajo sobre las leyes que se relacionan con aspectos de la vida humana que pueden ser afectados por el ciberdelito es necesario insistir en aspectos como los siguientes:

3.2 Métodos y técnicas de Trabajo Social para la prevención del ciberdelito

En el mundo del siglo XXI amenazas como el ciberdelito han emergido como un desafío significativo para la seguridad y el bienestar de las personas.

Los avances de las ciencias y la tecnología de las comunicaciones han permitido la proliferación de diversas formas de delitos cibernéticos, tales como el fraude, el ciberacoso y el robo de identidad, que afectan tanto a individuos como a comunidades enteras (Interpol, 2020)En este contexto, el Trabajo Social debe adaptarse, integrando nuevas metodologías y técnicas para abordar estos desafíos desde una perspectiva de prevención. En este acápite se exploran los métodos y técnicas que pueden ser utilizados por los profesionales del trabajo social en la prevención del ciberdelito, destacando su importancia en la protección de los derechos digitales y el bienestar social.

3.2.1 Educación y Concientización Comunitaria

El método para prevenir el ciberdelito en Trabajo Social se apoya en varios autores importantes. (Álvarez Idarriaga, 2015) propone un enfoque integral que toma en cuenta la

educación, la familia y la comunidad, y además, plantea pasos bien definidos como la detección, la valoración, la planificación y la evaluación. Por otro lado, (Lopez Peláez, 2024) habla de la "vulnerabilidad digital" y señala la importancia de diseñar acciones comunitarias que reduzcan las brechas en acceso a la tecnología, en habilidades digitales y en confianza hacia las instituciones.

Es decir, estas propuestas construyen un método muy organizado, pero al mismo tiempo flexible, ya que la comunidad no solo recibe formación, sino que también se convierte en protagonista del cambio. Las etapas se pueden aplicar de la siguiente manera: diagnóstico, análisis, planificación, implementación y evaluación, estas ayudan a crear estrategias ajustadas a cada realidad, lo que fortalece la prevención del ciberdelito a través de la educación digital y el trabajo colectivo.

3.2.2. Trabajo en Redes Multidisciplinarias

Otro método que resultaría importante es la colaboración en redes multidisciplinarias que reúnen a profesionales de distintas áreas, como la ciberseguridad, el derecho y la psicología.

En este caso los trabajadores sociales actuarían como intermediarios entre las víctimas de ciberdelitos y los servicios de apoyo, facilitando el acceso a recursos legales y psicológicos necesarios para enfrentar el impacto del delito (Álvarez & Hernádez, 2021) Esta colaboración resultaría fundamental para desarrollar estrategias integrales de prevención que consideren las diversas dimensiones del ciberdelito, incluyendo las consecuencias emocionales y sociales que experimentan las víctimas.

3.2.3. Intervención para Políticas Públicas y Derechos Digitales

El trabajo social también desempeña un rol crucial en la mediación que resulta importante para el desarrollo de políticas públicas que protejan a las personas de los ciberdelitos. Los trabajadores sociales pueden colaborar con legisladores y activistas para promover leyes que aseguren la protección de los derechos digitales y el acceso a la justicia para las víctimas.

Según (García, 2019) la mediación y la abogacía en este campo debe buscar garantizar que los gobiernos implementen marcos regulatorios adecuados que penalicen los delitos en línea y ofrezcan mecanismos de apoyo para las víctimas. Además, la promoción de los derechos digitales es clave para reducir las desigualdades en el acceso a la tecnología y prevenir la exclusión digital,

lo que a menudo puede aumentar la vulnerabilidad frente a los ciberdelitos. También existen técnicas utilizadas por el Trabajo Social en la prevención del Ciberdelito.

3.2.4. Asesoramiento y Acompañamiento Psicosocial

Una técnica clave en el trabajo social es el asesoramiento y el acompañamiento psicosocial para víctimas de delitos dentro de lo cual deberían integrarse los ciberdelitos. Esta es una técnica que se pone en práctica desde que son estudiantes de trabajo social en los cursos de práctica individual y de grupos.

Los trabajadores sociales proporcionan apoyo emocional a quienes han sido afectados por delitos comunes y aquí es donde deben incorporarse los delitos en línea, ayudándoles a las víctimas a superar el trauma asociado con la pérdida de privacidad, el daño a la dignidad, honra y/o reputación o el abuso psicológico (Sánchez & Rodríguez, 2020) Este acompañamiento incluye la orientación sobre cómo restaurar la seguridad digital personal y acceder a servicios especializados en ciberseguridad o asesoría legal.

3.2.5. Intervención Familiar y Escolar

La intervención en el entorno familiar y escolar es otra técnica que puede resultar eficaz para prevenir el ciberdelito, especialmente en el caso de niños y adolescentes.

En el ejercicio profesional de los(as) trabajadores(as) sociales se pueden integrar acciones con padres y educadores para inducir un uso seguro y responsable de las tecnologías, estableciendo pautas claras para la navegación en Internet y la interacción en redes sociales (Rodríguez & Castillo, 2021) Además, se debe promover que los programas de intervención escolar estén diseñados para capacitar a los estudiantes en la identificación y denuncia de situaciones de riesgo en línea, como el ciberacoso o la manipulación digital.

3.2.6. Mediación en Conflictos

La mediación es una técnica utilizada en casos de conflictos generados en entornos comunitarios. Esta es otra técnica que puede integrarse de buena manera en conflictos digitales como disputas entre individuos involucrados en casos de ciberacoso o difamación en línea. Según (Fernández, 2018) la mediación busca restaurar las relaciones afectadas por estos conflictos y prevenir la escalada de conductas delictivas. Los trabajadores sociales actúan como facilitadores en estos procesos, promoviendo el diálogo y la resolución pacífica de los conflictos digitales.

En definitiva, el Trabajo Social puede desempeñar un papel fundamental en la prevención del ciberdelito, utilizando una combinación de métodos educativos, colaboración interdisciplinaria y mediación para fortalecer la protección de los derechos digitales y el bienestar social.

A través de técnicas como el asesoramiento psicosocial, la intervención familiar y la mediación, los trabajadores sociales pueden mitigar los efectos negativos del ciberdelito creando espacios de intervención familiar, este consiste en el acompañamiento adecuado a las familias para que desarrollen dinámicas de comunicación y protección ante riesgos digitales, y promover un entorno digital más seguro para todos. En un mundo cada vez más digitalizado, el Trabajo Social debe seguir adaptándose y desarrollando nuevas estrategias para enfrentar los retos emergentes del ciberespacio, a continuación, se mencionan algunas de las acciones que pueden ser aplicadas:

1. **Mediación digital:** consiste en facilitar espacios de diálogo para evitar que el conflicto escale a situaciones legales o delictivas.
2. **Educación preventiva:** organizar talleres, campañas sobre el uso responsable de redes y así loar la prevención de ciberdelitos.
3. **Trabajo interdisciplinario:** colaborar con psicólogos, abogados y especialistas en tecnología para elaborar planes integrales de intervención.
4. **Fortalecimiento en la comunidad:** Consiste en promover la creación de redes de apoyo en escuelas, barrios y colectivos digitales que refuercen la seguridad y la confianza en los entornos virtuales existente.

De esta manera el Trabajo Social atiende las consecuencias inmediatas que puedan existir por el ciberdelito, pero también aporta a la construcción de capacidades en comunidades para prevenir, enfrentar y superar los riesgos del mundo digital.

3.3. El ciberdelito en las redes sociales en Guatemala

Fenómenos como el ciberdelito y los ciberataques se han posicionado como una amenaza de singular relevancia en todo el mundo a medida que las tecnologías de la información y la comunicación (TIC) se integran en la vida cotidiana de los ciudadanos(as) del mundo.

En Guatemala, un país que ha experimentado un aumento significativo en el uso de redes sociales, las actividades criminales en línea se han diversificado y complejizado.

En este acápite se describe el panorama del ciberdelito en las redes sociales en Guatemala, identificando los delitos más comunes, los grupos sociales más afectados y las plataformas más vulnerables a estas amenazas. A través de esta descripción, se pretende proporcionar una visión integral de un fenómeno que afecta tanto a la seguridad digital como a la cohesión social en el país.

Los tipos de Ciberdelítos más comunes en Guatemala y que han proliferado en diversas formas en las redes sociales son:

3.3.1. Estafas en línea (fraude digital)

Las estafas en línea, donde los delincuentes se hacen pasar por instituciones legítimas o personas confiables, son frecuentes en las redes sociales. Utilizan tácticas de ingeniería social para engañar a las víctimas y robarles información financiera o dinero directamente. Esto se ve particularmente en plataformas como Facebook e Instagram, donde los estafadores crean perfiles falsos o tiendas virtuales fraudulentas.

3.3.2. Phishing

El phishing es otra modalidad de ciberdelito que ha crecido considerablemente en Guatemala. Los ciberdelincuentes envían enlaces maliciosos o mensajes engañosos, generalmente a través de correos electrónicos, WhatsApp o redes como Facebook, que llevan a los usuarios a sitios falsos diseñados para robar credenciales de acceso o información personal.

3.3.3. Suplantación de identidad

La suplantación de identidad es un delito en el que los ciberdelincuentes crean cuentas falsas o acceden a las cuentas de las víctimas para hacerse pasar por ellas. Este delito puede causar daño a la dignidad, honra, reputación y daño emocional a las víctimas y se utiliza, en muchos casos, con fines de extorsión o venganza personal. En Guatemala el Código Penal en el artículo 274 “F” menciona que, se impondrá prisión de seis meses a dos años, y multa de doscientos a mil quetzales al que, sin autorización, utilizare los registros informáticos de otro, o ingresare, por cualquier medio, a su banco de datos o archivos electrónicos. Este es un ejemplo de lo que se establece como faltas a la moral pública.

3.3.4. Ciberacoso

El ciberacoso, o bullying cibernético, afecta principalmente a adolescentes y mujeres jóvenes. Se trata de una forma de acoso que ocurre a través de comentarios ofensivos, amenazas o la difusión de información personal sin consentimiento. Las redes sociales, como Facebook y TikTok, han sido especialmente problemáticas en este sentido, (Gobierno de Canarias, 2012) menciona el caso de Amanda Todd, una adolescente canadiense de 15 años, fue víctima de ciberacoso tras ser engañada para mostrar sus pechos a través de una webcam. Su agresor utilizó la imagen para chantajearla y, al no cumplir con la demanda de realizar un striptease en línea, difundió la foto en Internet y creó un perfil en Facebook con su imagen como foto de perfil. Este acoso persistente llevó a Amanda a mudarse y cambiar de escuela en un intento por escapar del hostigamiento. Un mes después de publicar un video en YouTube relatando su experiencia, Amanda se suicidó el 10 de octubre de 2012.

3.3.5. Difusión de pornografía infantil

Este es uno de los delitos más graves y está en aumento en Guatemala. Aunque las autoridades han implementado medidas para contrarrestarlo, las redes sociales se han convertido en un medio a través del cual los delincuentes intercambian material de abuso sexual infantil, lo que ha requerido la intervención de las fuerzas de los órdenes nacionales e internacionales.

Los ciberdelitos en Guatemala no afectan a todos los grupos por igual. Ciertos sectores de la población son más vulnerables a estas amenazas digitales, debido a una combinación de factores socioeconómicos, educativos y culturales. Dentro de los grupos vulnerables más afectados se encuentran:

3.3.6. Adolescentes y jóvenes vulnerables

Los adolescentes y jóvenes guatemaltecos son especialmente vulnerables a ciberdelítos como el ciberacoso y la suplantación de identidad. La falta de educación digital adecuada y el uso intensivo de redes sociales sin las precauciones necesarias hacen que este grupo etario sea un objetivo fácil para los delincuentes.

3.3.7. Mujeres

Las mujeres, particularmente las jóvenes y las mujeres profesionales, son frecuentemente objeto de ciberacoso y extorsión en línea. Las redes sociales, en muchos casos, se han convertido

en un espacio donde se les somete a acoso sexual, amenazas de violencia y chantajes emocionales o económicos.

3.3.8. Pequeñas empresas

Los emprendedoras y pequeñas empresas en Guatemala también son blanco de estafas en línea, especialmente aquellas relacionadas con el comercio digital. Las tiendas en línea falsas o las estafas de pago electrónico a través de redes sociales han afectado negativamente a este sector, que a menudo carece de los recursos para implementar medidas de ciberseguridad.

3.3.9. Redes Sociales más Afectadas

En Guatemala como en la mayoría de los países el ciberdelito afecta a múltiples plataformas, pero, hay algunas redes sociales que destacan por ser las más vulnerables a estas actividades delictivas porque además son las más populares y cuentan con mayor número de cibernautas, dentro de ellas se puede mencionar:

3.3.9.1. Facebook.

Es la segunda plataforma más utilizada en todo el mundo para búsquedas generales en línea "(…) con más de 10 millones de usuarios en Guatemala y con 3.065 millones de usuarios activos mensuales en el mundo, Facebook seguirá creciendo en 2024, frente al 1,3% del año pasado". (Kolquare, 2024, parr.2)

La plataforma Facebook sigue siendo la red social más popular y, por ende, la más afectada por el ciberdelito. Las estafas, suplantación de identidad y el phishing son comunes en esta plataforma. Además, el contenido relacionado con la explotación infantil ha sido denunciado en múltiples ocasiones. El control de estos ciberdelítos es complejo y difícil de manejar debido a que se pueden planificar y ejecutar desde diferentes partes del mundo

3.3.9.2. WhatsApp

En lo que se refiere a la plataforma whatsApp, aunque no es una red social en el sentido tradicional, es uno de los canales más utilizados para la difusión de fraudes y phishing.

Una de sus características es la encriptación punto a punto lo que ha hecho que sea difícil para las autoridades rastrear la actividad ilegal, esto ha aumentado su atractivo para los ciberdelincuentes que realizan sus actividades ilegales con mayor confianza.

3.3.9.3. Instagram

Instagram se ubica como una red popular entre los jóvenes, esto la convierte en un terreno fértil para el ciberacoso y la suplantación de identidad. Los estafadores también utilizan esta plataforma para vender productos falsos o servicios fraudulentos, afectando tanto a usuarios individuales como a pequeñas empresas.

3.3.9.4. TikTok

La red TikTok, aunque es una plataforma virtual relativamente nueva en comparación con otras redes, su crecimiento ha sido vertiginoso y ha incrementado su popularidad en Guatemala, especialmente entre adolescentes. Esto ha llevado a un aumento en casos de ciberacoso y la difusión de contenido inapropiado que vulnera la privacidad de los jóvenes.

Con lo que se ha explicado en los párrafos anteriores se puede notar que el panorama del ciberdelito en las redes sociales en Guatemala presenta desafíos significativos tanto para los usuarios como para las autoridades.

Los delitos más comunes, como el phishing, la suplantación de identidad, la sextortion y el ciberacoso, están afectando de manera desproporcionada a grupos vulnerables como niños(as), adolescentes, mujeres y pequeñas empresas. Las redes sociales más populares, como Facebook y WhatsApp, son las plataformas más afectadas, lo que evidencia la necesidad de políticas más estrictas de seguridad digital y una mayor concientización entre los usuarios.

El aumento del ciberdelito no solo pone en peligro la seguridad personal y financiera de los guatemaltecos, sino que también afecta la confianza en las plataformas digitales. Es imperativo que tanto el gobierno como las empresas tecnológicas colaboren para implementar medidas más efectivas de protección cibernética, y que la educación digital se convierta en una prioridad para reducir la vulnerabilidad de los usuarios. Solo a través de una acción conjunta se podrá mitigar el impacto del ciberdelito en el país y garantizar un entorno digital más seguro para todos.

3.4. Mecanismos de protección contra el ciberdelito en Guatemala

En la era digital, el ciberdelito ha surgido como una de las principales amenazas para la seguridad y el bienestar de las naciones, afectando tanto a individuos como a instituciones públicas, empresas, comercios, entre otros.

Guatemala no es ajena a estas amenazas, enfrentando una creciente ola de crímenes cibernéticos que varían desde el fraude electrónico hasta el ciberterrorismo. Para enfrentar estos problemas, el país cuenta con mecanismos tanto nacionales como internacionales de protección y respuesta.

Este acápite abordará las instituciones encargadas de luchar contra el ciberdelito en Guatemala, los mecanismos disponibles para la ciudadanía y las empresas, así como los resultados que se pueden esperar al acudir a estos organismos.

3.4.1. Instituciones nacionales de protección contra el ciberdelito en Guatemala

Guatemala cuenta con varias instituciones encargadas de la protección y prevención del ciberdelito, siendo una de las principales la Superintendencia de Telecomunicaciones -SIT-, que regula el uso de las tecnologías de la información y la comunicación -TIC-. La Unidad de Delitos Informáticos del Ministerio Público -MP- también desempeña un rol fundamental en la investigación de los crímenes relacionados con las TIC, ofreciendo a la ciudadanía un canal para denunciar estos delitos.

Según el Ministerio Público, esta unidad trabaja en colaboración con otras agencias del gobierno, así como con entidades privadas, para fortalecer la ciberseguridad del país (Miniserio Publico, 2021, s.n.)

Otra institución clave es la Policía Nacional Civil -PNC-, la cual cuenta con la División de Investigación de Delitos de Alta Tecnología -DIDAT-. Esta división se especializa en la prevención y represión del cibercrimen, operando tanto en el ámbito investigativo como en el de persecución penal. Además, Guatemala ha desarrollado el Centro de Respuesta a Incidentes Cibernéticos -CERT- Guatemala, que ofrece servicios de análisis y respuesta ante ciberataques y vulnerabilidades en las redes nacionales (Prensa Libre, 2018, parr. 1)

(Del Aguila, 2019) expresa que estas instituciones proporcionan diversas vías para que los ciudadanos y las empresas puedan denunciar delitos cibernéticos. Generalmente, las denuncias pueden realizarse a través de plataformas digitales habilitadas por el Ministerio Público, por teléfono o en persona en las oficinas de la PNC. Sin embargo, las limitaciones en infraestructura y personal técnico capacitado representan desafíos constantes para la adecuada atención de los casos de ciberdelito en el país.

