El ciberdelito en Centroamérica y el Caribe

conose
RED DE CONOCIMIENTO SOBRE SEGURIDAD CIUDADANA

Personas autoras
Patricia Vargas
Karen Vargas

infoSEGURA | USAID DEL PUEBLO DE LOS ESTADOS UNIDOS DE AMÉRICA | PNUD

El ciberdelito en
Centroamérica y el Caribe

conose

RED DE CONOCIMIENTO SOBRE **SEGURIDAD CIUDADANA**

La **Red CONOSE** se fundó en el 2016, como resultado del Foro Regional "Gestión de conocimiento en seguridad ciudadana: una mirada desde la sociedad civil", para responder a la necesidad de articular una serie de instituciones que abordan el tema de seguridad ciudadana.

El objetivo último de la Red es generar espacios de reflexión y colaboración para coadyuvar a la construcción de conocimientos y a la generación de evidencia rigurosa en materia de violencia y criminalidad, así como aportar académicamente a la discusión, formulación y orientación de las políticas públicas que abordan dichas problemáticas.

En consecuencia, se han desarrollado diferentes acciones que responden a las necesidades coyunturales congruentes con las líneas de trabajo que guían el quehacer de la Red. Así, uno de los ejes centrales de trabajo de la Red es el desarrollo de investigaciones.

Entre las líneas de trabajo central se encuentra el desarrollo de una agenda de investigación regional que alimente el diálogo informado entre la academia, los estados y las sociedades de la región. De modo que, como práctica de gestión del conocimiento, resulta de gran utilidad para la toma de decisiones, pues permite contar con documentación actualizada y rigurosa sobre diversas intervenciones en la región para el abordaje de la seguridad ciudadana. Este tipo de información debe dar cuenta no solo de los esfuerzos que se están realizando, sino de las lecciones aprendidas y potenciales mejoras por aplicar en futuras intervenciones.

Para tales efectos, desde el Plan de Trabajo de CONOSE para el periodo 2021-2022, se abrió un espacio para el estudio de diferentes intervenciones en materia de seguridad ciudadana y violencia a partir de un programa de becas para equipos de investigación de toda la región en una convocatoria abierta.

En esta publicación se presenta el resultado de este esfuerzo académico realizado por equipos compuestos por investigadoras e investigadores jóvenes que forman parte de la comunidad académica de la región. Desde la Red CONOSE, queremos reconocer y agradecer su esfuerzo y su dedicación en este proceso; estamos muy complacidos con los resultados que se muestran a continuación.

De igual manera, queremos agradecer a la Agencia de los Estados Unidos para el Desarrollo internacional (USAID) y al Programa de las Naciones Unidas para el Desarrollo (PNUD) por el apoyo y acompañamiento brindado a través del equipo de trabajo del proyecto INFOSEGURA.

Red de Conocimiento sobre Seguridad Ciudadana (CONOSE)

El ciberdelito en Centroamérica y el Caribe

COLECCIÓN: LECCIONES Y APRENDIZAJES

Comité Coordinador:
Facultad Latinoamericana de Ciencias Sociales,
FLACSO sede académica Costa Rica: Ilka Treminio
Universidad de Panamá: José Lasso
Universidad Rafael Landívar: Anabella Amado Alemán

Secretaría Técnica:
Carlos Guillermo Ramos González y Karla Salazar Sánchez

Personas Autoras: Patricia Vargas y Karen Vargas

Edición: María Amalia Amador Fournier, Karla Salazar Sánchez y Carlos Guillermo Ramos González
Revisión filológica: Sergio Barboza Quesada
Diseño de cubierta: Diana Castro Brenes
Diagramación: Elissa Reyes Díaz

304.69728
V297c Vargas, Patricia
Ciberdelito en Centroamérica y el Caribe [recurso electrónico] / Patricia Vargas, Karen Vargas. – primera edición – San José, Costa Rica, FLACSO, 2023.
E-book ; pdf : 2,47 Mb.

ISBN 978-9977-68-346-1

1.DELITOS INFORMÁTICOS. 2. FRAUDES. 3. PRUEBA ELECTRÓNICA. COMUNICACIÓN ELECTRÓNICA. I. Vargas, Karen. II.Título.

Esta publicación contó con el apoyo y financiamiento de:

Esta publicación ha sido posible gracias al apoyo brindado por el pueblo de los Estados Unidos por medio de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID, por sus siglas en inglés), y al Programa de las Naciones Unidas para el Desarrollo (PNUD). Las opiniones y los puntos de vista que se presentan en este documento son exclusiva responsabilidad de sus autores y autoras, y no reflejan necesariamente los de USAID, del Gobierno de los Estados Unidos, del PNUD o de los países miembros de las Naciones Unidas.

Editorial FLACSO Costa Rica, 2023

Contenido

Índice de tablas

Índice de ilustraciones

Índice de gráficos

1. **Antecedentes**

La Red Conose surgió en el año 2015, a partir del foro regional *Gestión de conocimiento en seguridad ciudadana: una mirada desde la sociedad civil*, como una respuesta a la necesidad de articular una serie de instituciones que abordan el tema de seguridad ciudadana. Dentro de uno de los ejes centrales de trabajo de la Red se encuentra el desarrollo de investigaciones que, preferencialmente, aborden fenómenos y procesos de carácter regional, en ese marco se estructura esta investigación sobre el tema de ciberseguridad y delito digital en América Central. El punto de referencia principal para este estudio fue una base de datos perteneciente a una encuesta regional aplicada en cinco países centroamericanos por la casa encuestadora CID Gallup, a solicitud de las oficinas de PNUD, en el primer cuatrimestre del año 2021. Con base en dicho insumo se generó un proceso de análisis de los datos con enfoque de género e interseccionalidad, a fin de tener una perspectiva más amplia sobre la ciberdelincuencia y las características victimológicas de las personas pertenecientes a la muestra de la base de datos que recabó información de Costa Rica, El Salvador, Guatemala, Honduras y República Dominicana.

2. **Marco Conceptual**

Existe una hiperconexión en el mundo digital, la mayoría de actividades diarias hoy en día se han virtualizado, tales como el trabajo, la educación, la comunicación, el comercio y el uso de la banca, lo cual provoca que al día se generen miles de interacciones para realizar las actividades cotidianas. El uso del Internet y plataformas digitales es parte de la vida diaria de las personas, "Según un estudio de la agencia especializada en comunicación digital We Are Social, en 2021 más de 4.600 millones de personas acceden a internet en todo el mundo, 316 millones más que en 2020. Esto quiere decir que alrededor de 60% de la población mundial se encuentra en Internet y más de la mitad de los habitantes del planeta 4.200 millones ya usa por la menos una red social, mientras 5.200 millones de personas dos tercios de la población mundial comentan con un teléfono inteligente. 2020 fue un año que cambio las tendencias del consumo de medios tal y como se verificaron año a año por décadas" (Kanarek, 2021, pág. 33).