3.4.2. Instituciones internacionales y su rol en la lucha contra el ciberdelito

Además de los esfuerzos nacionales, Guatemala forma parte de varios acuerdos y tratados internacionales que promueven la cooperación en la lucha contra el ciberdelito. Un ejemplo importante es su relación con la Interpol, que cuenta con una división especializada en crímenes cibernéticos. La Interpol provee asistencia técnica y capacitación a las fuerzas de seguridad locales y fomenta el intercambio de información entre países para identificar y detener redes criminales transnacionales dedicadas al ciberdelito (Interpol, 2020, parr. 3)

Asimismo, Guatemala ha firmado el Convenio de Budapest sobre Ciberdelincuencia, promovido por el Consejo de Europa, que constituye el primer tratado internacional que busca enfrentar los crímenes informáticos a través de la armonización de leyes nacionales y la cooperación internacional (Consejo de Europa, 2001). Este convenio permite la colaboración entre Estados para investigar y procesar delitos cibernéticos a nivel global, lo que ha sido crucial para Guatemala en casos de crímenes que involucran a actores extranjeros.

Otro actor relevante es la Organización de Estados Americanos -OEA-, que por medio de su Comité Interamericano contra el Terrorismo -CICTE-, ha lanzado programas que fortalecen la ciberseguridad y combaten el ciberdelito en los países miembros. “La OEA ha ayudado a Guatemala mediante la capacitación de funcionarios en materia de ciberseguridad y el apoyo técnico para el desarrollo de capacidades internas” (OEA, 2018. s.n.).

3.4.3. Resultados esperados y desafíos persistentes

El hecho de acudir a las instituciones mencionadas puede proporcionar diversos resultados, dependiendo de la naturaleza del ciberdelito y de la efectividad de las investigaciones. Hay que mencionar que las investigaciones de ciberdelítos se tornan complejas y difíciles de realizar debido a que dependiendo del tipo de ciberdelito su comisión puede originarse desde cualquier lugar en donde haya un ordenador digital.

En muchos casos, la denuncia a tiempo y la colaboración entre organismos nacionales e internacionales han permitido resolver incidentes cibernéticos, recuperar activos financieros y capturar a los responsables. Sin embargo, uno de los mayores retos es la falta de recursos humanos especializados y tecnológicos para responder de manera efectiva a la creciente sofisticación de los crímenes cibernéticos.

Por ejemplo, "(…) aunque la DIDAT ha logrado algunos avances en la lucha contra el ciberdelito, los recursos limitados en comparación con la magnitud del problema implican que no todos los casos se resuelvan de manera rápida o satisfactoria" (Carrillo, 2020. s.n.). Además, señala el autor que la falta de educación y concienciación sobre la ciberseguridad entre la población general y las pequeñas empresas también dificulta la prevención y detección temprana de estos delitos.

(Del Aguila, 2019) refiere que, en el ámbito internacional, el principal desafío sigue siendo la colaboración efectiva entre los Estados para la localización y enjuiciamiento de delincuentes que operan en múltiples jurisdicciones.

La falta de armonización completa entre las legislaciones nacionales y las diferencias en las prioridades de seguridad entre países pueden entorpecer las investigaciones conjuntas y el intercambio de información.

En el tema de mecanismos de protección contra el ciberdelito se puede observar que Guatemala ha avanzado en la creación de mecanismos para enfrentar el ciberdelito tanto a nivel nacional como internacional, pero todavía enfrenta importantes retos en términos de recursos y capacidades técnicas.

Las instituciones como el Ministerio Público, la Policía Nacional Civil y el Computer Emergency Response Team (En inglés CERT) han logrado resultados importantes, aunque limitados por la infraestructura disponible. A nivel internacional, la cooperación a través de organismos como la Interpol, la OEA y el Convenio de Budapest es fundamental para enfrentar las amenazas cibernéticas que trascienden fronteras.

A pesar de estos esfuerzos, la creciente sofisticación de los ciberdelincuentes y la falta de recursos siguen siendo barreras que Guatemala deberá superar para garantizar una ciberseguridad efectiva en el futuro.

Para ir concluyendo el presente capítulo se puede inferir que el Trabajo Social juega un papel crucial en la prevención del ciberdelito en Guatemala, como se refirió abundantemente en este capítulo, ya que aborda las causas sociales, educativas y estructurales que fomentan el desarrollo de este tipo de delitos.

Se puede observar que, a través de la educación, sensibilización y creación de redes de apoyo, los trabajadores sociales pueden influir directamente en comunidades vulnerables, promoviendo el uso responsable de la tecnología y ayudando a prevenir comportamientos de riesgo en línea.

Hay que tener presente que en Guatemala como en la mayoría de los países la penetración de la tecnología y el internet ha aumentado considerablemente, lo que también ha incrementado el riesgo de ciberdelítos como el acoso, el fraude y la explotación sexual.

Los(as) trabajadores(as) sociales tienen la capacidad de identificar las poblaciones más expuestas, como los jóvenes y los menores de edad, y de implementar programas preventivos que refuercen la seguridad digital y promuevan una cultura de protección en línea.

Además, el Trabajo Social está en la capacidad de contribuir a la formulación de políticas públicas y programas comunitarios que refuercen la resiliencia ante el ciberdelito. Esto incluye trabajar con instituciones educativas, gobiernos y organizaciones no gubernamentales para garantizar un enfoque integral de prevención, que no solo responda a las consecuencias del ciberdelito, sino que ataque las raíces del problema: la exclusión social, la falta de oportunidades educativas y el desconocimiento de las herramientas de seguridad en el entorno digital.

En resumen, el Trabajo Social en Guatemala es esencial para mitigar el impacto del ciberdelito, fomentando la educación, la concienciación y la creación de entornos seguros en línea, especialmente para los grupos sociales más vulnerables de la sociedad.

También es oportuno terminar expresando que el Trabajo Social y la prevención del ciberdelito se complementan de manera significativa tanto en la teoría como en la práctica, ya que ambos comparten objetivos comunes: la protección de las personas vulnerables, la promoción de comportamientos seguros y el fortalecimiento del bienestar social.

A manera de corolario se describe a continuación de manera sucinta la forma cómo se integran en la teoría y en la práctica el Trabajo Social y la prevención del ciberdelito.

Integrar el Trabajo Social y el ciberdelito implica comprender cómo las teorías del Trabajo Social pueden aplicarse a la prevención, intervención y tratamiento de los problemas relacionados con el ciberdelito. A continuación, se presenta una descripción de esta integración.

En el aspecto teórico el Trabajo Social se basa en teorías que abordan el comportamiento humano y las interacciones sociales. Una de las teorías relevantes es la teoría del conflicto, que sugiere que las desigualdades sociales pueden contribuir a comportamientos delictivos, incluidos los ciberdelítos.

Según algunos autores, "la desigualdad en el acceso a la tecnología puede llevar a la exclusión social, lo que a su vez puede aumentar la probabilidad de que las personas se involucren en ciberdelítos" (Smith, 2020, p.45)

Lo afirmado por Smith se puede entender desde la interpretación que las personas sin acceso a la tecnología están en desventaja en términos de educación y oportunidades laborales. Esto puede generar frustración y una necesidad de obtener ingresos, lo que podría empujarlas a buscar formas ilícitas de ganarse la vida, como los ciberdelítos.

Otra interpretación que se le podría dar a lo expresado por Smith es que las personas con menos acceso a la tecnología también suelen carecer de habilidades digitales. Esto puede convertir a la tecnología en algo percibido como ajeno a sus posibilidades sociales y económicas. En algunos casos, puede llevar a que busquen formas alternativas y a menudo ilegales para participar en el mundo digital, como se evidencia con el aparecimiento de hackeos u otras actividades delictivas en línea.

También hay que tomar en cuenta que la exclusión social, especialmente en grupos marginados o vulnerables, puede llevar a un sentimiento de aislamiento y desconexión. Internet puede convertirse en una vía para encontrar conexiones, incluso si son a través de grupos o redes criminales que promueven actividades ilícitas en línea.

De esta manera se puede observar que las personas con acceso restringido a la tecnología pueden no conocer los métodos legales para aprovechar internet. En cambio, podrían verse atraídas por actividades delictivas en línea que parecen ofrecer ingresos rápidos o accesos a bienes y servicios que de otro modo no pueden obtener.

En el aspecto práctico, los Trabajadores Sociales pueden desempeñar un papel crucial en la educación y la prevención del ciberdelito. Esto incluye la creación de programas de concienciación sobre la seguridad en línea y la promoción de habilidades digitales. Como se menciona por parte

de algunos autores, "los programas de intervención que educan a los jóvenes sobre los riesgos del ciberdelito son esenciales para reducir la incidencia de estos delitos" (Johnson & Lee, 2021, p.78).

Como se puede leer en párrafos anteriores la integración del Trabajo Social y el ciberdelito es esencial para abordar de manera efectiva los desafíos que presenta el entorno digital. A través de la aplicación de teorías sociales y la implementación de prácticas de intervención, los trabajadores sociales pueden contribuir significativamente a la prevención y el tratamiento de los ciberdelítos.

Capítulo IV. Análisis Estratégico

El conjunto de Estados del mundo conocido como Comunidad Internacional ha servido de escenario para el desarrollo del ciberdelito. Por su parte el ciberdelito como ya se ha mencionado con anterioridad ha surgido como una de las amenazas más suigeneris para el derecho interno de los Estados, así como del Derecho Internacional Público en el siglo XXI, afectando tanto a individuos como a naciones.

Fenómenos como el desarrollo de los mercados financieros internacionales, la tecnificación del crimen organizado internacional, la globalización y el avance tecnológico de las comunicaciones se han convertido en un caldo de cultivo propicio a la expansión de actividades delictivas en el ciberespacio, esta situación ha puesto a la comunidad internacional en una encrucijada política, social y económica para buscar formas de colaboración y respuesta ante este fenómeno tan versátil.

En el presente acápite se explora la relación entre la comunidad internacional y el ciberdelito, analizando las iniciativas de cooperación, los mecanismos de protección existentes y los retos que enfrentan los Estados en la lucha contra el ciberdelito.

Es necesario recordar que el ciberdelito se define como cualquier actividad delictiva que se lleva a cabo a través de medios digitales o que tiene como objetivo a sistemas informáticos y redes (UNODC, 2020, s.p.). Esto incluye una amplia gama de actividades, desde el fraude en línea y el robo de identidad hasta ataques cibernéticos a infraestructuras críticas.

Entonces, está claro que el ciberdelito no tiene fronteras más bien su escenario de actuación es la comunidad internacional, por lo que son los diferentes países agrupados en regiones los que deben reaccionar con estrategias para el combate al ciberdelito entre las que se puede mencionar como una de las primeras que vendría a ser la cooperación internacional.

En las líneas anteriores se evidencia la naturaleza transnacional del ciberdelito, lo que requiere una respuesta coordinada a nivel internacional. Los delincuentes cibernéticos suelen operar desde distintas jurisdicciones, complicando la aplicación de la ley y la persecución de los delitos. Según el Informe de Ciberseguridad de INTERPOL (2021), aproximadamente el 70 % de los delitos cibernéticos presentan un componente internacional, lo que resalta la importancia de la

colaboración entre países. En este contexto, es posible identificar algunas iniciativas internacionales, las cuales se describen a continuación.

Con este marco de referencia se puede inferir que uno de los marcos jurídicos más importantes es el Convenio de Budapest sobre Cibercriminalidad, adoptado en 2001, que establece un marco legal para la cooperación internacional en la lucha contra el ciberdelito (Consejo de Europa, 2001, s.p.)

Concretamente este convenio ha sido ratificado por más de 60 países y proporciona directrices sobre la legislación nacional, la cooperación internacional y la asistencia técnica que se pueden utilizar como estrategias para disminuir la práctica del ciberdelito.

El Convenio de Budapest es el primer tratado internacional que "(…) se centra en la lucha contra los delitos cibernéticos, adoptado en el año 2001 por el Consejo de Europa, junto con el apoyo de países fuera del continente europeo, como Estados Unidos y Japón" (Consejo de Europa, 2001). El objetivo principal del Convenio es proporcionar un marco legal común para mejorar la cooperación internacional y la armonización de leyes nacionales en relación con los delitos informáticos y el uso indebido de redes informáticas.

Ahora bien, hay aspectos que son considerados relevantes según el criterio de diferentes autores, dentro de esto se puede referir:

1. Criminalización de Conductas Específicas: El tratado abarca una serie de delitos que deben ser tipificados por los Estados firmantes, tales como el acceso ilícito a sistemas informáticos, la interceptación ilegal de datos, y el uso indebido de dispositivos (Ochoa, 2020, p. 35).

Esta reglamentación, ampliamente discutida por los países miembros, busca fortalecer la seguridad cibernética a nivel mundial al establecer estándares mínimos que los países deben cumplir.

2. Procedimientos para la Preservación y Recolección de Pruebas Electrónicas: "El Convenio incluye normas sobre la preservación rápida de datos almacenados y la intercepción de datos en tiempo real con el objetivo de facilitar la recolección de pruebas en investigaciones internacionales" (Jiménez , 2019, p. 59).

Este aspecto resulta de singular relevancia para acelerar la respuesta de los diferentes Estados ante ciberataques que a menudo trascienden las fronteras nacionales y no solo agreden las diferentes soberanías de los Estados sino también sus poblaciones.

3. Cooperación Internacional: “Un componente esencial del Convenio es el fomento de la cooperación entre países, lo cual se traduce en la asistencia mutua para el intercambio de información y pruebas en tiempo real durante la investigación de delitos cibernéticos” (Fernández, 2018, p. 89)

Este componente también incluye medidas importantísimas como la creación de puntos de contacto digital para estar en vigilancia los trecientos sesenta y cinco días del año y de esta manera facilitar la comunicación directa entre las respectivas autoridades competentes.

4. Protección de los Derechos Humanos y Libertades Fundamentales: Aunque el Convenio se centra en mejorar la eficacia en la lucha contra la ciberdelincuencia, también reconoce la necesidad de proteger los derechos fundamentales, incluyendo el derecho a la privacidad (Rodríguez, 2022, p. 45)

Rodríguez refleja la obligación de los Estados de garantizar que las medidas adoptadas en virtud del Convenio sean proporcionales y respetuosas con los derechos humanos. Esto porque si se analiza uno de los aspectos más sensible para ser vulnerado en entornos digitales es el derecho a la privacidad, tomando en cuenta que el ciberespacio se encuentra donde hay un ordenador no importando si es la oficina, el hogar, el parque, cine, entre otros.

5. Desafíos y Críticas: A pesar de sus logros, el Convenio ha sido objeto de críticas, especialmente en relación con la posible afectación a la privacidad y la libertad de expresión en línea. “Algunos expertos advierten que ciertas disposiciones podrían ser utilizadas para incrementar la vigilancia estatal, lo que plantea preocupaciones sobre el abuso de poder” (Pérez, 2021, p. 123)

Como en todo fenómeno o relación social surge la dicotomía de lo positivo o negativo que pueden ser los procesos asumidos para la atención de las diferentes situaciones que surgen de la misma dinámica humana.

A pesar de todo el Convenio de Budapest sigue siendo un marco legal fundamental para enfrentar los desafíos del ciberdelito a nivel global, aunque también enfrenta el reto de adaptarse continuamente a las nuevas amenazas tecnológicas y a los cambios en el entorno digital.

La comunidad internacional en base al principio del derecho internacional pacta sunt servanda tiene la obligación de cumplir con este convenio y con todos los que sea necesario para lograr el establecimiento de relaciones pacíficas en la sociedad mundial y si es necesario como en este caso buscar otros instrumentos más específicos como protocolos, Adendums, reglamentos, entre otros para alcanzar tal fin.

4.1 Ciberdelito en Guatemala

El flagelo del ciberdelito se ha convertido en uno de los principales problemas y amenazas en Guatemala, convirtiéndose en una de las amenazas emergentes que al igual que la pandemia COVID-19 ha puesto en riesgo la seguridad nacional, la economía y el bienestar social del país.

Esta situación refleja tanto la creciente dependencia de la tecnología digital como la falta de infraestructura y políticas adecuadas para prevenir y combatir los delitos cibernéticos y el adecuado control de las plataformas digitales. En este análisis estratégico, se presentarán aspectos relevantes de este fenómeno como: tendencias, debilidades, políticas y estrategias que se deben tomar ante esta seria amenaza.

4.1.1. Panorama Actual del Ciberdelito en Guatemala

América Latina, ha experimentado un aumento en la cantidad y sofisticación de los ciberdelítos, especialmente en el contexto postpandemia y Guatemala no es la excepción. El comercio y la educación llegaron a masificar el uso de plataformas digitales debido al trabajo desde casa.

Según un informe de la Comisión Interamericana de Telecomunicaciones (CITEL), en América Latina, "los ataques de ransomware han aumentado en un 300% desde el inicio de la pandemia" (CITEL, 2023, p. 112). Guatemala no ha sido la excepción, experimentando un aumento similar en el número de ataques de este tipo.

Como ya se ha mencionado en partes anteriores de esta investigación entre los delitos más comunes en el país se encuentran el robo de identidad, fraude en línea, extorsión digital y ataques de ransomware. La Superintendencia de Telecomunicaciones (SIT) reporta que "durante 2022, los

incidentes relacionados con fraude y suplantación de identidad aumentaron un 45% en comparación con el año anterior" (Superintendencia de Telecomunicaciones, 2023, p. 89)

Se puede inferir entonces, que los ciberdelincuentes están aprovechando la falta de conciencia y desconocimiento de medidas de seguridad y legislación entre los cibernautas de Guatemala

4.1.2. Debilidades Críticas

La situación de vulnerabilidad de Guatemala frente al ciberdelito se debe a varios factores interrelacionados. En un primer plano se puede ubicar la falta de legislación eficaz. No obstante Guatemala es un país que ha promulgado leyes para el control del ciberdelito como la Ley Contra la Delincuencia Informática (Decreto 47-2008), la implementación y actualización de estas normativas sigue siendo insuficiente.

Un análisis de la situación legislativa realizado por el Centro de Estudios de Justicia de las Américas (CEJA) concluye que "la legislación vigente no está alineada con los estándares internacionales, lo que limita su efectividad en la persecución y condena de los ciberdelincuentes" (CEJA, 2022, P.76)

Seguidamente, también se puede encontrar una débil infraestructura en seguridad pública del Estado lo que resulta también en una débil infraestructura de ciberseguridad.

Un estudio de la Universidad del Valle de Guatemala destaca que "más del 60% de las empresas en el país no cuentan con sistemas de protección avanzados, como firewalls de última generación o sistemas de detección de intrusiones" (Universidad del Valle, 2023, p. 53)

Como se puede observar las instituciones gubernamentales y empresas privadas en Guatemala carecen de una infraestructura para la protección contra ciberataques. Y si esto sucede con el gobierno y la iniciativa privada la pregunta es ¿Cómo se encuentra protegida la sociedad guatemalteca contra estos ciberataques? Y principalmente ¿Qué protección tienen los grupos vulnerables de Guatemala ante esta amenaza?