Según los datos de Digital Global Overview Report (2022):

- El último año la humanidad paso 12½ billones de horas en Internet.
- Población mundial: La población mundial es de 7.910 millones en enero de 2022, Usuarios mundiales de móviles: Más de dos tercios (67,1%) de la población mundial utiliza ya un teléfono móvil, con 5.310 millones de usuarios únicos a principios de 2022.
- El número mundial de usuarios de Internet ha aumentado hasta los 4.950 millones a principios de 2022, con una penetración de Internet del 62,5% de la población mundial.
- En enero de 2022 había 4.620 millones de usuarios de redes sociales en todo el mundo.
- Un internauta pasa en Internet 6 horas y 58 minutos en promedio al día.
- Las redes sociales cuentan con 4.62 billón de usuarios.
- El tiempo que dedica a una persona en promedio al día en las redes sociales es de 2 horas 27 minutos.
- Los usuarios de YouTube dedican casi un día entero al mes (23,7 horas) a utilizar la aplicación móvil.
- Facebook y Tiktok son las redes que los usuarios ocupan una media mensual de 19,6 horas en la aplicación.
- WhatsApp ocupa el tercer lugar en términos de tiempo total dedicado, con usuarios que pasan una media de 18,6 horas al mes utilizando la

aplicación de mensajería en teléfonos Android. (Digital Global Overview Report, 2022).

Esto es en un solo minuto, por lo cual la mayoría de las interacciones y exposición a diversa información, requieren que las personas que usan las plataformas, redes, diversos dispositivos, tengan la suficiente alfabetización y ciudadanía digital desarrolladas. Dado los miles de beneficios que brinda el mundo digital para facilitar la vida, es necesario que las personas estén conscientes de los riesgos y vulnerabilidades a las que se enfrentan al navegar.

Es parte de las obligaciones de los Estados poder brindar a sus ciudadanos las herramientas necesarias, educación, disminuir la brecha digital, para lograr que cualquier persona pueda interactuar de forma segura con las tecnologías y prevenir ser víctima de ciberdelitos.

Con la pandemia Covid-19 la población mundial pasó a interactuar con la tecnología en todos los niveles de la vida, se agilizó la inmersión tecnológica, solo en 2020 la humanidad pasó un total de 1250 millones de años utilizando Internet (Kanarek, 2021).

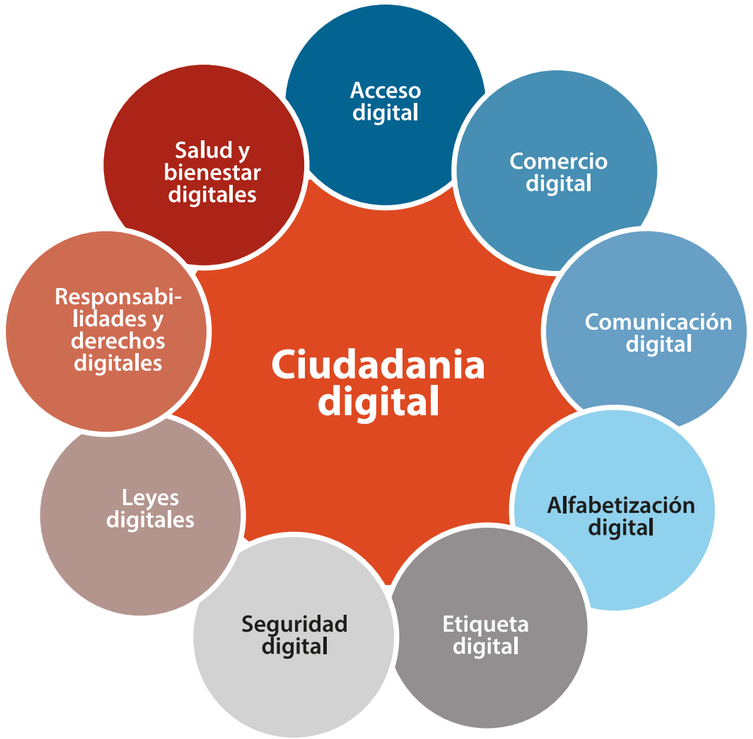
La inmersión tecnológica se ha dado de forma diferenciada y desigual, lo que impacta en la relación de las personas con la tecnología. Hoy en día en Internet interactúan 3 tipos de personas:

- Los nativos digitales, aquellos que nacieron cuando el Internet ya se había popularizado, por lo que tienen un alto nivel de familiaridad con la tecnología.
- Los migrantes digitales aquellas personas que vivieron la transición del mundo sin internet hacia un mundo conectado.
- Los huérfanos digitales son los niños, niñas y adolescentes que pasan largas horas en internet sin la supervisión de los padres.

Lo complejo es que, independientemente del grupo al cual se pertenezca, la mayoría de las personas no contó con un desarrollo orgánico de su ciudadanía digital, careció de alfabetización digital y está familiarizándose constantemente con la tecnología mediante ensayo y error, lo que incrementa su vulnerabilidad cuando interactúan en plataformas tecnológica o redes sociales.

En un mundo ideal una persona, antes de generar una inmersión completa en plataformas digitales e interactuar de forma ilimitada con la tecnología, debería desarrollar su ciudadanía digital, esa serie de habilidades que permiten a las personas, “acceder, recuperar, comprender, evaluar y utilizar, crear y compartir información y medios en todos los formatos, utilizar varias herramientas, de manera crítica, ética y, de forma eficaz, participar y comprometerse en actividades personales, profesiones y sociales.” (Cicam, 2021) En total son 9 los elementos digitales necesarios para lograr que las personas interactúen de forma segura en plataformas digitales y alcanzar un nivel de desarrollo para madurar dicha ciudadanía (Cicam, 2021), a fin de minimizar los riesgos al interactuar con la tecnología.

Ilustración 1. Elementos de la ciudadanía digital



Fuente: elaboración propia.

Para lograr que una persona cuente con una ciudadanía digital (ver Ilustración 1) debe tener acceso digital, es decir, debe poder participar en esa comunidad virtual, también poder comprar productos y servicios a través de medios tecnológicos en un comercio digital seguro, así como contar con los mecanismos para poder comunicarse digitalmente e intercambiar información electrónica, acceder a procesos de alfabetización digital donde aprenda acerca de la tecnología y su uso. Es clave que las personas en las plataformas digitales comprendan la etiqueta digital, esa serie de estándares electrónicos de conducta o procedimiento, también el marco legal, las leyes digitales, la responsabilidad electrónica ante hechos y acciones, esto aunado a las responsabilidades y derechos digitales, esas libertades extendidas a todos en el mundo digital, así como los mecanismos básicos de seguridad digital, bienestar físico y psicológico en el mundo tecnológico digital.

Todos los días se interactúa en plataformas virtuales, los cuales son sistemas que permiten la ejecución de diversas aplicaciones a las que se accede a través de internet (Cicam, 2021). En ellas se desarrollan diversas plataformas digitales, programas o aplicaciones cuyo contenido es ejecutable en determinados sistemas operativos, ya sean contenidos visuales, de texto, audios, videos, simulaciones, etc. (Cicam, 2021). Cada vez que se accede a una página web existe un URL, el cual es un localizador uniforme de recurso o dirección web que, al ser encontrada y visualizada por un navegador, muestra un recurso de información al usuario, "Por las siglas en inglés Uniform Resource Locator, se refiere a la dirección específica que se asigna a cada uno de los recursos disponibles en la red (páginas, sitios, documentos) con la finalidad de que puedan ser localizados o identificados" (OEA, 2021).

De esta forma cada vez que se navega e interactúa en la red, una persona deja una huella digital, la cual es una recopilación de información sobre la

persona que se basa en su comportamiento *online*: lo que publica, lo que busca, dónde lo hace y en qué se basa para hacerlo (MGS, 2022). Muchas personas, sobre todo las nacidas después del 2020, tienen una huella digital incluso antes de acceder directamente a la tecnología, es el caso de los bebes a quienes sus padres ya les han generado perfiles, compartido fotos, etc. La huella digital es el rastro que deja una persona en el mundo digital, cuando una persona navega en Internet, visita páginas web, está proporcionando una serie de información con su IP, la que revela la ubicación geográfica, navegador, sistema operativo del ordenador o dispositivo, idioma, sexo, edad e incluso el último lugar que se ha visitado, estos datos habitualmente no suponen una intrusión en la privacidad. No se está revelando de manera involuntaria ningún dato personal o privado, sino estadístico que se utiliza para crear perfiles de comprador o de visitante a un sitio web. Las webs, a su vez, dejan una cadena de dígitos en el navegador que se conoce como cookie (literalmente 'galleta'). Estas cadenas quedan en el navegador hasta que se opta por borrarlas y tienen un uso práctico muy claro, de perfilar gustos, intereses etc. Lo cual hace que, en muchos casos, el acceso a la información que tiene una persona está algorítmicamente generada a partir de los intereses personales y el perfil que ha generado su huella digital.

Hoy en día existe amplia gama de redes sociales, Facebook, Instagram, Tiktok, plataformas informáticas que albergan comunidades virtuales de individuos interconectados, los cuales comparten contenido, información, archivos, fotos, audios, videos, entre otros. Además, la tecnología se ha expandido para mejorar los niveles de vida mediante múltiples dispositivos inteligentes, lo cual ha brindado desarrollo al internet de las cosas, toda esta red de dispositivos inteligentes conectados a internet que pueden compartir datos entre sí. El internet de las cosas va más allá de la conectividad entre computadoras, teléfonos celulares y tabletas, e incluye dispositivos como televisiones, relojes, frigoríficos, sistemas de calefacción, cámaras o cerraduras inteligentes. Se dice que estos dispositivos son "inteligentes" porque pueden recolectar y analizar datos, comunicarse entre ellos y ejecutar acciones sin intervención humana directa (OEA y Cicte, 2020). El internet de las cosas, el cual hoy se encuentra en muchos hogares, es un tema desconocido para la mayoría de las personas que interactúan con dispositivos inteligentes conectados al internet en sus residencias y que comparten datos entre sí (OEA y Cicte, 2020).

En muchos hogares centroamericanos hoy se cuenta con cafeteras, computadores, teléfonos, televisores, relojes, refrigeradores, luces, cámaras y otra serie de dispositivos inteligentes, los cuales se comunican entre ellos, recopilan y analizan datos, que representan un avance en el confort y estilo de vida; sin embargo, pueden tener riesgos potenciales a la seguridad y privacidad. Cuando una persona ha logrado tener una alfabetización digital, desarrollar su ciudadanía digital, puede interactuar de forma más segura con el internet de las cosas, comprende los riesgos, vulnerabilidades y toma las medidas de seguridad necesarias para lograr una interacción informada en las plataformas digitales.

Las maravillas y beneficios de las plataformas de internet, también han generado una serie de riesgos en la virtualidad, aquí se abordan la violencia digital y los ciberdelitos. Es importante tener en cuenta que, aunque muchas de las conductas delictivas expuestas a continuación existen en los espacios

digitales, falta mucho para lograr que sean integradas todas estas conductas en los sistemas normativos y sean perseguidas y judicializadas por los sistemas de seguridad y justicia.

En 2018, la Relatora Especial sobre la Violencia contra la Mujer de Naciones Unidas definió la violencia en línea contra las mujeres como "todo acto de violencia por razón de género contra la mujer cometido con la asistencia, en parte o en su totalidad, del uso de las TIC, o agravado por este, como los teléfonos móviles y los teléfonos inteligentes, Internet, plataformas de medios sociales o correo electrónico, dirigida contra una mujer porque es mujer o que la afecta en forma desproporcionada" (REVM-ONU, 2018, párr. 23).

Es importante diferenciar entre ciberseguridad y ciberdelincuencia. La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales, busca proteger los sistemas de información, las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. Las medidas de seguridad están diseñadas para combatir las amenazas a sistemas en red y aplicaciones (Cisco, 2022; IBM, 2022). Mientras que, "la ciberdelincuencia es un acto que infringe la ley y que se comete usando las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito.

La ciberdelincuencia se diferencia de los delitos comunes en que «no tiene barreras físicas o geográficas» y se puede cometer con menos esfuerzo y más facilidad y velocidad que los delitos comunes" (UNODC, 2022). Esos diferentes actos de ciberdelincuencia se configuran en diferentes ciberdelitos, que son todos aquellos delitos cometidos a través de cualquier medio tecnológico (OEDI, 2022). Para llevar a cabo estos delitos se utilizan las TIC y según el delito la tecnología juega una función u otra, en algunos casos en los delitos ciberdependientes la plataforma tecnológica es el objetivo del ataque o cuando el delito no se puede producir sin ella (UNODC, 2022). Mientras que en los delitos ciberfacilitados la tecnología se utiliza como medio para cometer el delito, la tecnología permite la comisión más fácil, más dañina o con más protección para el agresor o grupo (UNODC, 2022).

Los principales ciberdelitos son:

1. **Sextorsión:** "Consiste en amenazar a una persona con difundir imágenes o videos íntimos con la finalidad de obtener más material sobre actos sexuales explícitos, mantener relaciones sexuales u obtener dinero" (OEA, 2021).
2. **Difusión de contenido sin consentimiento:** "Consiste en crear, compartir o difundir en línea, sin consentimiento, material, imágenes o videos íntimos o sexualmente explícitos obtenidos con o sin el consentimiento de una persona, con el propósito de avergonzarla, estigmatizarla o perjudicarla" (REVM-ONU, 2018, párr. 41).
3. ***Ransomware:*** "Es un programa de software malicioso mediante el cual se toma el control del equipo infectado y se 'secuestra' la información de la persona usuaria (cifrándola) con el objetivo de extorsionarla solicitando un rescate económico" (OEA, 2021: 40).

4. ***Malware:*** "El término nace de la unión de las palabras en inglés malicious software (software malintencionado) y hace referencia a un tipo de software que tiene como objetivo infiltrarse y/o dañar un sistema de información sin el consentimiento de la persona usuaria" (OEA, 2021: 40).

5. ***Doxing* o *doxxing*:** "El término proviene de la frase en inglés dropping docs y consiste en la extracción y la publicación no autorizadas de información personal —como el nombre completo, la dirección, números de teléfono, correos electrónicos, el nombre del cónyuge, familiares e hijos, detalles financieros o laborales— como una forma de intimidación o con la intención de localizar a la persona en 'el mundo real' para acosarla (APC, 2017; Women's Media Center, 2019). También se ha observado que la información personal puede ser publicada en sitios pornográficos junto con el anuncio de que la víctima está ofreciendo servicios sexuales" (OEA y Cicte, 2020: 28).