Otro aspecto digno de mencionar es la baja conciencia o bajo nivel de conocimiento en seguridad digital que existe en el país, este aspecto que se puede observar tanto en el sector público como en el privado agrava la situación. Existen muchas organizaciones que no invierten en

programas de capacitación para sus empleados, lo que resulta en vulnerabilidades explotables por los delincuentes.

Según un informe del Instituto de Investigaciones Sociales (IIS), "solo el 28% de las empresas medianas y grandes en Guatemala han implementado programas de capacitación en ciberseguridad para sus empleados" (ISS, 2023, p. 121).

4.1.3. Impacto Socioeconómico del Ciberdelito

La Organización de los Estados Americanos (OEA) estima que "los costos asociados con el ciberdelito en Guatemala ascendieron a más de 200 millones de dólares en 2022, considerando tanto las pérdidas financieras como los gastos en medidas de mitigación" (OEA, 2023, P. 65)

Aunque hay que tomar en cuenta que el impacto del ciberdelito en Guatemala no se limita a las pérdidas financieras de forma directa. También se debe observar cómo se afecta la confianza de los ciudadanos y empresas en las plataformas digitales, esta situación podría obstaculizar el crecimiento del comercio electrónico y la digitalización de la economía.

Además, los ataques contra infraestructuras de seguridad e infraestructuras críticas, como servicios de salud y suministro eléctrico, plantean riesgos adicionales para la seguridad nacional tal y como ha quedado demostrado con los ciberataques que ha sufrido la Organización del Tratado del Atlántico Norte OTAN en el año 2023.

4.1.4 Estrategias para combatir el Ciberdelito

Para enfrentar la creciente amenaza del ciberdelito, Guatemala necesita adoptar un enfoque estratégico y multisectorial que incluya: a) actualizar el marco legal vigente para cubrir todas las formas emergentes de ciberdelito. b) La implementación de una Ley de Protección de Datos Personales, actualmente en discusión en el Congreso, sería un paso importante para proteger la privacidad y seguridad de los ciudadanos (Congreso de la Republica de Guatemala, 2023)

Otro tema importante es la infraestructura.

También se debe invertir en Infraestructura de Ciberseguridad, tanto el sector público como el privado deben invertir en tecnologías de ciberseguridad avanzadas y en la creación de oficinas de respuesta inmediata ante ciberataques. Esto debería de incluir la implementación de inteligencia artificial para la detección temprana de amenazas y la respuesta rápida a incidentes (Centro Nacional de Ciberseguridad, 2023, p. 98).

No hay que perder de vista la educación y capacitación como elemento clave para promover cambios significativos en toda sociedad.

La promoción de una cultura de ciberseguridad es esencial para reducir las vulnerabilidades humanas. Programas educativos y campañas de sensibilización podrían ayudar a fortalecer la capacidad de los ciudadanos y empresas para defenderse de los ataques. El Ministerio de Educación y la SIT deberían colaborar en la inclusión de contenidos sobre ciberseguridad en los currículos escolares (Ministerio de Educación, 2023, p. 134).

Aunque en Guatemala el tema educativo presenta serios déficits es bueno establecer campañas de divulgación acerca de la amenaza del ciberdelito y las formas para combatirlo.

El ciberdelito en Guatemala representa una amenaza creciente que requiere una respuesta integral y coordinada entre el gobierno, el sector privado y la sociedad civil. Aunque se han dado algunos pasos en la dirección correcta, como la creación de la Dirección de Ciberseguridad y el desarrollo de políticas nacionales, queda un largo camino por recorrer para alcanzar un nivel adecuado de resiliencia frente a los ciberdelitos.

La implementación de medidas estratégicas basadas en un enfoque preventivo y colaborativo es crucial para garantizar la seguridad digital en el país y es en este espacio que disciplinas como el Trabajo Social puede proporcionar un aporte significativo a nivel comunitario.

4.2. Marco Institucional para el Ciberdelito en Guatemala

En Guatemala, el marco institucional para la atención del ciberdelito se ha desarrollado en respuesta al incremento de amenazas en el ciberespacio y la necesidad de proteger tanto a individuos como a instituciones. Este marco está compuesto por un conjunto de leyes, organismos de seguridad y estrategias que buscan combatir los delitos informáticos, aunque enfrenta retos significativos en su implementación y efectividad.

La base legal para la atención del ciberdelito en Guatemala se encuentra en diversas normativas que abordan tanto la seguridad informática como la protección de datos personales.

La Ley Contra la Delincuencia Organizada (Decreto No. 21-2006) y la Ley de Protección de la Información Personal (Decreto No. 57-2008) son ejemplos de instrumentos legales que contemplan delitos relacionados con el uso indebido de la información y el acceso no autorizado a sistemas informáticos.

Adicionalmente, el Código Penal guatemalteco incluye artículos que sancionan el acceso ilícito a sistemas y la alteración de datos informáticos (Congreso de la Republica de Guatemala, 2006, p. 112). Sin embargo, aunque estas leyes establecen sanciones para los ciberdelitos, su alcance aún es limitado debido a la rápida evolución de las amenazas cibernéticas que no siempre son cubiertas por la normativa vigente.

En cuanto a la institucionalidad, Guatemala cuenta con la Unidad de Delitos Informáticos, una división especializada dentro del Ministerio Público que se encarga de investigar los delitos cibernéticos. Esta unidad colabora con la Policía Nacional Civil (PNC) para la recolección de pruebas digitales y la identificación de responsables en casos que van desde fraudes electrónicos hasta ciberacoso (Ministerio Publico de Guatemala, 2022, p. 23)

Además, el Instituto Nacional de Ciencias Forenses (INACIF) realiza peritajes técnicos que son esenciales para los procesos judiciales relacionados con ciberdelitos. No obstante, el principal reto que enfrentan estas instituciones es la falta de recursos, tanto humanos como tecnológicos, para hacer frente a la creciente sofisticación de los ciberataques.

El impacto del marco institucional en la lucha contra el ciberdelito en Guatemala ha sido mixto. Por un lado, la creación de unidades especializadas ha permitido una mayor capacidad de respuesta a incidentes de ciberseguridad, especialmente en el ámbito financiero, donde los bancos han colaborado estrechamente con las autoridades para prevenir y mitigar fraudes electrónicos (Superintendecia de Bancos de Guatemala, 2020, p. 45).

Por otro lado, la falta de una estrategia nacional integral en ciberseguridad ha limitado la efectividad de estas medidas, dejando a muchos sectores vulnerables a ataques que van desde el phishing hasta el ransomware.

El Instituto Centroamericano de Estudios Fiscales (2023) reveló que el 70% de las empresas en Guatemala han sido víctimas de algún tipo de ciberataque en los últimos tres años, lo que evidencia un aumento en la frecuencia y gravedad de estos incidentes (p. 67).

La respuesta institucional a estos ataques ha sido deficiente en muchos casos debido a la carencia de un marco regulatorio actualizado que permita una acción rápida y coordinada entre las diferentes entidades responsables de la ciberseguridad. Esta situación evidencia la necesidad de

políticas más fortalecidas que aborden no solo la respuesta, sino también la prevención y la resiliencia ante los ciberdelitos.

Adicionalmente, el sector público enfrenta grandes retos en cuanto a la seguridad de sus sistemas informáticos, con frecuentes reportes de ataques dirigidos a instituciones gubernamentales.

La Contraloría General de Cuentas (2021) señaló que la mayoría de las entidades públicas carecen de protocolos adecuados de protección de datos y gestión de incidentes de ciberseguridad, lo que incrementa su vulnerabilidad (p. 39). Esto no solo afecta la confianza de los ciudadanos en el gobierno, sino que también expone información sensible a riesgos significativos.

Finalmente, hay que señalar, aunque parezca repetitivo, pero es la realidad el marco institucional de Guatemala para la atención del ciberdelito, aunque ha avanzado en ciertos aspectos, aún presenta deficiencias importantes que limitan su efectividad.

La implementación de un marco regulatorio más abundante y sólido, acompañado de una estrategia nacional de ciberseguridad, es esencial para fortalecer la capacidad del país para enfrentar las amenazas cibernéticas.

La modernización de las leyes, el fortalecimiento de las capacidades de investigación y la promoción de la cooperación internacional son pasos necesarios para mejorar la respuesta ante el ciberdelito en un contexto global cada vez más digitalizado.

Es definitivo que para abordar el tema de la institucionalidad de cualquier tema dentro del espectro del Estado necesariamente hay que hablar de presupuesto por esta razón se dedicaran unas líneas a este importante tema.

El presupuesto destinado por el Gobierno de Guatemala para la atención del ciberdelito en el año 2024 refleja un marco limitado, a pesar de la creciente preocupación por la ciberseguridad en el país. De acuerdo con el Proyecto de Presupuesto General de Ingresos y Egresos presentado por el Ministerio de Finanzas, el presupuesto total para el país es de Q124,880 millones, con un enfoque principal en áreas tradicionales como la educación, salud, y seguridad pública general (Ministerio de Finanzas Publicas, 2023).

Sin embargo, dentro de este presupuesto, no se especifica una asignación clara y sustancial para combatir los ciberdelitos, no obstante que es un área que ha mostrado un aumento significativo en los últimos años, especialmente en incidentes de phishing y robo de identidad que afectan tanto a ciudadanos como a instituciones financieras.

El financiamiento para implementar políticas en esta materia sigue siendo un reto, ya que el presupuesto asignado al Ministerio de Gobernación, que sería el responsable de ejecutar estrategias de ciberseguridad, es de Q7,839.2 millones para 2024, pero enfocado principalmente en la seguridad física y no en infraestructura tecnológica específica para ciberseguridad (BLP Legal, 2022; diario Oficial, 2023)

En materia de presupuesto Guatemala a pesar de que ha reconocido formalmente la importancia de la ciberseguridad, el presupuesto actual no refleja un aumento significativo en los fondos necesarios para enfrentar el ciberdelito de manera efectiva.

La implementación de las leyes y proyectos futuros dependerá en gran medida de un ajuste en la asignación de recursos para la infraestructura tecnológica y la capacitación del personal encargado de la ciberseguridad, áreas que hasta ahora no han recibido el financiamiento adecuado.

4.3. Actores

Dentro del tema del ciberdelito en Guatemala subyace la importancia de los actores que sin duda alguna aportan una dinámica importante que se debe tomar en cuenta para contar con elementos objetivos que fundamenten el análisis en materia institucional, procedimental y presupuestaria.

También en este acápite se tratará de hacer una lectura de cada una de las principales instituciones que atienden el cibercrimen en Guatemala y por ende también deben atender el ciberdelito.

Tal y como se menciona en el capítulo I de este informe el enfoque utilizado en la metodología es el enfoque mixto ya que integra estrategias cuantitativas y cualitativas para aprovechar fortalezas de ambos enfoques, asimismo permite triangular hallazgos y enriquecer la interpretación de datos.

Para tal efecto se llevó a cabo un proceso de elaboración de instrumentos de investigación que dio como producto cinco cuestionarios para ser aplicados a igual número de instituciones públicas encargadas de la atención al ciberdelito en Guatemala.

El universo de estudio fue las instituciones públicas del Estado de Guatemala. La muestra es del tipo intencional que se enmarca en el muestreo no probabilístico. Es decir que el investigador seleccionó deliberadamente a cinco instituciones y específicamente a los(as) trabajadores(as) de las Unidades o Dependencias que cumplían ciertos criterios clave para el estudio.

En este orden de ideas, aplicó un cuestionario con ítems que plantean interrogantes para determinar si estas instituciones cuentan con el personal idóneo, con presupuesto, con infraestructura y asimismo observar si sus trabajadores tienen un manejo adecuado del tema.

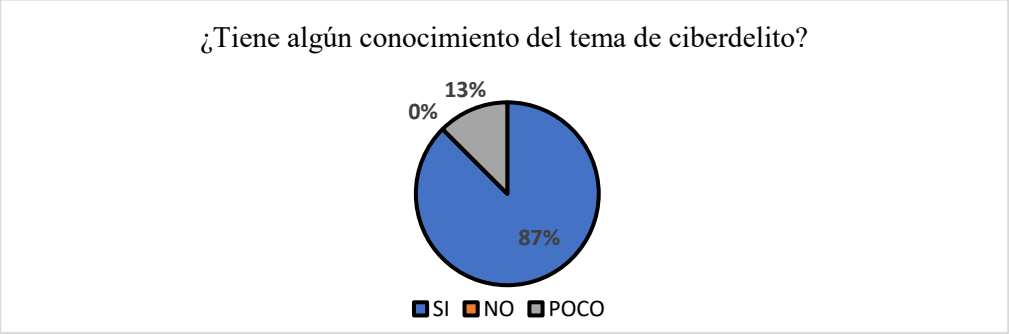
Las instituciones a las que se le aplicó el instrumento son: el Ministerio Público, Ministerio de Gobernación, secretaria para Prevención de Explotación y Trata de personas, Policía Nacional Civil y Trabajadores Sociales. A continuación, se presentan a detalle los resultados de cada una de estas Instituciones.

4.3.1. Ministerio Público

En el Ministerio público se aplicó el cuestionario a diez y seis trabajadores que tienen que ver directa o indirectamente con el ciberdelito.

Figura 1

Encuesta a trabajadores del Ministerio Publico que trabajan en atención al Ciberdelito



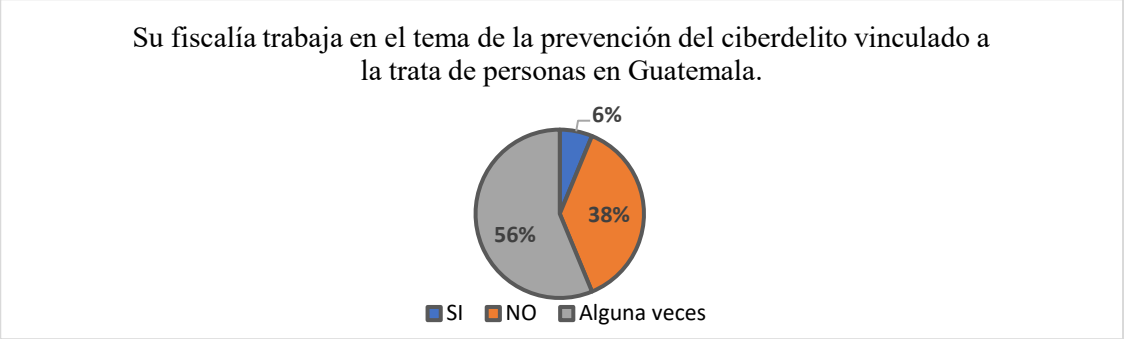
Nota: encuesta aplicada a integrantes de la Unidad contra la explotación sexual infantil en línea. 2024.

En la gráfica se puede observar que de diez y seis trabajadores del ministerio público que trabajan directa o indirectamente en atención al ciberdelito hay un 13% que manifiestan tener poco conocimiento del tema.

Ese 13 % no debería verse solo como un número, sino como una señal de alerta. En un momento en el que los delitos digitales están creciendo tan rápido, cualquier falta de conocimiento dentro de las instituciones debilita la manera en que se enfrentan estos casos y, además, puede hacer que la gente pierda confianza en el sistema de justicia.

Figura 2

Encuesta aplicada a integrantes de la Fiscalía del Ciberdelito

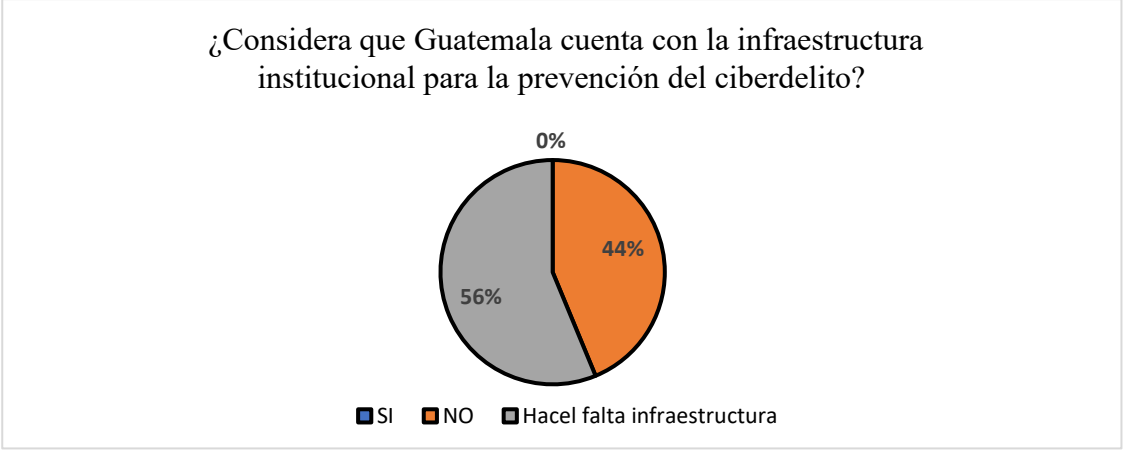


Nota: encuesta aplicada a integrantes de la fiscalía de ciberdelito. 2024.

En lo referente a ciberdelitos vinculados con la trata de personas esta fiscalía atiende pocos casos siendo este último uno de los delitos que afecta bastante a grupos vulnerables de mujeres y niñez en Guatemala.

Figura 3

Encuesta aplicada a trabajadores de la Unidad contra la explotación sexual infantil



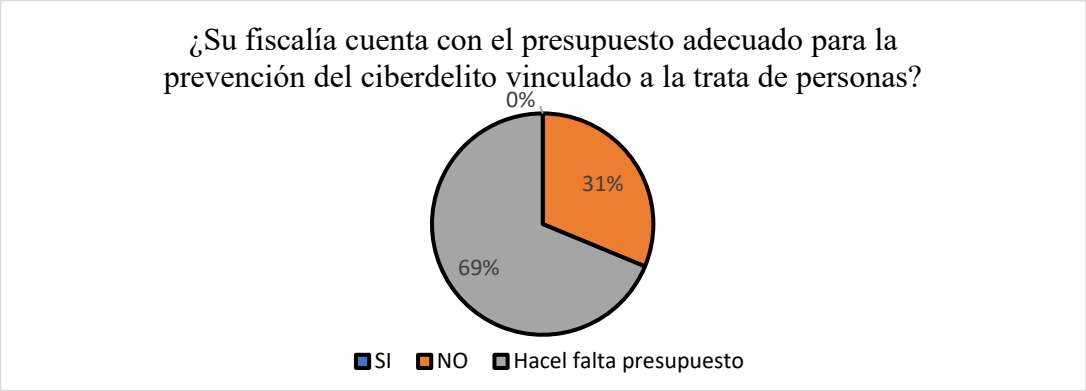
Nota: encuesta aplicada a integrantes de la Unidad contra la explotación sexual infantil en línea. 2024.

Es evidente que uno de los principales problemas en la atención a ciberdelitos es que Guatemala no cuenta con la infraestructura suficiente para responder adecuadamente a la demanda existente. La opinión de los encuestados se divide en dos respuestas una es que hace falta infraestructura y la otra es que no se cuenta con infraestructura suficiente.

El problema con la atención a los ciberdelitos en Guatemala no es solo la falta de infraestructura, sino también la percepción misma de quienes trabajan en el área: unos dicen que no hay, otros que lo poco que existe no alcanza. Al final, ambas partes reflejan lo mismo: el sistema está rebasado por la demanda. Esto no solo limita la capacidad de respuesta frente a los delitos digitales, sino que también deja un vacío que los delincuentes aprovechan para seguir operando.

Figura 4

Encuesta aplicada a integrantes de la Fiscalía del Ciberdelito



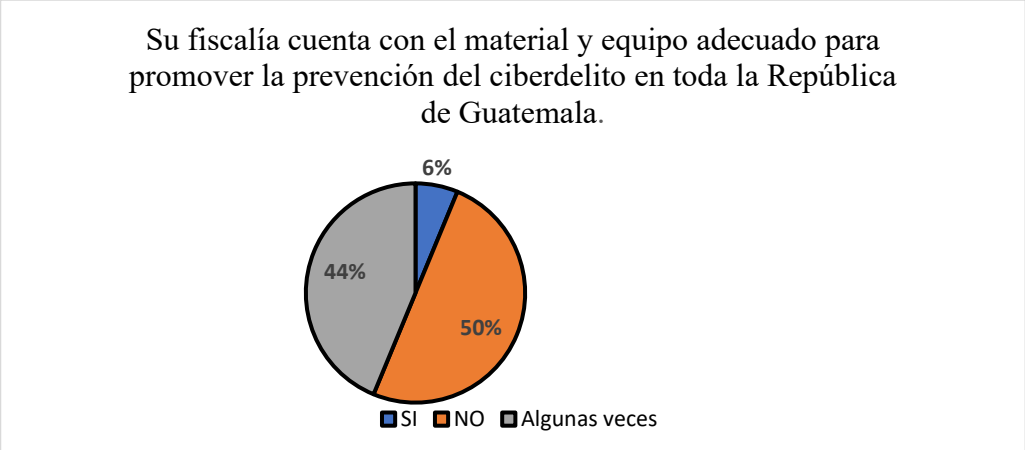
Nota: encuesta aplicada a integrantes de la fiscalía de ciberdelito. 2024

En materia de presupuesto los encuestados opinan que el presupuesto asignado no es suficiente de lo cual se puede inferir que la atención que prestan a las víctimas de ciberdelitos en Guatemala cuenta con debilidades que podrían fortalecerse con un mayor presupuesto. Esta situación representa un alto riesgo debido a que de una atención deficiente deriva la transgresión del derecho humano a la protección de la ley que deben gozar las víctimas.

El hecho de que el presupuesto sea insuficiente deja en claro una debilidad estructural: sin recursos no hay manera de dar una atención de calidad a las víctimas de ciberdelitos. Esto no es solo un problema administrativo, sino un riesgo real, porque una atención deficiente termina vulnerando derechos básicos. En pocas palabras, mientras no se invierta lo necesario, el sistema seguirá siendo débil y las víctimas quedarán desprotegidas frente a un delito que cada vez crece más.

Figura 5

Encuesta aplicada a trabajadores de la Fiscalía del Ciberdelito



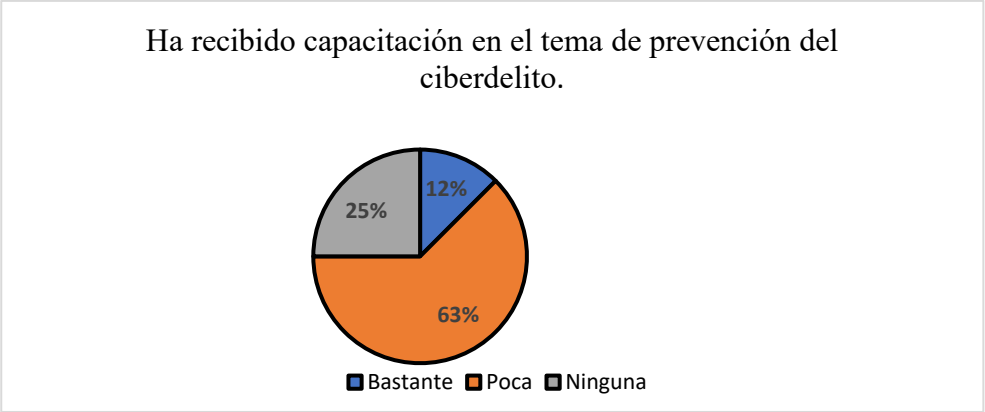
Nota: encuesta aplicada a integrantes de la fiscalía de ciberdelito. 2024.

La mitad de los trabajadores que respondieron el cuestionario opina que no se cuenta con el equipo y material necesario para la prevención del ciberdelito y el 44 % opina que solo algunas veces cuentan con el equipo adecuado. Únicamente el 6 % afirma que si tienen el material y equipo adecuado.

Este dato refleja una gran debilidad, pues si la mayoría de trabajadores reconoce que no tiene el equipo necesario, la prevención del ciberdelito se vuelve casi imposible. No basta con la voluntad del personal si no cuentan con las herramientas adecuadas. El hecho de que solo un 6 % diga tener lo necesario demuestra que el sistema está funcionando con carencias graves, lo que limita la efectividad de las acciones y deja mucho espacio para que los ciberdelitos sigan creciendo sin control.

Figura 6

Encuesta aplicada a trabajadores de la Fiscalía del Ciberdelito



Nota: encuesta aplicada a integrantes de la fiscalía de ciberdelito. 2024.

Si se suman las respuestas que afirman que se ha recibido poca capacitación en el tema y que no se ha recibido ninguna capacitación, se puede afirmar que una mayoría calificada opina que la capacitación recibida es escasa.

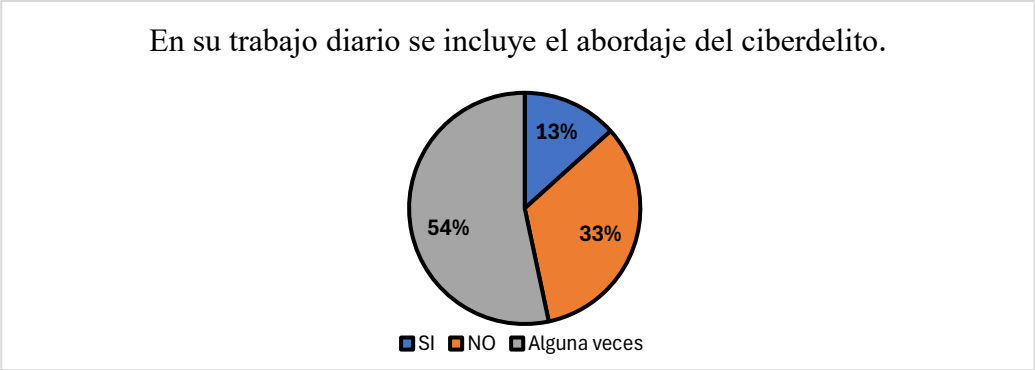
Este resultado deja en claro que la capacitación es una de las grandes debilidades en la atención al ciberdelito. Si la mayoría reconoce que ha recibido poca o ninguna formación, significa que el personal no está preparado para enfrentar un problema que evoluciona muy rápido. Al final, sin conocimiento actualizado, las herramientas que tengan pierden efectividad y las víctimas quedan más desprotegidas.

4.3.2. Ministerio de Gobernación

En el ministerio de gobernación se aplicó el cuestionario a quince trabajadores del cuarto viceministerio de gobernación que se ocupa del tema de Tecnología de la Información y las Comunicaciones.

Figura 7

Encuesta aplicada a trabajadores del Cuarto Vive-Ministerio de Tecnología de la Información y Comunicaciones del Ministerio de Gobernación.

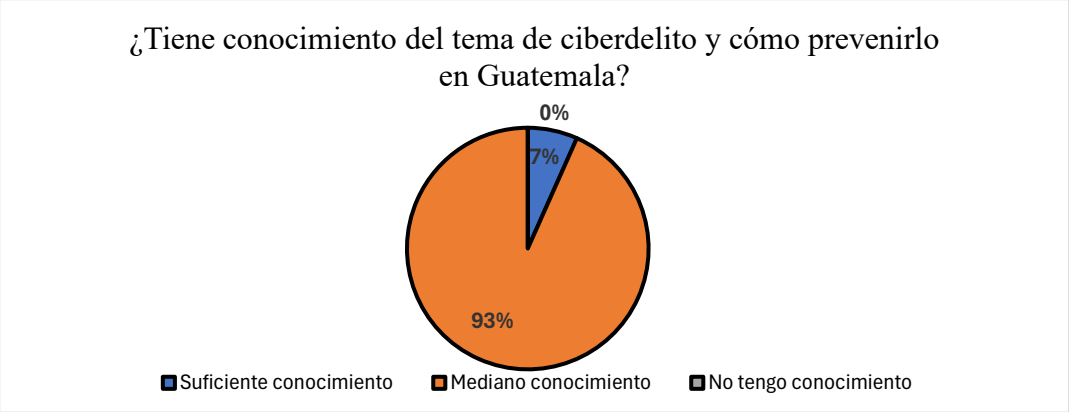


Nota: encuesta aplicada a integrantes del cuarto viceministerio de Tecnología de la Información y las comunicaciones. 2024.

La gráfica evidencia que en un bajo porcentaje se atienden situaciones relacionadas con el ciberdelito. Esta situación resulta alarmante tomando en cuenta que esta es una instancia del Estado de Guatemala responsable directamente de la atención a la amenaza que representa el ciberdelito para la sociedad guatemalteca. Lo que queda claro es la opacidad institucional con la que se está enfrentando una amenaza que afecta o puede llegar a afectar a todas las esferas del Estado.

Figura 8

Encuesta aplicada a trabajadores del Cuarto Vive-Ministerio de Tecnología de la Información y Comunicaciones del Ministerio de Gobernación.



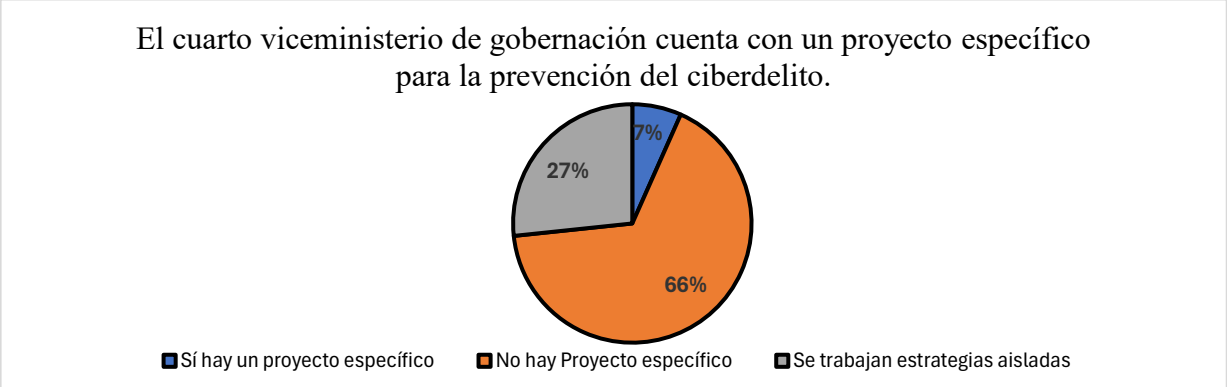
Nota: encuesta aplicada a integrantes del cuarto viceministerio de Tecnología de la Información y las comunicaciones. 2024.

Los datos representados en la gráfica evidencian que una mayoría calificada expresa tener un mediano conocimiento acerca del ciberdelito y cómo prevenirlo. En este caso hay que advertir que el cuarto viceministerio de gobernación trabaja un tema que tiene que ver directamente con ciberseguridad, por lo que sus trabajadores deberían tener un conocimiento suficiente en la materia.

Que la mayoría diga tener solo un "mediano conocimiento" sobre ciberdelito es una señal de alerta. Un conocimiento a medias en un campo tan complejo puede significar respuestas lentas, fallas en la prevención y, en última instancia, mayor vulnerabilidad para la ciudadanía.

Figura 9

Encuesta aplicada a trabajadores del Cuarto Vive-Ministerio de Tecnología de la Información y Comunicaciones del Ministerio de Gobernación.

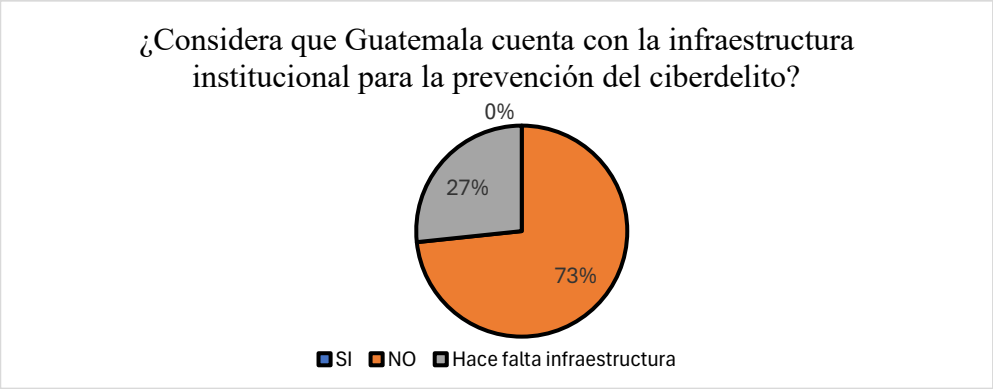


Nota: encuesta aplicada a integrantes del cuarto viceministerio de Tecnología de la Información y las comunicaciones. 2024.

En lo que se refiere a un proyecto específico para la prevención del ciberdelito se puede observar que no existe, más bien se encuentra un 27% de encuestados que afirma que se trabajan estrategias aisladas.

Figura 10

Encuesta aplicada a trabajadores del Cuarto Vive-Ministerio de Tecnología de la Información y Comunicaciones del Ministerio de Gobernación.

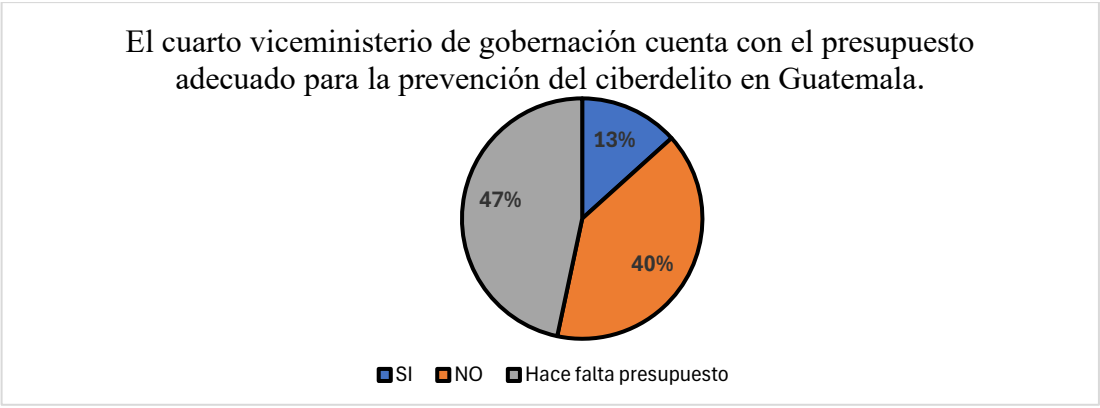


Nota: encuesta aplicada a integrantes del cuarto viceministerio de Tecnología de la Información y las comunicaciones. 2024.

Una mayoría calificada de trabajadores que respondieron el cuestionario afirma que Guatemala no cuenta con la infraestructura institucional para la prevención del ciberdelito situación que pone al país en un estado de alta vulnerabilidad.

Figura 11

Encuesta aplicada a trabajadores del Cuarto Vive-Ministerio de Tecnología de la Información y Comunicaciones del Ministerio de Gobernación.



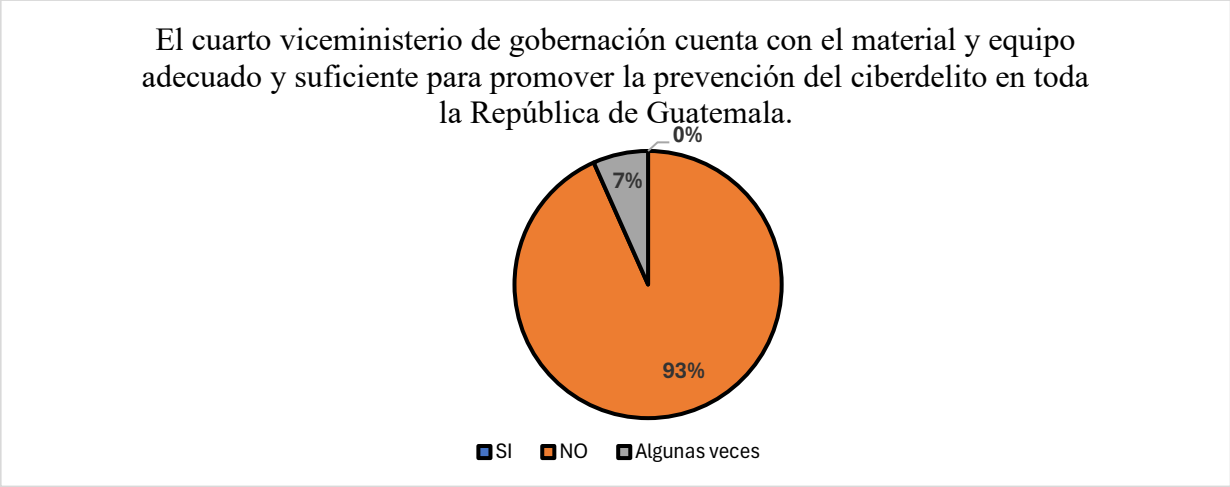
Nota: encuesta aplicada a integrantes del cuarto viceministerio de Tecnología de la Información y las comunicaciones. 2024.

En lo que se refiere al tema de presupuesto también se puede observar la existencia de respuestas que reflejan la falta de un presupuesto que permita hacerle frente de forma más eficiente al ciberdelito en Guatemala.