6. **Suplantación y robo de identidad:** "Es una actividad malintencionada que consiste en hacerse pasar por otra persona en línea usando sus datos personales con el fin de amenazarla o intimidarla (Women's Media Center, 2019). Esto puede hacerse mediante la creación de perfiles o cuentas falsas en redes sociales o la usurpación de cuentas de correo o números de teléfono que puedan ser utilizados para contactar amistades, familiares, colegas o conocidos de la víctima con el propósito de entablar comunicación y tener acceso a información sobre ella (APC, 2017; Barrera, 2017)" (OEA y Cicte, 2020: 29).

7. **Ciberhostigamiento:** "(...) actividad intencional y reiterada realizada mediante computadoras, teléfonos celulares y otros dispositivos electrónicos, que puede constituir o no actos inofensivos por separado, pero que, en conjunto, constituye un patrón de conductas amenazantes que socavan la sensación de seguridad de una persona y le provocan miedo, angustia o alarma (EIGE, 2017: 4; PRC, 2018; Maras, 2016). Esta actividad puede estar dirigida también contra familiares, amistades o la pareja sentimental de la víctima. A diferencia del ciberacoso, el ciberhostigamiento implica un patrón y la comisión de más de un incidente a lo largo de un tiempo usando las TIC, con el objetivo reiterado de hostigar, acechar, molestar, atacar, humillar, amenazar, asustar u ofender a una persona o abusar verbalmente de ella (UNODC, 2015). Puede consistir en correos electrónicos, llamadas, mensajes de texto, chat en línea o el envío constante de comentarios obscenos, vulgares, difamatorios o amenazantes por internet" (OEA y Cicte, 2020: 32).

8. **Ciberacoso:** "implica el uso intencional de las TIC para humillar, molestar, atacar, amenazar, alarmar, ofender o insultar a una persona (Maras, 2016). A diferencia del ciberhostigamiento, en el que hay un patrón de comportamientos amenazantes, en el caso del ciberacoso basta con un solo incidente, aunque puede implicar también más de uno (UNODC, 2019)" (OEA y Cicte, 2020: 33).

9. **El *ciberbullying* o ciberintimidación:** es el uso de tecnologías por menores de edad para humillar, molestar, alarmar, insultar o atacar a otra/o

menor de edad o difundir información falsa o rumores sobre la víctima, así como para amenazarla, aislarla, excluirla o marginarla (Maras, 2016; Hinduja y Patchin, 2014) (UNODC, 2015).

10. **Trata virtual:** "el uso de tecnologías para seleccionar y enganchar mujeres y niñas con fines de abuso sexual o trata, obligarlas a aceptar situaciones de trata y abuso sexual, ejercer poder y control sobre ellas o impedirles que se liberen del abuso, incluso con amenazas de revelar información privada" (REVM-ONU, 2018).
11. **El *grooming* o ciberengaño pederasta:** "actos deliberados de un adulto para acercarse a una persona menor de edad (posiblemente cultivando una conexión sentimental) con el objetivo de establecer una relación y un control emocional que le permita cometer abusos sexuales, entablar relaciones virtuales, obtener pornografía infantil o traficar al o la menor" (Women's Media Center, 2019).

Las plataformas digitales han creado canales de comunicación ampliados, los cuales permiten una interconexión simultánea y diversifican los medios de comunicar, expresar e interactuar en la actualidad. La pandemia de Covid-19, sin la interconectividad que brinda el acceso a internet y a la tecnología, hubiera generado más caos e incomunicado a miles de personas. La interconectividad facilita las acciones cotidianas de la vida, el acceso a la información, democratiza el acceso a los medios de comunicación, sin embrago en la era de la información existe un alto riesgo a estar desinformados, debido a que el ecosistema digital, también ha sido plataforma donde personas utilizan las vulnerabilidades personales y de los sistemas, redes y dispositivos para violentar y delinquir (Del Pino, s.f.). Razón por la cual hoy más que nunca es importante que se preste atención en el comportamiento y relacionamiento de las personas con la tecnología.

3. **Objetivos**

Objetivo General

Brindar un análisis sobre ciberdelito en América Central a partir de la encuesta disponible y la revisión de la literatura.

Objetivos Específicos

- Caracterizar a la población consultada a partir de la base de datos de la encuesta.
- Describir la situación de los países y de la región en temas de ciberdelitos a partir de los resultados de la encuesta y en contraste con la información obtenida a partir de la revisión documental.
- Caracterizar a la víctima y al agresor a partir del enfoque victimo-criminológico.
- Describir los efectos psicosociales de las personas con base en la encuesta y en revisión de la literatura.
- Analizar los desafíos que esta modalidad de crimen plantea a los aparatos jurídicos e institucionales de los Estados de la región a partir de la revisión bibliográfica, jurídica y reflexiones del equipo consultor.

4. **Metodología utilizada**

Este proceso prioriza el enfoque de género, tiene en cuenta las brechas de acceso a internet, los riesgos y vulnerabilidades de las personas en la web. Es importante comprender los factores de riesgos y los factores de protección frente al ciberdelito.

El abordaje metodológico partió del proceso de análisis de la base de datos de una encuesta regional corrida en cinco países centroamericanos por la casa encuestadora CID Gallup, a solicitud de las oficinas de PNUD, durante el primer cuatrimestre del año 2021 fue llevada a cabo en 5 países de la región, a saber: de Costa Rica, El Salvador, Guatemala, Honduras y República Dominicana. Se enfatizó en la información en relacionada con los ciberdelitos, se estructuró la información por país y en comparativo entre los 5 países priorizados en la encuesta, información nutrida con información bibliográfica, la cual tuvo en cuenta sus marcos jurídicos. *La Encuesta de Ciberdelito* contó con una muestra total de 3000 personas 600 por cada país participante. Las desagregaciones de los datos se centraron en lograr comprender el ciberdelito fueron principalmente las relacionadas en la Tabla 1.

Tabla 1. Desagregación de base de datos

Ítem	Desagregación de la base de datos													
	Edad	*Género*	*Ocupación*	*Nivel educativo*	*Urbano/ rural*	*Tipo de red social o plataforma que utilizan*	*Tipo de dispositivo que utilizan*	*Tipo de red social o plataforma en el que fueron víctimas*	*Identificación del agresor*	*Relación con el agresor*	*Medidas de protección utilizadas*	*Mes en que fue víctima*	*Daños a la salud*	*Denuncia*
Cantidad de personas participantes														
Cantidad de personas por país														
Cantidad de personas por país víctimas de ciberdelitos														
Cantidad total de personas víctimas de ciberdelito en Centroamérica														
Tipo de ciberdelito (ciberacoso, software malicioso, hackeo, ransomware) y número de personas víctimas por país														

Fuente: elaboración propia.

La desagregación de variables de la Tabla 1, dio la pauta para poder generar algunos cruces entre 2 o 3 variables que ampliaron el umbral de análisis, para lo cual se cruzaron:

a. Edad – Género – País
b. Área -Género-País
c. Ocupación-Género-País
d. Nivel educativo-Género-País
e. Tipo dispositivo-Género-País
f. Tipo red social-Género-País
g. Delitos – Género – País
h. Delitos – Rango de edad – País
i. Delitos – País

Los anteriores cruces ayudaron a observar las variaciones en relación a los niveles de victimización, lo cual contribuyó a un análisis diferencial de las problemáticas, para lograr entender las acciones prioritarias a tener en cuenta para avanzar en la prevención de ciberdelitos y un análisis más profundo del contexto. El presente informe, reporta los datos en números absolutos.

Encuesta en cinco países

En la encuesta participaron 3000 personas de 5 países, a saber: Costa Rica, Guatemala, El Salvador, Honduras y República Dominicana. Los participantes, de acuerdo con su género,1 fueron 1511 de género femenino y 1489 de género masculino. Del total de la muestra en relación con la edad, el grupo etario más representativo con el 36% fueron personas entre los 18 a 24 años, seguido

1 De acuerdo con la Corte Interamericana de Derechos Humanos, se denomina Sexo: se refiere a las diferencias biológicas entre el hombre y la mujer, a sus características fisiológicas, a la suma de las características biológicas que define el espectro de las personas como mujeres y hombres o a la construcción biológica que se refiere a las características genéticas, hormonales, anatómicas y fisiológicas sobre cuya base una persona es clasificada como macho o hembra al nacer, (OEA, Consejo Permanente de la Organización de los Estados Americanos, Comisión de asuntos jurídicos y Políticos. Orientación sexual, identidad de género y expresión de género: algunos términos y estándares relevantes). Mientras que Género: Se refiere a las identidades, las funciones y los atributos construidos socialmente de la mujer y el hombre y al significado social y cultural que se atribuye a esas diferencias biológicas,(Naciones Unidas, Comité para la Eliminación de la Discriminación contra la Mujer – CEDAW, Recomendación general Nº 28 relativa al artículo 2 de la Convención sobre la eliminación de todas las formas de discriminación contra la mujer, CEDAW/C/GC/28, 16 de diciembre de 2010, párr. 5, y OEA, Consejo Permanente de la Organización de los Estados Americanos, Comisión de asuntos jurídicos y Políticos. Orientación sexual, identidad de género y expresión de género: algunos términos y estándares relevantes. Estudio realizado por la Comisión Interamericana de Derechos Humanos, OEA/Ser.G. CP/CAJP/INF. 166/12. 23 abril 2012, párr. 14.) Al existir una confusión sistemática sobre estos dos términos, las personas normalmente cuando se les pregunta el sexo no responden el grupo cromosomático al que corresponden, sino la categoría del género con la que se identifican, para el presente caso dentro del binarismo hombre y mujer.

del grupo etario de 24 a 34 que representó el 29%, el 18% fueron personas de 35 a 44 años, el 10% de entre 45 a 54 años y un 7% de 55 o más.

Los principales niveles de ocupación de las personas encuestadas son, en primer lugar, estudiantes, el segundo amas de casa y el tercero son no identificados o desempleados. En relación con el nivel educativo de las personas encuestadas, 1767 contaban con nivel secundario equivalente al 59% de la muestra, 1002 con nivel educativo superior correspondiente al 33% y 231 con nivel primario equivalente al 8%.

La encuesta contó con la participación de un 83% de personas participantes del área urbana y 17% del área rural. En el área rural la participación fue menor por múltiples factores como la brecha digital que existe entre el área rural y urbana en los diferentes países, falta de infraestructura para conexión de internet y factores económicos. En relación con los dispositivos que utilizaban las personas encuestadas, el 94.3% utilizan smartphone, el 2.8 % utilizan computadora de escritorio, el 1.5 % utilizan *laptops*, el 0.9% dijo utilizar tabletas y el 0.4% utiliza otros dispositivos.

El 68% de las personas participantes no respondieron a la pregunta que red o plataforma que utilizan, el 15% afirma utiliza redes sociales como Facebook, Instagram, Twitter y el 8% mensajería instantánea como WhatsApp, Telegrama, Viber, WeChat.

Tabla 2. Uso redes sociales o plataformas por país y género 2021

Cantidad de personas por país y género																
Redes sociales o plataformas	**Costa Rica**			**El Salvador**			**Guatemala**			**Honduras**			**República Dominicana**			**Total general**
	Fem	**Masc**	**Total**	**Fem**	**Masc**	**Total**	**Fem**	**Masc**	**Total**	**Fem**	**Masc**	**Total**	**Fem**	**Masc**	**Total**	
Correo electrónico (e-mail)	0	6	**6**	1	12	**13**	13	35	**48**	15	8	**23**	3	3	**6**	**96**
Mensajería instantánea (WhatSapp, Telegram, etc.)	50	64	**114**	186	146	**332**	130	97	**227**	101	101	**202**	56	82	**138**	**1013**
Mensajes de texto (SMS)	21	12	**33**	1	4	**5**	37	32	**69**	6	4	**10**	4	15	**19**	**136**
No sabe/No contesta	10	2	**12**	8	7	**15**	0	3	**3**	4	0	**4**	5	9	**14**	**48**
Otros medios (especifique)	2	6	**8**	3	0	**3**	13	18	**31**	2	0	**2**	0	4	**4**	**48**
Plataformas de redes sociales (Facebook, Instagram)	118	87	**205**	147	118	**265**	398	239	**637**	79	115	**194**	98	64	**162**	**1463**
Total general	**201**	**177**	**378**	**346**	**287**	**633**	**591**	**424**	**1015**	**207**	**228**	**435**	**166**	**177**	**343**	**2804**

Fuente: elaboración propia con base en la encuesta de PNUD 2021.

En la Tabla 2 se ve la correspondencia en relación con el género por país del uso de redes sociales y mensajería instantánea. En cuatro países parte de la muestra Costa Rica, El Salvador, República Dominicana y Guatemala, las personas de género femenino interactúan más en redes sociales en comparación a las de género masculino, solamente en Honduras el número de personas con género masculino que usan redes sociales es mayor al de género femenino. Con

relación a la mensajería instantánea, en República Dominicana y Costa Rica es mayor el número de personas con género masculino que utilizan mensajería instantánea, en contraposición con Guatemala y El Salvador donde es mayor la población femenina que utiliza mensajería instantánea. En Honduras la encuesta muestra que es igual el número de personas, tanto femeninas como masculinas, que tienen acceso a la mensajería instantánea. Conocer dónde interactúan las personas en relación con su género es primordial, ya que la violencia en plataformas digitales es diferenciada en relación al género.

Tabla 3. Tipo de dispositivo que usan por país y género 2021

Cantidad de personas por país y género																
Tipo de dispositivo	**Costa Rica**			**El Salvador**			**Guatemala**			**Honduras**			**República Dominicana**			**Total general**
	Fem	**Masc**	**Total**	**Fem**	**Masc**	**Total**	**Fem**	**Masc**	**Total**	**Fem**	**Masc**	**Total**	**Fem**	**Masc**	**Total**	
Otro (e.g. Smart TV) Especifíque	0	1	**1**	3	0	**3**	0	3	**3**	0	1	**1**	3	3	**6**	**96**
Un smartphone	481	525	**1006**	579	591	**1170**	757	655	**1412**	417	504	**921**	56	82	**138**	**1013**
Una computadora de escritorio	18	15	**33**	20	8	**28**	57	11	**68**	15	24	**39**	4	15	**19**	**136**
Una laptop	2	8	**10**	7	2	**9**	41	15	**56**	6	11	**17**	5	9	**14**	**48**
Una tablet	2	3	**5**	0	0	**0**	9	10	**19**	9	3	**12**	0	4	**4**	**48**
Total general	**503**	**552**	**1055**	**609**	**601**	**1210**	**864**	**694**	**1558**	**447**	**543**	**435**	**166**	**177**	**343**	**2804**

Fuente: elaboración propia con base en la encuesta de PNUD 2021.