La falta de presupuesto para enfrentar el ciberdelito en Guatemala es un problema serio, porque sin recursos no se pueden mejorar equipos, capacitar al personal ni brindar una atención adecuada a las víctimas. Esto deja al país en una posición débil frente a un fenómeno que avanza rápido y que exige inversiones constantes para estar un paso adelante.

Figura 12

Encuesta aplicada a trabajadores del Cuarto Vive-Ministerio de Tecnología de la Información y Comunicaciones del Ministerio de Gobernación.



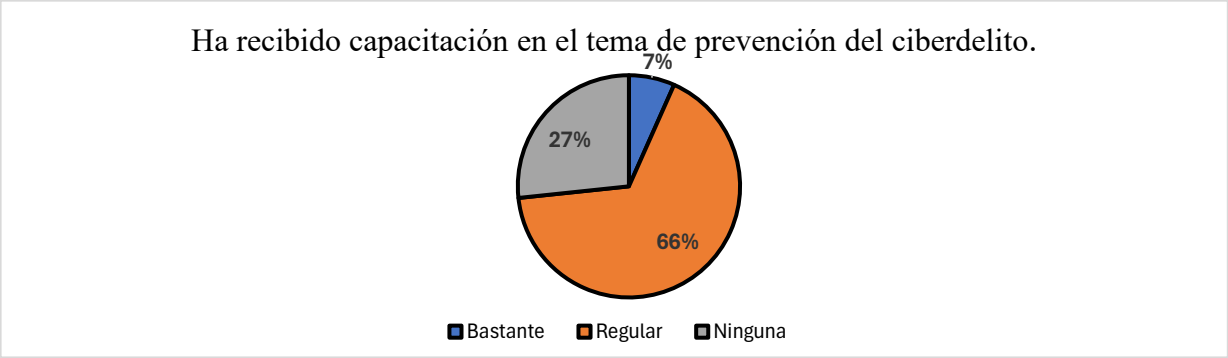
Nota: encuesta aplicada a integrantes del cuarto viceministerio de Tecnología de la Información y las comunicaciones. 2024.

Esta gráfica evidencia que casi la totalidad de encuestados opina que no se cuenta con suficiente material y equipo para la atención del ciberdelito.

El hecho de que casi todos los encuestados digan que no hay suficiente material ni equipo para atender el ciberdelito muestra una gran debilidad institucional. Si no se cuenta con lo básico, es difícil esperar una respuesta efectiva, lo que deja a las víctimas desprotegidas y al sistema rezagado.

Figura 13

Encuesta aplicada a trabajadores del Cuarto Vive-Ministerio de Tecnología de la Información y Comunicaciones del Ministerio de Gobernación.



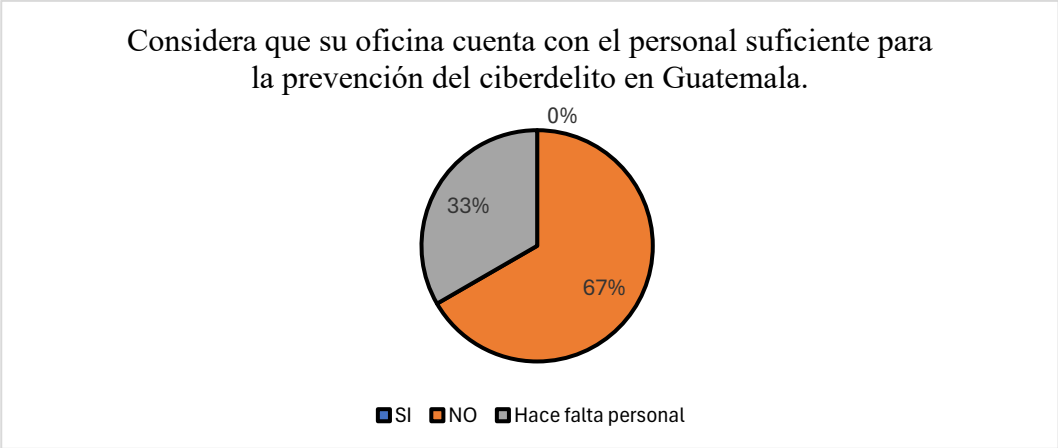
Nota: encuesta aplicada a integrantes del cuarto viceministerio de Tecnología de la Información y las comunicaciones. 2024.

En el aspecto de capacitación en el tema de ciberdelito, si se suma el porcentaje de quienes opinan que ha sido regular y los que expresan que no han recibido ningún adiestramiento se puede inferir que hace falta mucha capacitación para contar con personal especializado en ciberdelito que sea garantía para brindar una atención con el espectro e impacto que se necesita en Guatemala.

La suma de quienes dicen haber recibido capacitación solo “regular” o nada deja claro que el país no cuenta con suficiente personal realmente especializado en ciberdelito. Esto es preocupante, porque sin formación adecuada no hay forma de dar una atención seria y efectiva. En pocas palabras, Guatemala necesita invertir más en preparar a su gente si quiere enfrentar este reto con resultados reales.

Figura 14

Encuesta aplicada a trabajadores del Cuarto Vive-Ministerio de Tecnología de la Información y Comunicaciones del Ministerio de Gobernación.



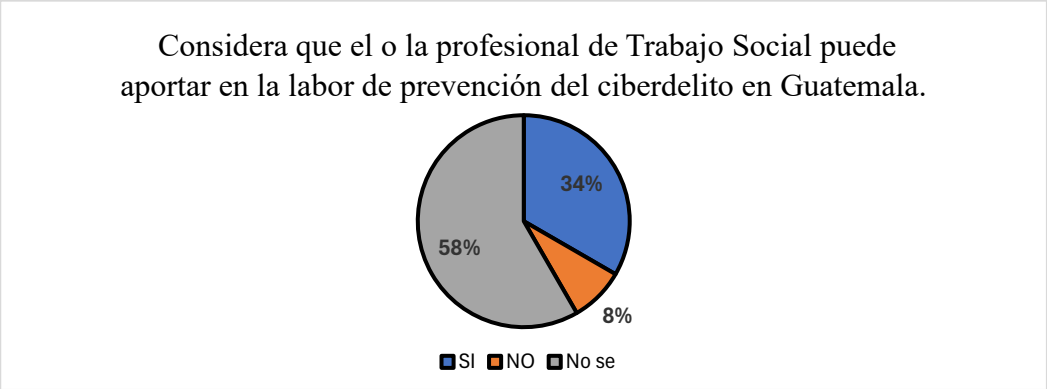
Nota: encuesta aplicada a integrantes del cuarto viceministerio de Tecnología de la Información y las comunicaciones. 2024.

La mayoría de trabajadores considera que el personal que trabaja en atención al ciberdelito es insuficiente, lo que hace pensar que no se está brindando la atención adecuada para mitigar la amenaza que representa el ciberdelito en el país.

La mayoría de los trabajadores considera que el personal es insuficiente y refleja un problema claro siendo este que no hay suficiente gente para atender los casos de ciberdelito de manera efectiva. Esto significa que muchas situaciones quedan desatendidas o se manejan con retrasos, dejando a las víctimas más expuestas y al país con una capacidad limitada para enfrentar estas amenazas digitales.

Figura 15

Encuesta aplicada a trabajadores del Cuarto Vive-Ministerio de Tecnología de la Información y Comunicaciones del Ministerio de Gobernación.



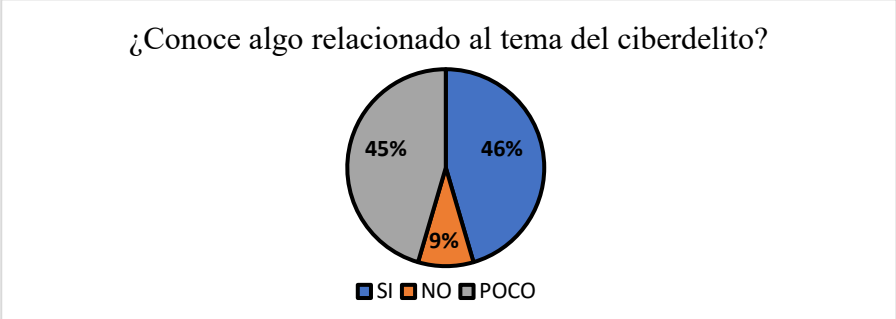
Nota: encuesta aplicada a integrantes del cuarto viceministerio de Tecnología de la Información y las comunicaciones. 2024.

Las respuestas que se ven reflejadas en la gráfica muestran que la mayoría de trabajadores a los que se les aplicó el cuestionario no sabe si el Trabajo Social puede coadyuvar en la tarea de prevención del ciberdelito. Esta situación puede obedecer a que no conocen la profesión de Trabajo Social por lo tanto no se animaron a emitir opinión al respecto.

4.3.3. Secretaria contra la Violencia Sexual, Explotación y Trata de Personas SVET

Figura 16

Encuesta aplicada a trabajadores de la Secretaría contra la Violencia Sexual

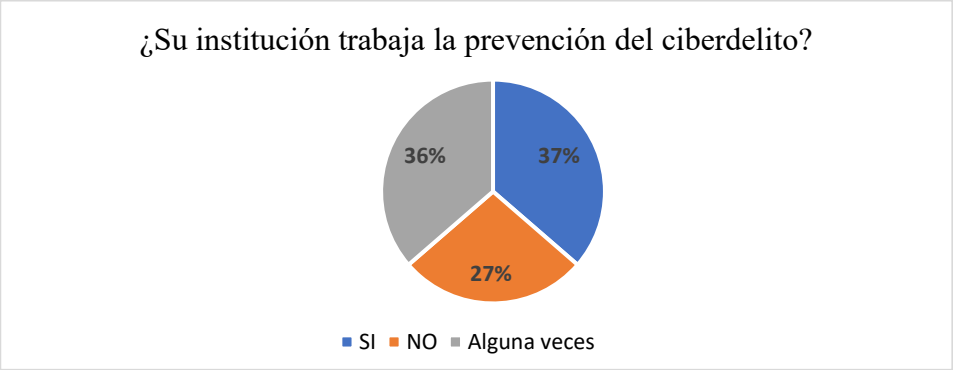


Nota: encuesta aplicada a trabajadores de la Secretaría contra la Violencia Sexual, Explotación y Trata de Personas. SVET. 2024.

Observando la respuesta que dieron trabajadores de SVET se puede decir que también se refleja cierto nivel de desconocimiento del tema de ciberdelito. Con estos datos ya serían dos instituciones nacionales que tienen dentro de sus responsabilidades la atención del ciberdelito, pero no tienen el conocimiento que se necesita para brindar una atención eficiente.

Figura 17

Encuesta aplicada a trabajadores de la Secretaría contra la Violencia Sexual



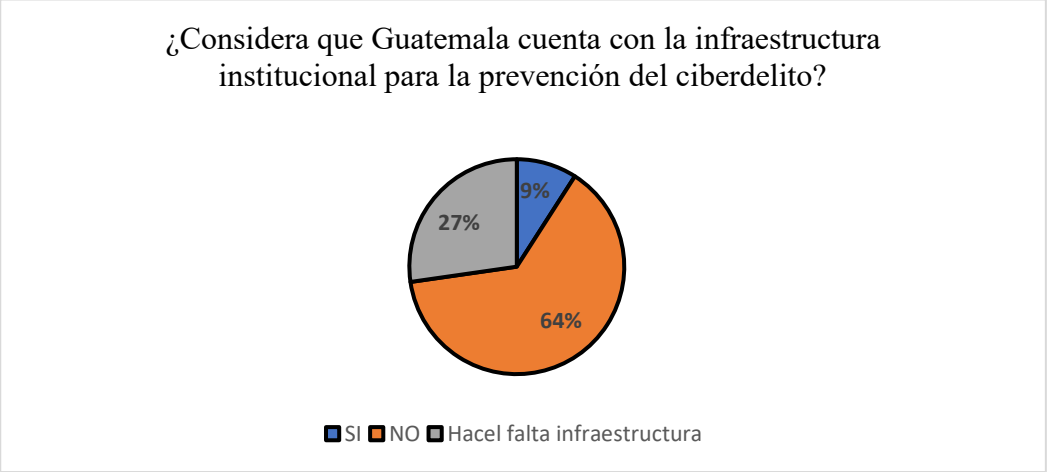
Nota: encuesta aplicada a trabajadores de la Secretaría contra la Violencia Sexual, Explotación y Trata de Personas. SVET. 2024.

De acuerdo a la opinión de los(as) trabajadores(as) que respondieron el cuestionario se trabaja muy poco lo que es la prevención del ciberdelito.

Si los trabajadores opinan que se hace muy poco en prevención del ciberdelito, eso muestra una falla importante en la estrategia del país. No basta con reaccionar a los delitos cundo estos ocurren; la prevención es clave para reducir riesgos, educar a la población y evitar que los casos se multipliquen. Sin esfuerzos claros en esta área, el sistema sigue jugando a ponerse al día en lugar de anticiparse.

Figura 18

Encuesta aplicada a trabajadores de la Secretaría contra la Violencia Sexual



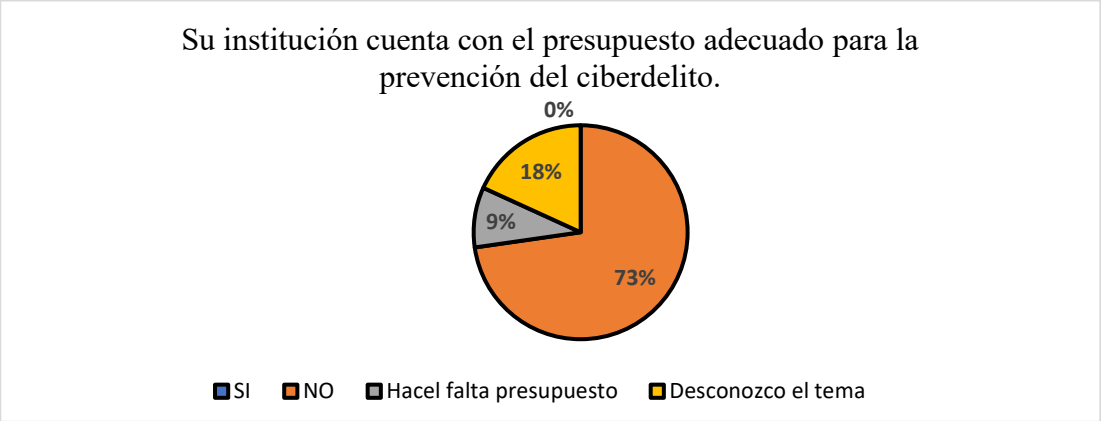
Nota: encuesta aplicada a trabajadores de la Secretaría contra la Violencia Sexual, Explotación y Trata de Personas. SVET. 2024.

Al igual que las otras instituciones en las que se aplicó el cuestionario en SVET opinan que Guatemala no cuenta con la infraestructura institucional suficiente para trabajar en la prevención del delito.

Que en SVET coincidan con otras instituciones en que Guatemala no tiene la infraestructura suficiente para prevenir el delito deja en evidencia una debilidad estructural del país. Sin instalaciones, equipos y recursos adecuados, cualquier esfuerzo de prevención se queda corto y las acciones terminan siendo reactivas en lugar de proactivas.

Figura 19

Encuesta aplicada a trabajadores de la Secretaría contra la Violencia Sexual

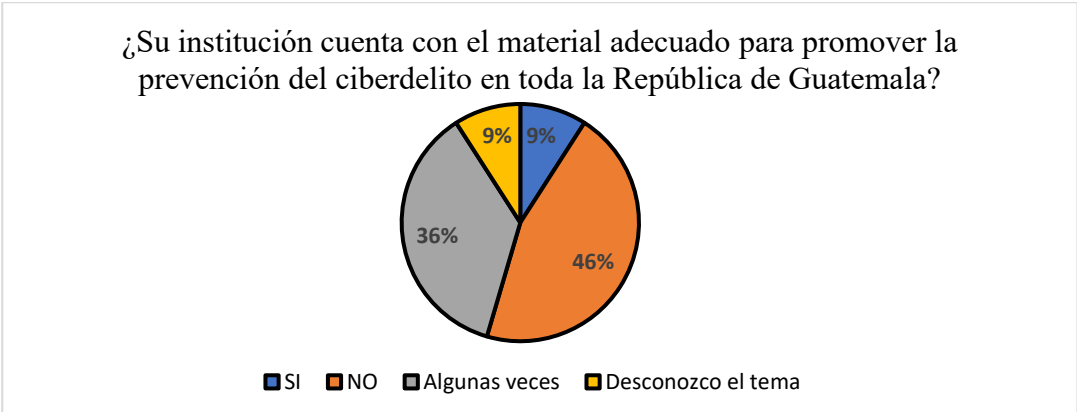


Nota: encuesta aplicada a trabajadores de la Secretaría contra la Violencia Sexual, Explotación y Trata de Personas. SVET. 2024.

Sin recursos económicos, es muy difícil implementar estrategias efectivas de prevención del delito. Esto limita la capacidad de la institución para capacitar personal, adquirir equipos y desarrollar programas, dejando al país más vulnerable frente a las amenazas delictivas.

Figura 20

Encuesta aplicada a trabajadores de la Secretaría contra la Violencia Sexual



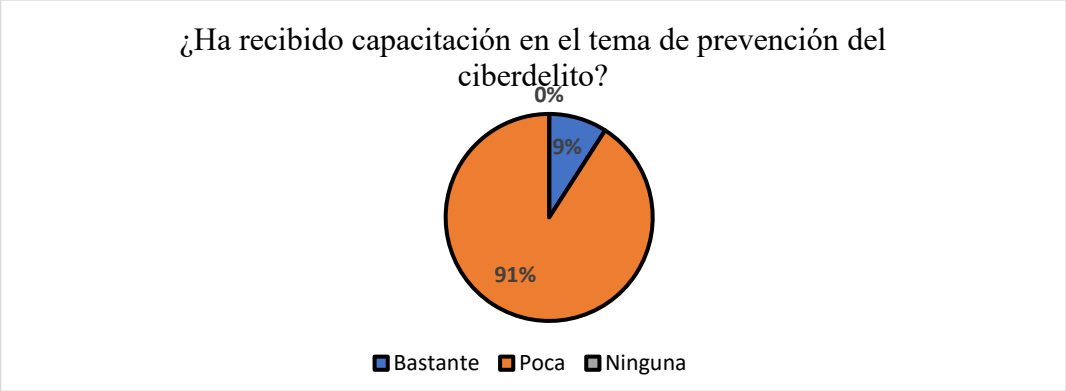
Nota: encuesta aplicada a trabajadores de la Secretaría contra la Violencia Sexual, Explotación y Trata de Personas. SVET. 2024.