En relación con los dispositivos utilizados, como lo muestra la Tabla 3, las personas participantes en la encuesta afirman el 94% usa *smartphone*, el 5% computadoras de escritorio y el 1% *laptops*. Lo que muestra que el uso de dispositivos móviles es la tendencia de uso, lo que determina factores de movilidad, conectividad móvil y uso de otras IPs. En relación con los datos sobre los ciberdelitos, la Tabla 4 muestra la cantidad de casos que fueron reportados en la encuesta cuando se preguntó si la persona ha sido víctima de: ciberacoso, malware, hackeo de email, hackeo de redes, ransonware. Se reportaron 6229 casos de ciberdelitos, los cuales tienen mayor frecuencia en las áreas urbanas de los 5 países. Es importante tener en cuenta que, entre las personas de la muestra, varias expresaron haber sido víctimas de más de un ciberdelito por lo cual incluso cuando la muestra es de 3000, se documentan más de 6229 casos.

Tabla 4. Cantidad de casos de ciberdelitos según área rural o urbana por país 2021

Cantidad de personas por país							
Género	**Área**	**Costa Rica**	**El Salvador**	**Guatemala**	**Honduras**	**República Dominicana**	**Total general**
Femenino	**Rural**	114	111	212	87	97	**621**
Masculino		91	107	174	83	58	**513**
Femenino	**Urbana**	411	521	720	405	466	**2523**
Masculino		479	524	566	509	494	**2572**
Total general		**1095**	**1263**	**1672**	**1084**	**1115**	**6229**

Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Tabla 5. Casos de ciberdelitos desagregados por edad, género y país 2021

Cantidad de personas por país							
Edad	**Género**	**Costa Rica**	**El Salvador**	**Guatemala**	**Honduras**	**República Dominicana**	**Total general**
18-14	Femenino	145	247	452	208	214	**1,266**
	Masculino	155	209	360	205	161	**1,090**
25-34	Femenino	143	183	263	131	181	**901**
	Masculino	119	198	198	198	192	**905**
35-44	Femenino	84	101	160	100	90	**535**
	Masculino	122	126	120	105	104	**577**
45-54	Femenino	85	72	44	44	56	**301**
	Masculino	83	69	55	55	34	**296**
55+	Femenino	68	29	13	9	22	**141**
	Masculino	91	29	7	29	61	**217**
Total general		**1095**	**1263**	**1672**	**1084**	**1115**	**6229**

Fuente: elaboración propia con base en la encuesta de PNUD 2021.

De acuerdo con la Tabla 5, los nativos digitales fueron la población que reportó más casos de ciberdelitos, lo que implica que el nivel de desarrollo de la ciudadanía digital en las personas de los rangos de edad de entre 18-24 y 25-34 es bajo. El alto índice de víctimas muestra, en parte, la carencia de alfabetización digital y que muchas personas de este grupo pueden ser huérfanos digitales, de modo que más acceso no necesariamente implica conocer y comprender los riesgos de las plataformas digitales y específicamente del Internet.

Las personas migrantes digitales enfocan el uso de dispositivos digitales a procesos laborales o de estudio, situación que fue cambiando con la pandemia Covid-19, debido a la cual diversos servicios básicos se digitalizaron como la telemedicina, la información, el comercio, el teletrabajo y el estudio, lo cual generó una inmersión tecnológica y el uso de diversas plataformas por parte de las personas migrantes digitales. Aun con este contexto, a más edad el uso de redes y mensajería instantánea disminuye, lo cual es proporcional al número de casos de víctimas de ciberdelitos, el cual disminuye a medida que se avanza en rangos etarios en la muestra de la encuesta.

Tabla 6. Cantidad de víctimas por ciberdelito según país 2021

Cantidad de personas por país						
Ciberdelito	**Costa Rica**	**El Salvador**	**Guatemala**	**Honduras**	**República Dominicana**	**Total**
Ciberacoso	199	305	333	220	156	**1213**
Malware	313	316	315	274	211	**1429**
Hackeo email	151	201	327	176	188	**1043**
Hackeo redes	213	296	416	266	373	**1564**
Ramsomware	38	61	108	52	63	**322**
No sabe / No responde	181	84	173	96	124	**658**
TOTAL	**1095**	**1263**	**1672**	**1084**	**1115**	**6229**

Fuente: elaboración propia con base en la encuesta de PNUD 2021.

De forma general, en relación con los ciberdelitos analizados en esta encuesta, la Tabla 6 refleja una tendencia en la cual las personas encuestadas han sido víctimas de hackeo en redes con un 25%, *malware* con un 23%, ciberacoso 19%, hackeo email 17%, No sabe/no responde 10% y *ransomware* con el 5%. El país que presenta más casos es Guatemala con el 26% de los casos, seguido de El Salvador con el 20% de los casos, el tercer lugar es para República Dominicana con el 18%, seguido Costa Rica con el 17.5% y, por último, Honduras 17%. La diferencia entre el primer país y el quinto es 9%, lo que implica en términos numéricos 588 casos de diferencia. Se evidencia una carencia de alfabetización digital, así como un pobre desarrollo de la ciudadanía digital en la población de los países participantes en encuesta.

Disminuir la prevalencia de ciberdelitos requiere que las personas se relacionen con la tecnología y las plataformas digitales desde el conocimiento de estas. Los países parte de la encuesta requieren trabajo de prevención del ciberdelito, donde las personas conozcan sus derechos y obligaciones en las plataformas digitales, los mecanismos de ciberseguridad personal, que las personas adviertan cómo funciona la criminalidad en Internet, así como las diversas formas de violencia. Madurar en los diferentes aspectos de la ciudadanía digital es el camino para lograr que, por ejemplo, en el caso de Hackeo de email las personas establezcan parámetros de uso del correo para reducir la vulnerabilidad a engaños.

En los 5 países priorizados el grupo etario más vulnerables a los delitos priorizados (ciberacoso, *malware*, hackeo email, hackeo redes y *ramsomware*) son las personas de entre 18 y 24 años, donde se presenta el 37% de los casos, seguido del grupo etario de 25 a 34 con el 29% de los casos, con lo cual el 60% de los casos se reportó en personas menores de 35 años. En el grupo etario de 18 a 24 años las personas con género femenino son las más vulnerables. El país con mayor vulnerabilidad es Guatemala donde la población joven concentra la mayoría de los casos. En los 5 países a mayor edad baja el nivel de vulnerabilidad, situación directamente relacionada con el menor uso de las plataformas y dispositivos en los migrantes digitales. Aunque los nativos digitales tienen una inmersión total a las plataformas digitales, distan mucho de tener una ciudadanía digital desarrollada, al ser la población que más reporta haber sido víctima de algún ciberdelito en los 5 países. Según datos de la encuesta los meses donde incrementa la actividad delictiva en ciberdelitos son enero, febrero y marzo, en contraposición a septiembre, mes en que existe la menor incidencia, lo que implica que el primer trimestre del año la mayoría de personas prestan menos atención a la seguridad cibernética.

5. **Situación por país**

5.1 **Costa Rica**

En la encuesta participaron 600 personas de Costa Rica, de las cuales 43% fueron nativos digitales entre 18 y 34; 57% migrantes digitales (personas de 45 años o más). Se contó con más participación de personas con género masculino en la encuesta con el 52% y 48% de personas con género femenino.