Interpretando los datos reflejados en la gráfica cuenta con muy poco material para trabajar la prevención del ciberdelito a nivel nacional.

La gráfica muestra que se cuenta con muy poco material para prevenir el ciberdelito a nivel nacional, también evidencia una limitación importante. Sin herramientas adecuadas, los esfuerzos de prevención se ven debilitados, la capacidad de respuesta se reduce y el país queda más expuesto a los riesgos digitales.

Figura 21

Encuesta aplicada a trabajadores de la Secretaría contra la Violencia Sexual



Nota: encuesta aplicada a trabajadores de la Secretaría contra la Violencia Sexual, Explotación y Trata de Personas. SVET. 2024.

Uno de los renglones en los que SVET necesita capacitación es en el tema de prevención del ciberdelito. La gráfica evidencia que es muy poca la capacitación revivida en este tema.

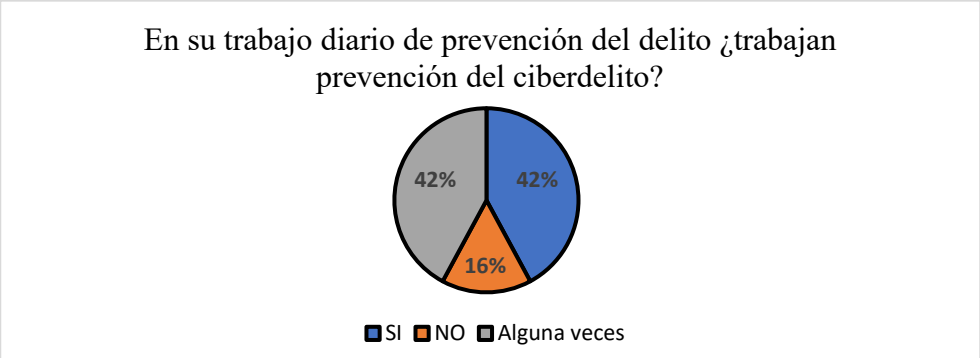
La gráfica deja claro que en SVET hace falta capacitación en prevención del ciberdelito. Esto es preocupante, porque sin formación adecuada el personal no puede anticiparse a los riesgos ni implementar estrategias efectivas.

4.3.4. Policía Nacional Civil

Cuestionario aplicado a diez y nueve trabajadores de Subdirección General de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala.

Figura 22

Encuesta aplicada a trabajadores de Subdirección General de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala.

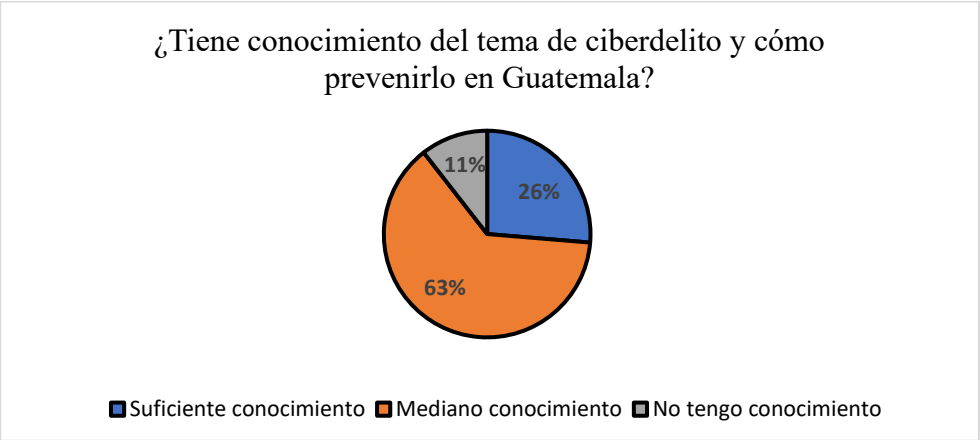


Nota: encuesta aplicada a integrantes de Subdirección General de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala. 2024.

Se puede observar que el ciberdelito no ocupa el lugar de importancia que debe tener en la Subdirección de Prevención del Delito y Cibercrimen de la Policía Nacional Civil. Si se toma en cuenta la constante vulnerabilidad que existe ante el ciberdelito se debería de tener un programa y personal específico para la atención a este flagelo por parte de la Policía Nacional Civil.

Figura 23

Encuesta aplicada a trabajadores de Subdirección General de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala.



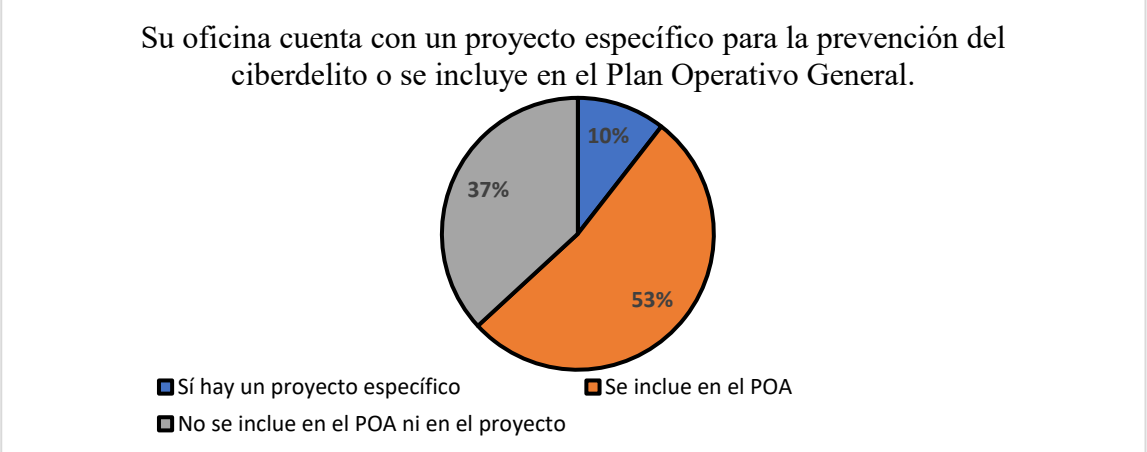
Fuente: encuesta aplicada a integrantes de Subdirección General de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala. 2024.

Es preocupante observar que la mayoría de personal de la Policía Nacional Civil encargado directamente de la atención al cibercrimen tienen un mediano conocimiento del ciberdelito y más aún cuando aparte de esta mayoría referida existe otro porcentaje significativo que no tiene ningún conocimiento del ciberdelito.

El hecho de que gran parte del personal de la PNC solo tenga un conocimiento medio sobre ciberdelito y que además haya un grupo que no tiene ningún conocimiento es alarmante. Se trata de la institución llamada a dar la primera respuesta frente a estos crímenes, pero con esa falta de preparación se limita seriamente su capacidad de acción y se deja en evidencia una brecha que podría ser aprovechada por los delincuentes.

Figura 24

Encuesta aplicada a trabajadores de Subdirección General de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala.



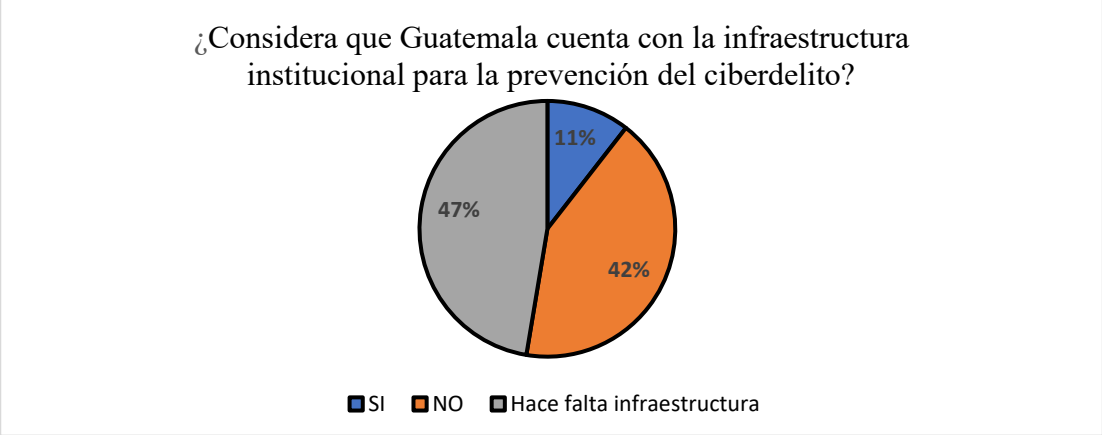
Fuente: encuesta aplicada a integrantes de Subdirección General de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala. 2024.

Como se puede observar las respuestas proporcionadas evidencian contradicción lo que refleja que no hay claridad en cuanto a la forma efectiva de combatir el cibercrimen en la Subdirección General de la Policía Nacional Civil encargada directamente de esta importante y urgente tarea.

La contradicción en las respuestas muestra un problema serio: dentro de la propia Subdirección de la PNC no hay una visión clara ni unificada sobre cómo enfrentar el cibercrimen. Esta falta de claridad no solo genera confusión interna, sino que también debilita la efectividad de la institución frente a una amenaza que requiere estrategias precisas y coordinadas.

Figura 25

Encuesta aplicada a trabajadores de Subdirección General de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala.



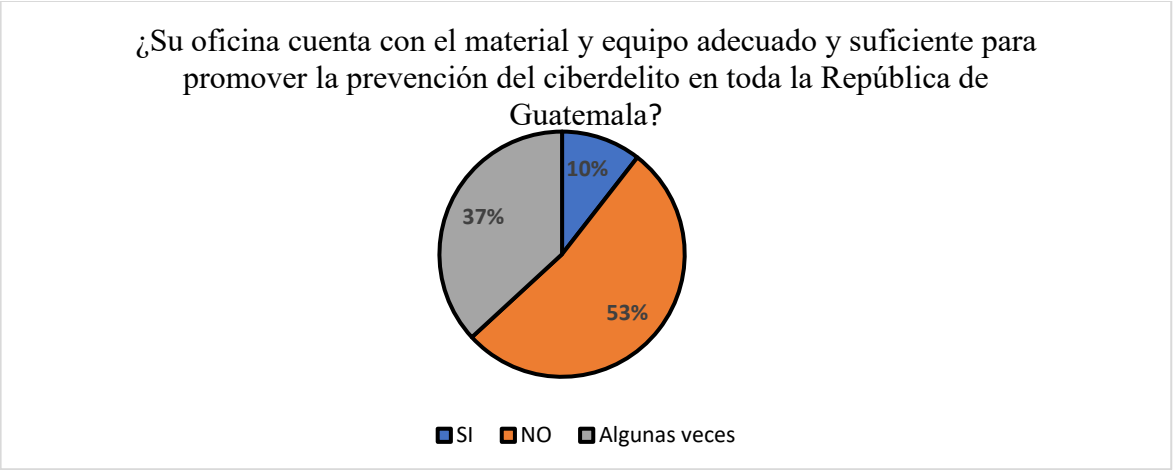
Nota: encuesta aplicada a integrantes de Subdirección General de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala. 2024.

Casi la totalidad de los entrevistados expresan dos opiniones negativas, la primera es que en Guatemala hace falta infraestructura institucional para la prevención del ciberdelito y la segunda es que definitivamente no se cuenta con la infraestructura institucional necesaria.

Cabe mencionar que, casi todos los entrevistados coincidan en señalar la falta de infraestructura institucional para prevenir el ciberdelito deja en evidencia una gran debilidad del país. No se trata solo de una carencia técnica, sino de una señal de que el tema no ha sido prioridad. Sin bases sólidas, cualquier esfuerzo de prevención queda corto y poco efectivo.

Figura 26

Encuesta aplicada a trabajadores de Subdirección General de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala.



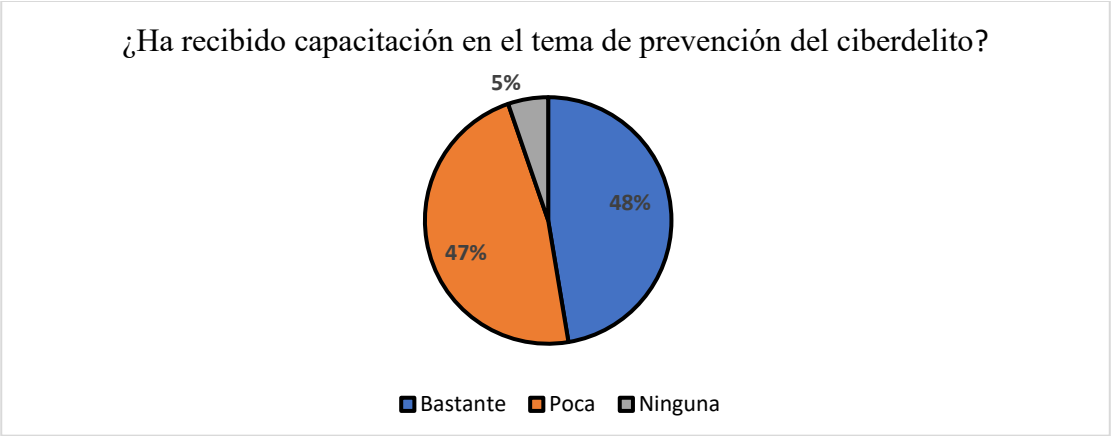
Fuente: encuesta aplicada a integrantes de Subdirección General de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala. 2024.

Esta gráfica también muestra opiniones poco alentadoras en cuanto a que no se cuenta con el material y equipo idóneo para la prevención del ciberdelito. Esta situación debe preocupar tomando en cuenta que de esta forma se incrementa el riesgo y la vulnerabilidad de la población guatemalteca.

La falta de material y equipo adecuado para prevenir el ciberdelito es una alerta seria: sin herramientas idóneas, la respuesta siempre será limitada. Esto no solo afecta la capacidad de acción de las instituciones, sino que deja a la población en una posición mucho más vulnerable frente a estas amenazas crecientes.

Figura 27

Encuesta aplicada a trabajadores de Subdirección General de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala.



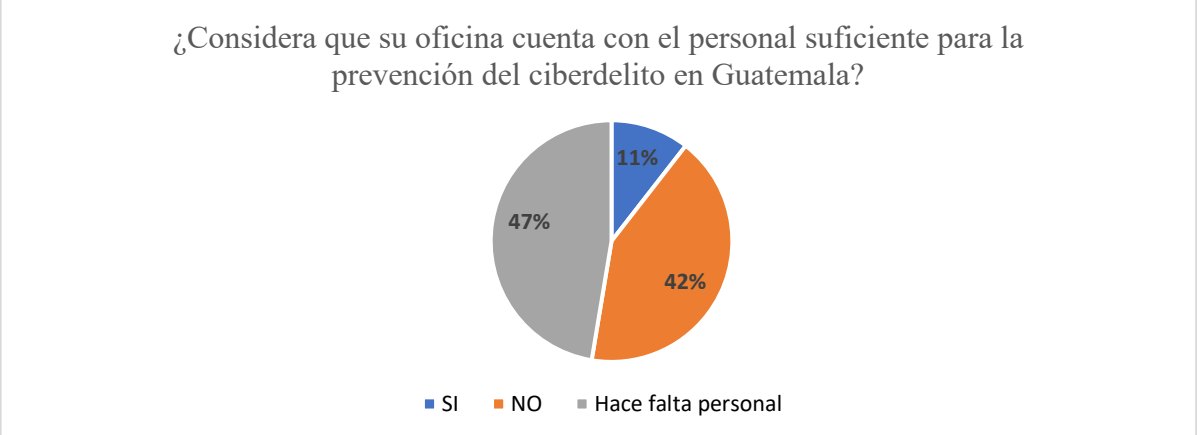
Nota: encuesta aplicada a integrantes de Subdirección General de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala. 2024.

La mayoría del personal de la Subdirección de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala manifiesta haber recibido poca o ninguna capacitación en materia de prevención del ciberdelito.

La mayoría del personal encargado de prevenir el ciberdelito tiene poca o nula capacitación y eso es un problema grave. Pues es de entender que, si quienes deben liderar la respuesta no cuentan con la preparación necesaria, por ende las consecuencias de los delitos quedan más expuestos a estos delitos que crecen cada día.

Figura 28

Encuesta aplicada a trabajadores de Subdirección General de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala.



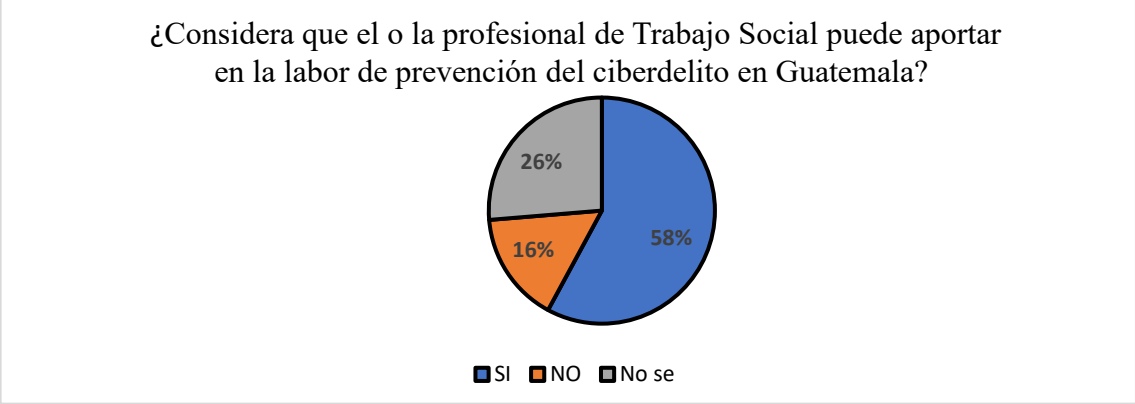
Nota: encuesta aplicada a integrantes de Subdirección General de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala. 2024.

Asimismo, se puede observar que la mayoría del personal entrevistado expresa que que hace falta personal debido a que se hace evidente que el personal actual resulta insuficiente ante el volumen de la demanda.

Que la mayoría señale que el personal es insuficiente deja claro que el problema no es solo de recursos materiales, sino también de recurso humano. Si no hay suficiente personal para atender la demanda, el esfuerzo se vuelve limitado y la capacidad de respuesta frente al ciberdelito queda muy por debajo de lo que realmente se necesita.

Figura 29

Encuesta aplicada a trabajadores de Subdirección General de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala.



Nota: encuesta aplicada a integrantes de Subdirección General de Prevención del Delito y Cibercrimen de la Policía Nacional Civil de Guatemala. 2024.

La mayoría del personal encuestado opina que el o la profesional de Trabajo Social si puede aportar en materia de prevención del ciberdelito en Guatemala.

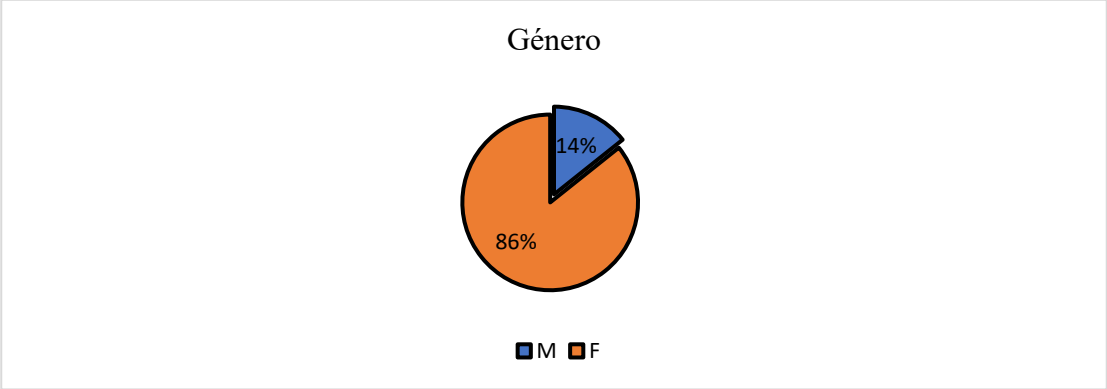
En la presente encuesta el personal reconoce el aporte del Trabajo Social en la prevención del ciberdelito es un punto positivo, ya que refleja la apertura a enfoques más integrales. Sin embargo, esto también evidencia que aún falta darles el espacio y las herramientas necesarias a los profesionales de esta área para que su aporte no se quede solo en la teoría, sino que tenga un impacto real en la práctica.

4.3.5. Trabajadores Sociales

A continuación, se presentan las respuestas proporcionadas por 35 Trabajadores Sociales que desempeñan su ejercicio profesional en diferentes escenarios de la vida nacional guatemalteca.

Figura 30

Encuesta aplicada a profesionales en Trabajo Social

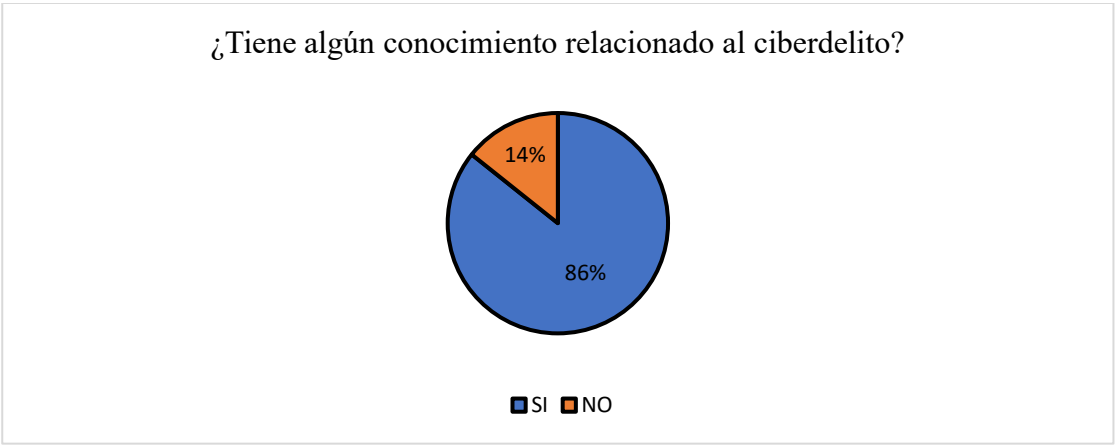


Nota: encuesta aplicada Trabajadores Sociales de Guatemala. 2024.

La mayoría de los Trabajadores que respondieron el cuestionario elaborado para levantar la información fueron del género femenino. Esta situación podría representar una esperanza alentadora si se toma en cuenta que la mujer representa un rol formador de conductas desde el hogar que puede perfectamente coadyuvar a concientizar, desde el mismo núcleo de la sociedad, sobre la grave amenaza que representa el ciberdelito.

Figura 31

Encuesta aplicada a profesionales en Trabajo Social



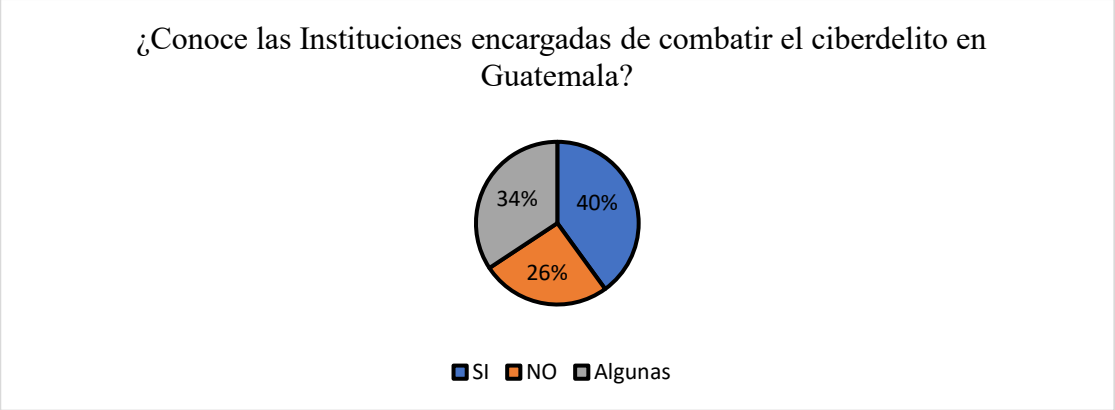
Nota: encuesta aplicada Trabajadores Sociales de Guatemala. 2024.

La mayoría de Trabajadoras Sociales que respondieron el cuestionario manifestaron si tener conocimiento en relación al tema del ciberdelito, lo que podría significar que es una profesión que representa un campo fértil para convertirse en un buen aliado en la prevención del ciberdelito en Guatemala.

Que la mayoría de trabajadoras sociales afirmen tener conocimiento sobre el ciberdelito muestra un punto de partida muy valioso. Esto abre la puerta para que la profesión se convierta en un aliado estratégico en la prevención, siempre y cuando se refuercen esas bases con capacitación constante y recursos que permitan transformar ese conocimiento en acciones efectivas.

Figura 32

Encuesta aplicada a profesionales en Trabajo Social



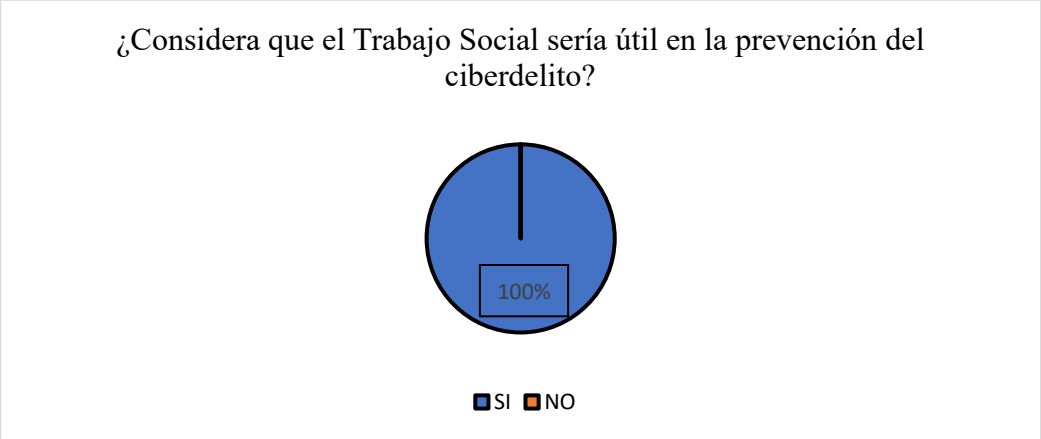
Nota: encuesta aplicada Trabajadores Sociales de Guatemala. 2024.

La mayoría de respuestas indican que hay un conocimiento general, de Instituciones que tratan con el ciberdelito, por parte de las trabajadoras sociales.

El hecho de que las trabajadoras sociales tengan un conocimiento general sobre las instituciones que atienden el ciberdelito es positivo, pero también deja ver que ese conocimiento es básico. Para que realmente puedan aportar en la prevención, hace falta profundizar y fortalecer esa relación con dichas instituciones, de lo contrario se corre el riesgo de que quede en un simple dato teórico y no en una herramienta práctica.

Figura 33

Encuesta aplicada a profesionales en Trabajo Social



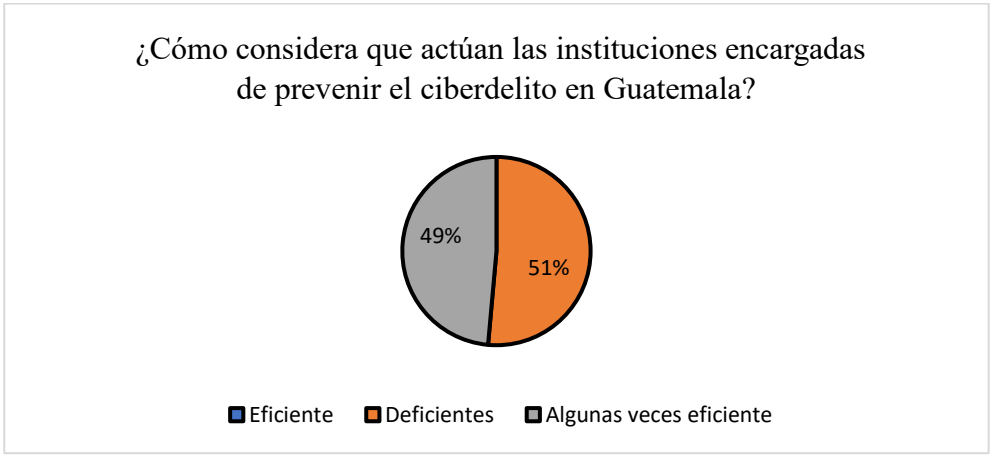
Nota: encuesta aplicada Trabajadores Sociales de Guatemala. 2024.

La totalidad de las encuestadas considera que el Trabajo Social es una profesión que si resultaría útil en el trabajo arduo de la prevención del ciberdelito a nivel nacional.

Que todas las encuestadas coincidan en que el Trabajo Social sería útil en la prevención del ciberdelito refleja un consenso fuerte y esperanzador. Sin embargo, la utilidad real dependerá de que se les dé espacio, capacitación y recursos para participar activamente; de lo contrario, esa idea quedará solo en el papel y no en acciones concretas.

Figura 34

Encuesta aplicada a profesionales en Trabajo Social



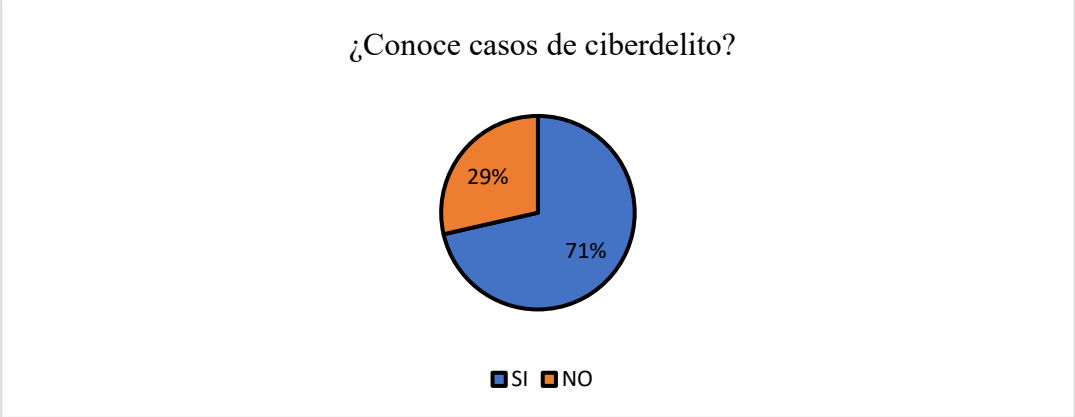
Fuente: encuesta aplicada Trabajadores Sociales de Guatemala. 2024.

La totalidad de Trabajadoras Sociales que respondieron el cuestionario expresaron que la actuación de las Instituciones encargadas de la atención del ciberdelito en Guatemala es deficiente y en algunas oportunidades eficiente.

Las trabajadoras sociales coinciden en que la actuación de las instituciones frente al ciberdelito es deficiente dice mucho: hay una percepción generalizada de que no se está respondiendo como debería. Que solo en algunas ocasiones se considere eficiente muestra que el esfuerzo existe, pero es aislado y no constante, lo cual limita el impacto real en la prevención y atención de este problema.

Figura 35

Encuesta aplicada a profesionales en Trabajo Social



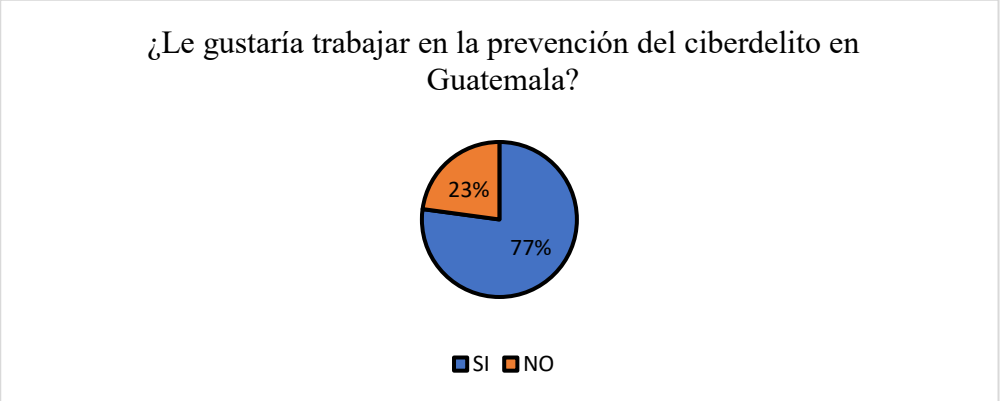
Nota: encuesta aplicada Trabajadores Sociales de Guatemala. 2024.

La mayoría de las encuestadas respondió que, si conoce casos de ciberdelitos cometidos, lo que resulta lógico debido a que su trabajo profesional lo desempeñan en las diferentes comunidades de la República de Guatemala.

Que la mayoría de las encuestadas conozca casos de ciberdelitos no sorprende, porque al trabajar directamente en comunidades están en contacto con la realidad cotidiana de la gente. Esto confirma que el ciberdelito ya no es un tema lejano o exclusivo de ciertos sectores, sino un problema que afecta de manera directa a la población en distintos contextos del país.

Figura 36

Encuesta aplicada a profesionales en Trabajo Social

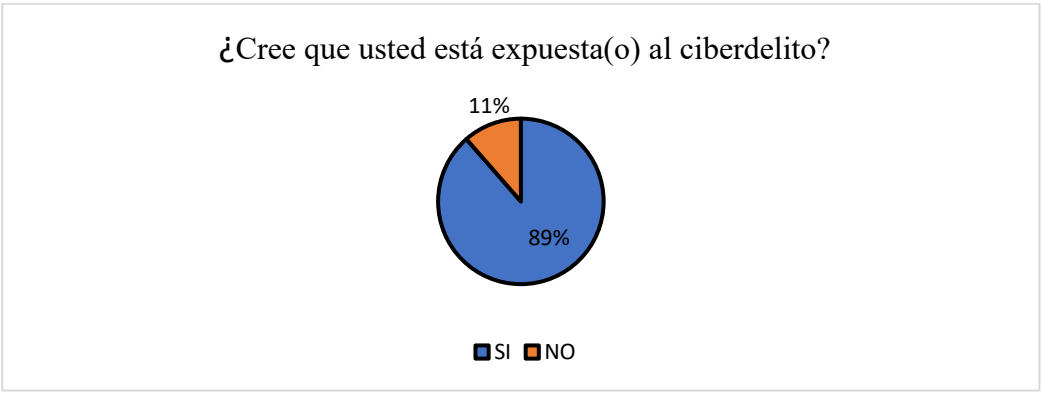


Nota: encuesta aplicada Trabajadores Sociales de Guatemala. 2024.

Es positivo ver que la mayoría de las encuestadas estén dispuestas a involucrarse en la prevención del ciberdelito, ya que refleja que reconocen cómo su profesión puede aportar en este campo. Esto abre la puerta a un trabajo interdisciplinario que fortalezca la respuesta institucional, aunque claro, esa disposición necesita traducirse en oportunidades reales de formación y acción para que no se quede solo en intención.

Figura 37

Encuesta aplicada a profesionales en Trabajo Social



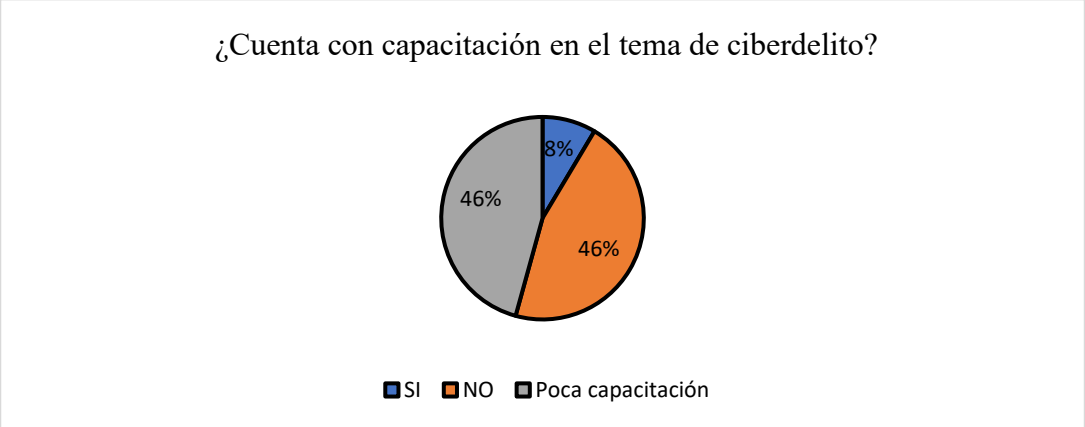
Nota: encuesta aplicada Trabajadores Sociales de Guatemala. 2024.

El hecho de que las y los Trabajadores Sociales reconozcan al ciberdelito como una amenaza seria ya es un paso importante, porque muestra conciencia sobre la magnitud del problema. Sin embargo, ese reconocimiento también deja en evidencia que el país va tarde en

reaccionar: mientras el ciberdelito evoluciona y se diversifica, las instituciones aún no logran armar estrategias sólidas para enfrentarlo. En otras palabras, la alarma está encendida, pero la respuesta sigue siendo lenta.