Las ocupaciones más representativas de las personas encuestadas fueron en el primer lugar profesional/ técnicos/gerentes y afines con el 32%, otros no identificado y/o desempleado el 14% y amas de casa con un 12%.

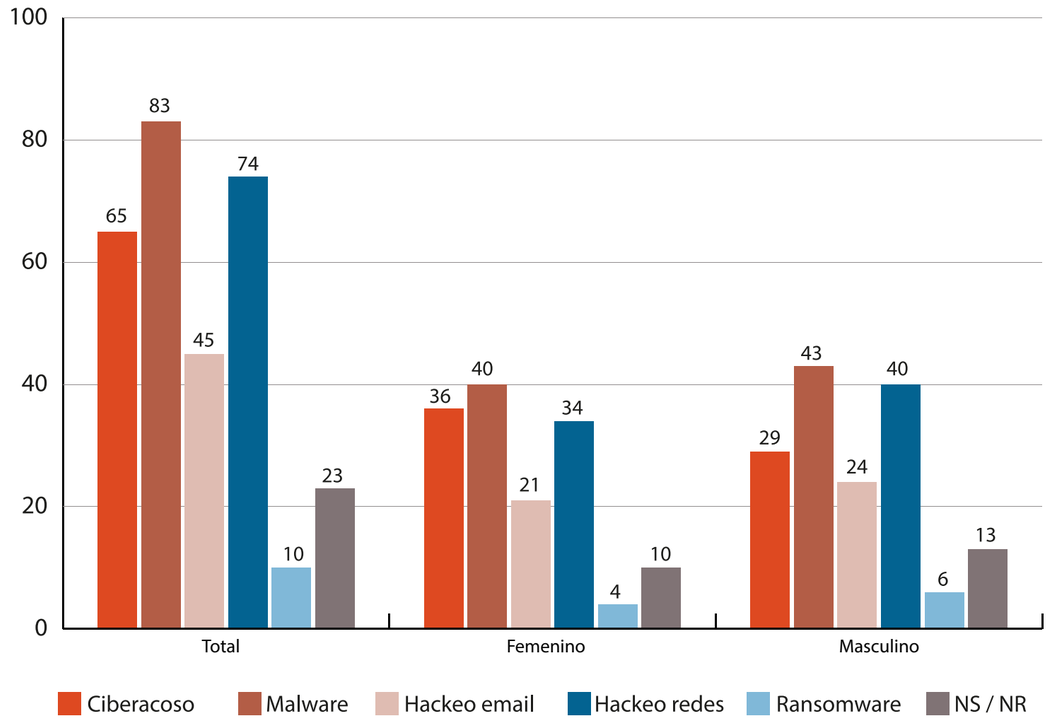
El 53 % de las personas participantes en la encuesta contaban con un nivel educativo de secundaria, 37% cuentan con nivel superior y 10 % con nivel primaria, el grupo con estudios secundarios son quienes registran mayor uso de internet. El 80% de los participantes fueron del área urbana y 20% del área rural. El 94% de las personas participantes utilizan como dispositivo un smartphone.

En relación con los datos de las redes sociales, 66% de las personas participantes no respondieron a esta pregunta, 12% reportaron utilizar las redes sociales como Facebook, Instagram, Twitter, el 7.5% utilizan mensajería instantánea como WhatsApp, Telegram, Viber, WeChat y el 1,5 % utilizan mensajes de texto (SMS).

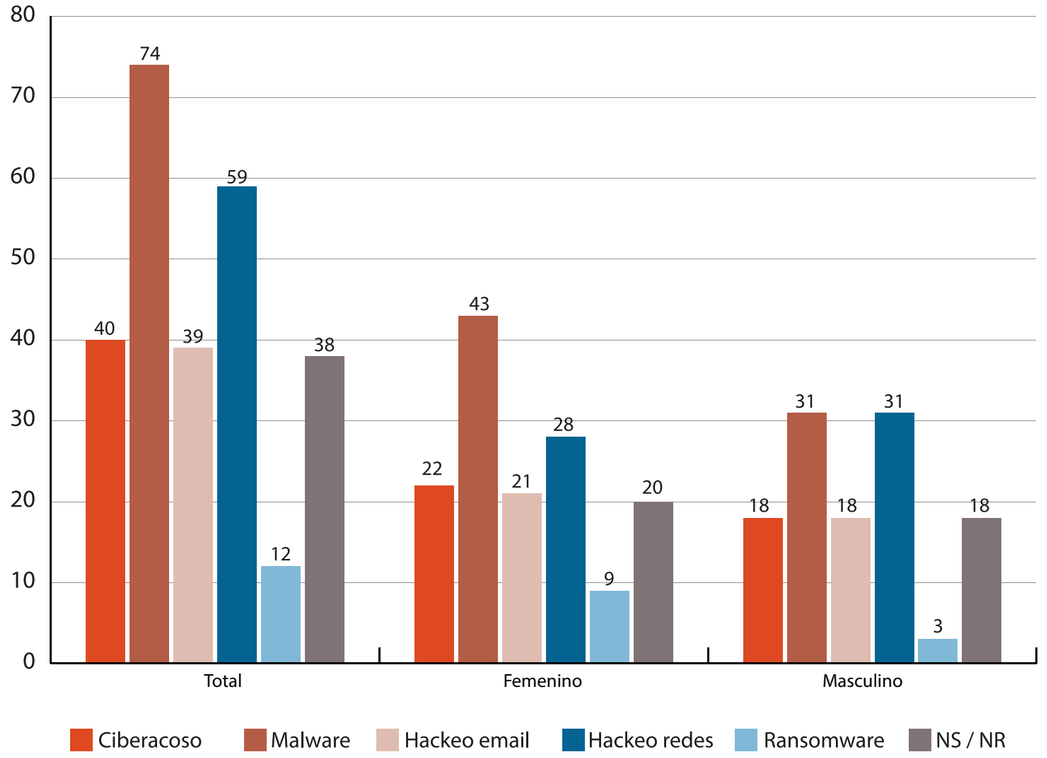
En Costa Rica existe una demanda de uso del internet en diversas plataformas que evidencia una alta participación de la población joven y personas adultas que integran en sus vidas cotidianas el uso del Internet. Las redes sociales más utilizadas son Facebook, Instagram, Twitter y el uso de la mensajería instantánea.

Gráfica 1. Costa Rica. Víctimas de ciberdelitos por rango de edad, 2021.

Gráfica 1.1. Costa Rica. Víctimas de ciberdelitos de 18 a 24, 2021.