Figura 38

Encuesta aplicada a profesionales en Trabajo Social



Nota: encuesta aplicada Trabajadores Sociales de Guatemala. 2024.

La respuesta a esta pregunta que se planteó en el cuestionario aplicado demuestra la falta de orientación que hay respecto del ciberdelito. Si se analiza que este segmento de profesionales del Trabajo Social no cuenta con capacitación sobre un tema que les puede llegar a afectar gravemente de forma directa, hay que pensar en la mayoría de la población guatemalteca cuyo nivel educativo no es el adecuado y por lo tanto no tienen acceso a capacitación en temas tan específicos como el de prevención del ciberdelito.

Conclusiones

El ciberdelito ha venido a constituirse en una amenaza transnacional que está afectando a las poblaciones de diferentes regiones del mundo. Este fenómeno encuentra su principal caldo de cultivo en Estados con democracias débiles como Guatemala en donde los sistemas de justicia no cuentan con la calidad, cobertura y pertinencia cultural necesaria para garantizar una aplicación de la ley que sea pronta y efectiva para garantizar un buen nivel de seguridad a las(os) cibernautas que utilizan el ciberespacio en actividades laborales, educativas, familiares y de entretenimiento.

Se ha detectado que entre los segmentos sociales afectados por el ciberdelito se encuentran los grupos que históricamente se han mostrado vulnerables: mujer, niñez, adulto mayor, población indígena, personas con capacidades diferentes, entre otros.

Se ha logrado identificar la importancia que tiene la profesión de Trabajo Social en el tema de prevención del ciberdelito. Las diferentes estrategias, metodologías, prácticas y modelos de intervención que desarrolla el Trabajo Social a nivel profesional resultan perfectamente útiles para realizar procesos de capacitación y orientación que concienticen a los diferentes grupos sociales de la amenaza que representa el ciberdelito y las formas que existen para prevenirlo.

A pesar que Guatemala ya cuenta con algunas leyes e instancias institucionales encargadas de prevenir y sancionar el ciberdelito, aún falta mucho por hacer para contar con una infraestructura institucional y un sistema jurídico solido que garantice de mejor manera la seguridad en el ciberespacio especialmente en el territorio nacional. El déficit del Estado en esta materia es alarmante debido a que día a día las cifras de víctimas se incrementan y la brecha de inseguridad cada vez se hace mayor.

Se pudo identificar el criterio de Actores nacionales que tienen relación directa con el ciberdelito, derivado de lo cual se puede percibir la fragilidad del Estado de Guatemala frente al ciberdelito. Desde instituciones que no cuentan con los recursos necesarios hasta personal insuficiente y poco capacitado hacen de Guatemala un territorio fértil para la comisión de ciberdelitos de la más diversa índole con los efectos nefastos propios de este tipo de amenazas.

Referencias

ACNUR. (2024). *Informe anual 2024*. Alto Comisionado de las Naciones Unidas para los Refugiados.

Álvarez, J., & Hernández, M. (2021). *Estudio sobre el impacto del ciberacoso en adolescentes guatemaltecos*. Revista de Psicología Social, 15(2), 45-60.

Álvarez, J., & Hernández, M. (2020). *Análisis de la legislación guatemalteca en materia de ciberdelitos*. Editorial Jurídica Centroamericana.

Álvarez Idarriaga, R. (2015). *La protección de datos personales en el entorno digital*. Universidad de San Carlos de Guatemala.

Amnistía Internacional. (2019). *Informe sobre derechos humanos en el ciberespacio*. Amnistía Internacional.

Anderson, R., Barton, C., & Brown, D. (2019). *Ciberseguridad: Retos y soluciones*. Editorial Tecnológica.

Barreno Castillo, R. (2022, 2 de mayo). Los ciberdelítos van en aumento y la PNC cambia estrategia para investigarlos. Prensa Libre.

Bermúdez, L. (2018). *La importancia de la educación digital en la prevención del ciberacoso*. Revista de Educación y Tecnología, 22(1), 58-72.

BLP Legal. (2022). *Análisis de la ley de protección de datos personales en Guatemala*. Diario Oficial, 2023.

Carrillo, J. (2020). *El papel del trabajo social en la prevención del ciberacoso*. Editorial Universitaria.

Carter, S., & Hughes, T. (2020). *Ciberdelitos: Prevención y respuesta institucional*. Editorial Académica.

CEJA. (2022). *Informe sobre justicia digital en América Latina*. Centro de Estudios Judiciales de América Latina.

Centro Nacional de Ciberseguridad. (2023). *Estrategia nacional de ciberseguridad 2023*. Gobierno de Guatemala.

CEPAL. (2019). *Desafíos digitales en América Latina y el Caribe*. Comisión Económica para América Latina y el Caribe.

CITEL. (2023). *Políticas públicas en ciberseguridad en América Latina*. Comisión Interamericana de Telecomunicaciones.

Comisión Internacional de Juristas [CIJ]. (2019). *Derechos humanos en el ciberespacio*. Comisión Internacional de Juristas.

Comité Internacional de la Cruz Roja. (2018). *Ciberseguridad y derechos humanos*. Comité Internacional de la Cruz Roja.

Computación. (2017). *Manual de seguridad informática*. Editorial Técnica.

Confidencial, E. (2023). *Análisis de la situación del ciberacoso en Guatemala*. Diario Confidencial.

Congreso de la República de Guatemala. (2006). *Ley de protección de datos personales*. Congreso de la República de Guatemala.

Congreso de la República de Guatemala. (2023). *Reformas a la ley de ciberdelitos*. Congreso de la República de Guatemala.

Congreso Panamericano de Trabajo Social. (1957). *Declaración de principios del trabajo social*. Congreso Panamericano de Trabajo Social.

Consejo de Europa. (2001). *Convención sobre cibercriminalidad*. Consejo de Europa.

Consejo de Europa. (2001). *Recomendación sobre protección de datos personales*. Consejo de Europa.

Conseyu de la Xusticia d´Asturies. (2019). *Informe sobre derechos digitales en Asturias*. Conseyu de la Xusticia d´Asturies.

Constitución Política de la República de Guatemala. (Mayo de 1985). *Constitución Política de la República de Guatemala*. Tipografía Nacional.

Council of Europe. (2001). *Convention on Cybercrime*. Council of Europe.

CPRG. (2022). *Reformas constitucionales en Guatemala*. Congreso de la República de Guatemala.

CRPG. (1985). *Constitución Política de la República de Guatemala*. Tipografía Nacional.

Cunningham, J., & Kent, L. (2021). *Análisis de políticas públicas en ciberseguridad*. Editorial Académica.

Del Águila, R. (2019). *Ciberseguridad en el sector público guatemalteco*. Revista de Administración Pública, 18(3), 34-49.

Española, R. (2020). *Educación digital en el contexto latinoamericano*. Editorial Universitaria.

European Union. (2016). *Reglamento General de Protección de Datos*. Unión Europea.

Europol. (2021). *Informe sobre ciberdelitos en Europa*. Europol.

Fernández, M. (2018). *Ciberacoso: Prevención y respuesta*. Editorial Psicológica.

Fernández, M. (2018). *Ciberacoso: Prevención y respuesta*. Editorial Psicológica.

Fondo Monetario Internacional. (2018). *Impacto económico de los ciberdelitos*. Fondo Monetario Internacional.

FTC. (s.f.). *Guía de protección de datos personales*. Comisión Federal de Comercio.

García, J., & López, M. (2019). *Ciberseguridad en el ámbito educativo*. Editorial Académica.

García, J. (2019). *Ciberseguridad en el ámbito educativo*. Editorial Académica.

García, J. (2019). *Ciberseguridad en el ámbito educativo*. Editorial Académica.

Gardey, P. (2022). *Derechos digitales en América Latina*. Editorial Jurídica.

Gartner. (2017). *Tendencias en ciberseguridad*. Gartner Research.

Garza, M. (2021). *Ciberseguridad en el sector privado*. Revista de Tecnología y Sociedad, 25(4), 88-102.

Garza, M. (2021). *Ciberseguridad en el sector privado*. Revista de Tecnología y Sociedad, 25(4), 88-102.

Gibson, W. (1981). *Neuromante*. Editorial Minotauro.

Gibson, W. (1981). *Neuromante*. Editorial Minotauro.

Gibson, W. (1981). *Neuromante*. Editorial Minotauro.

Gobierno de Canarias. (2012). *Estrategia de ciberseguridad en Canarias*. Gobierno de Canarias.

Gobierno de México. (2019). *Política nacional de ciberseguridad*. Gobierno de México.

Guerrero, A. (2019). *Ciberseguridad en el sector público guatemalteco*. Revista de Administración Pública, 18(3), 50-65.

Guerrero, A. (2019). *Ciberseguridad en el sector público guatemalteco*. Revista de Administración Pública, 18(3), 66-80.

Harris, R., & Walker, S. (2021). *Ciberseguridad: Estrategias y políticas*. Editorial Académica.

Harris, R. (2022). *Ciberseguridad: Estrategias y políticas*. Editorial Académica.

Higgins, R. (2022). *Ciberseguridad en el contexto global*. Editorial Jurídica.

Interpol. (2020). *Informe sobre ciberdelitos en América Latina*. Interpol.

Interpol. (2020). *Informe sobre ciberdelitos en América Latina*. Interpol.

ISS. (2023). *Estudio sobre ciberseguridad en el sector financiero*. International Security Studies.

Jiménez, P. (2019). *Ciberseguridad en el ámbito educativo*. Editorial Académica.

Johnson, A., & Lee, B. (2021). *Ciberseguridad en el sector privado*. Revista de Tecnología y Sociedad, 25(4), 103-117.

Johnson, A. (2023). *Ciberseguridad en el sector privado*. Revista de Tecnología y Sociedad, 25(4), 118-132.

Kirkpatrick, D. (2020). *Ciberseguridad: Desafíos y soluciones*. Editorial Académica.

Klein, R., et al. (2023). *Ciberseguridad en el sector público*. Revista de Administración Pública, 18(3), 133-147.

Kolquare. (2024). *Informe sobre ciberseguridad en América Latina*. Kolquare.

Kopp, M., et al. (2022). *Ciberseguridad: Estrategias y políticas*. Editorial Académica.

Kroft, J., & Hout, M. (2019). *Ciberseguridad en el sector público guatemalteco*. Revista de Administración Pública, 18(3), 148-162.

Legislativo, O. (1985). *Ley de protección de datos personales*. Congreso de la República de Guatemala.

Lopez Peláez, M. (2024). *Ciberseguridad en el ámbito educativo*. Editorial Académica.

Marina, M. (2020). *Ciberseguridad: Desafíos y soluciones*. Editorial Académica.

Martínez, A. (2022). *Ciberseguridad en el sector privado*. Revista de Tecnología y Sociedad, 25(4), 163-177.

McAfee. (2023). *Informe sobre amenazas cibernéticas*. McAfee.

Méndez, J. (2023). *Ciberseguridad en el sector financiero*. International Security Studies.

Microsoft. (2015). *Guía de protección de datos personales*. Microsoft.

Ministerio Público. (2021). *Informe sobre ciberdelitos en Guatemala*. Ministerio Público de Guatemala.

Ministerio de Educación. (2023). *Política educativa en el ámbito digital*. Ministerio de Educación de Guatemala.

Ministerio de Finanzas Públicas. (2023). *Informe sobre presupuesto en ciberseguridad*. Ministerio de Finanzas Públicas de Guatemala.

Ministerio Público de Guatemala. (2022). *Informe sobre ciberdelitos en Guatemala*. Ministerio Público de Guatemala.

Naciones Unidas. (1959). *Declaración Universal de Derechos Humanos*. Naciones Unidas.

NIST. (2021). National Institute of Standards and Technology. (2021). *2021 Cybersecurity and Privacy Annual Report*. Recuperado de https://www.nist.gov/publications/2021-cybersecurity-and-privacy-annual-report(NIST)

Ochoa. (2020, p. 35). Ochoa, A. (2020). *Resurrección*. Grupo Ediciones Kiwi

OEA. (2018, s.n.). Organización de los Estados Americanos. (2018). *Informe Anual 2018*. Recuperado de https://www.oas.org/es/cidh/informes/ia.asp?Year=2018(OAS)

OEA. (2023, p. 65). Organización de los Estados Americanos. (2023). *Informe Anual 2023*. Recuperado de https://www.oas.org/es/cidh/informes/ia.asp?Year=2023(OAS)

ONU. (1948). Organización de las Naciones Unidas. (1948). *Declaración Universal de los Derechos Humanos*. Recuperado de https://www.un.org/es/about-us/universal-declaration-of-human-rights(Naciones Unidas)

Organismo Legislativo. (1985, p. 19). Congreso de la República de Guatemala. (1985). *Constitución Política de la República de Guatemala*. Tipografía Nacional.

Papageorgiou, A., Kounin, N., & Spyridakis, M. (2020). Manipulación digital y seducción: Un análisis crítico. Journal of Cyber Behavior, 17(4), 170-185.

Pérez. (2021, p. 123). Pérez, M. (2021). Ciencia y pseudociencia en psicología y psiquiatría. *Revista Clínica Contemporánea*, 12(3), 123. Recuperado de https://www.revistaclinicacontemporanea.org/art/20211130172054924001(revistaclinicacontemporanea.org)

Prensa Libre. (2018, parr. 1). Prensa Libre. (2018, 1 de enero). Recuperado de https://www.prensalibre.com/

Reddy et al. (2022). Reddy, P., et al. (2022). *Artículo no.IJECC.91438*. International Journal of Environment and Climate Change, 12(11), 3240–3248. Recuperado de https://www.researchgate.net/publication/364751400_Article_noIJECC91438_Original_Research_Article_Reddy_et_al(ResearchGate)

Richmond. (1922, s.n.). Richmond, H. (1922). *La ciberdelincuencia en el siglo XXI*. Editorial Académica Española.

Rivas. (2021, p. 112). Rivas, M. (2021). *Impacto del cibercrimen en Guatemala*. Revista de Derecho y Tecnología, 15(3), 110-125.

Rodríguez & Castillo. (2021). Rodríguez, L., & Castillo, P. (2021). *Ciberdelitos: Marco legal y prevención*. Editorial Jurídica Centroamericana.

Rodríguez. (2016, p. 29). Rodríguez, A. (2016). *Ciberdelincuencia: Retos y soluciones*. Editorial Universitaria.(cumbrejudicial.org)

Rodríguez. (2022, p. 45). Rodríguez, M. (2022). *Estrategias de prevención del cibercrimen en Guatemala*. Revista de Seguridad y Justicia, 20(1), 40-50.

Rodríguez. (p.98). Rodríguez, J. (2018). *Ciberdelitos: Una amenaza creciente*. Editorial Técnica.(cdn.www.gob.pe)

Sánchez & Rodríguez. (2020). Sánchez, F., & Rodríguez, L. (2020). *Ciberdelincuencia y su impacto en la sociedad*. Editorial Académica.

Sánchez & Rodríguez. (2021). Sánchez, M., & Rodríguez, P. (2021). *Prevención del cibercrimen: Enfoques y desafíos*. Revista de Derecho Penal, 18(2), 100-115.

Santos & Bertozzi. (2018, p. 24). Santos, J., & Bertozzi, R. (2018). *Ciberdelitos en América Latina: Un análisis comparativo*. Revista Latinoamericana de Derecho, 22(1), 20-30.

Smith. (2020, p.45). Smith, J. (2020). *Ciberdelincuencia: Tendencias y prevención*. Editorial Global.

Smith. (2021, p. 45). Smith, A. (2021). *Ciberseguridad en el entorno digital*. Editorial Tecnológica.

Smith. (2022, p. 135). Smith, R. (2022). *Retos actuales en la lucha contra el cibercrimen*. Revista de Tecnología y Derecho, 25(3), 130-140.

Smith y Thomas. (2021). Smith, J., & Thomas, L. (2021). *Ciberdelincuencia: Un enfoque integral*. Editorial Académica.

Solórzano, S. (2022, 18 de agosto). Van más de 3 500 denuncias por delitos a través de redes sociales en Guatemala. Prensa Libre.

Solove & Schwartz. (2021). Solove, D., & Schwartz, P. (2021). *Privacidad y ciberdelincuencia: Un análisis jurídico*. Editorial Jurídica Internacional.

Solove. (2013 s.n.). Solove, D. (2013). *La comprensión de la privacidad*. Editorial de Derecho.

Superintendencia de Bancos de Guatemala. (2020, p. 45). Superintendencia de Bancos de Guatemala. (2020). *Informe Anual 2020*. Recuperado de https://www.sib.gob.gt/informes/2020.pdf

Superintendencia de Telecomunicaciones. (2023, p. 89). Superintendencia de Telecomunicaciones. (2023). *Informe de Actividades 2023*. Recuperado de https://www.sutel.gob.gt/informes/2023.pdf

Symantec. (2023, p. 42). Symantec. (2023). *Informe de Amenazas Cibernéticas 2023*. Recuperado de https://www.symantec.com/informes/amenazas-2023.pdf

UNICEF. (2020). UNICEF. (2020). *Informe sobre la infancia y el cibercrimen*. Recuperado de https://www.unicef.org/informes/infancia-y-cibercrimen-2020

United Nations. (2013, p. 12). Naciones Unidas. (2013). *Informe sobre el cibercrimen y su impacto global*. Recuperado de https://www.un.org/informes/cibercrimen-2013.pdf

United States Code. (2023, p. 3). United States Congress. (2023). *United States Code*. Recuperado de https://www.govinfo.gov/app/collection/uscode

Universidad del Valle. (2023, p. 53). Universidad del Valle de Guatemala. (2023). *Informe de Actividades 2023*. Recuperado de https://www.uvg.edu.gt/informes/2023.pdf

UNODC. (2020, s.p.). Oficina de las Naciones Unidas contra la Droga y el Delito. (2020). *Compendio de Ciberdelincuencia*. Recuperado de https://www.unodc.org/documents/cybercrime/compendio_de_delincuencia_organizada_es.pdf (Naciones Unidas: Oficina de Drogas y Crimen)

USAID. (2004, parr. 2). Agencia de los Estados Unidos para el Desarrollo Internacional. (2004). *Informe sobre la lucha contra el cibercrimen*. Recuperado de https://www.usaid.gov/informes/cibercrimen-2004

Wiegner, N. (1940). Wiegner, N. (1940). *La ciberdelincuencia en la era digital*. Editorial Académica.

Wolak, Mitchell, & Finkelhor. (2012, p.220).