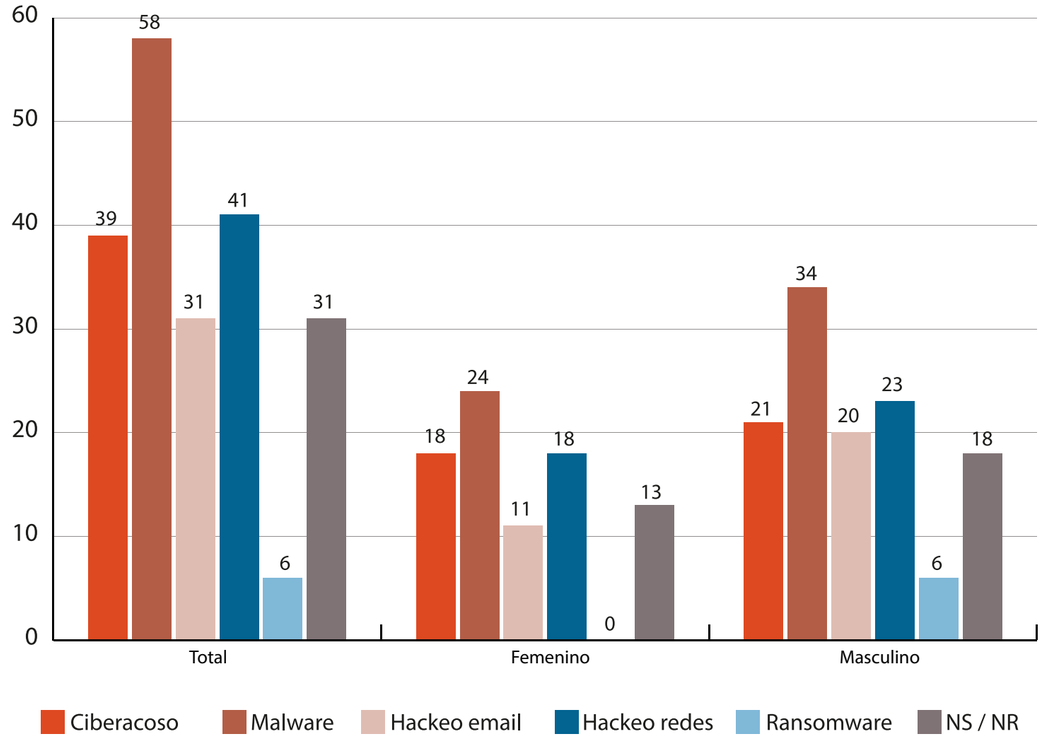


Gráfica 1.2. Costa Rica. Víctimas de ciberdelitos de 25 a 34, 2021.

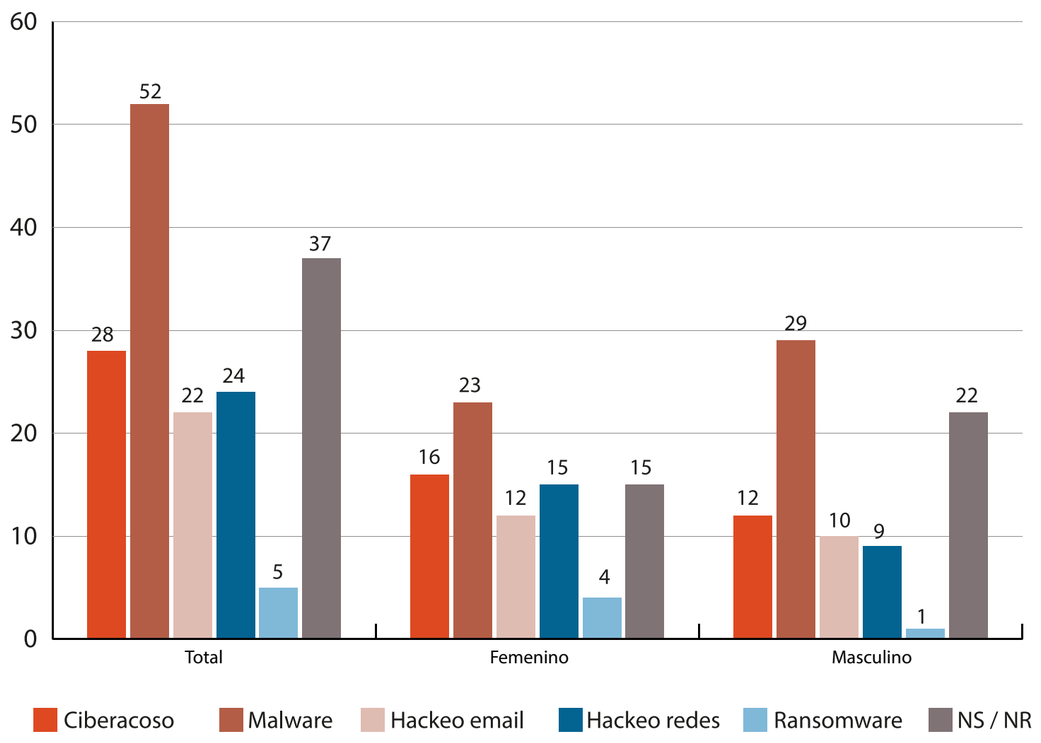


Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Gráfica 1.3. Costa Rica. Víctimas de ciberdelitos de 35 a 44, 2021.

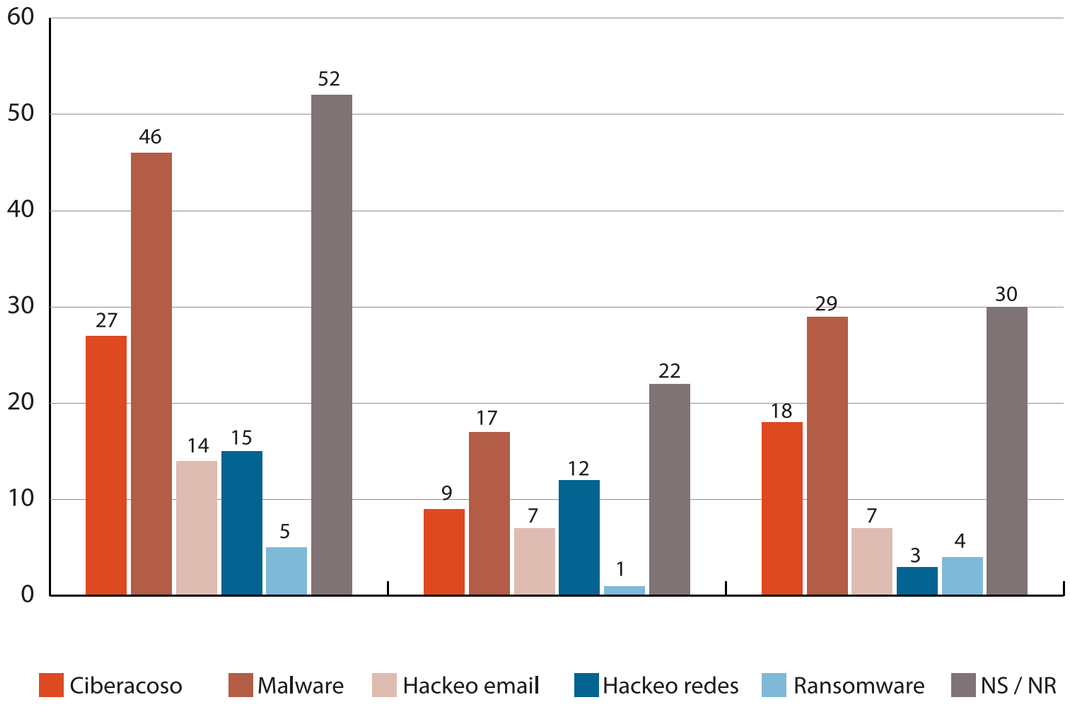


Gráfica 1.4. Costa Rica. Víctimas de ciberdelitos de 45 a 54, 2021.



Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Gráfica 1.5. Costa Rica. Víctimas de ciberdelitos de +55, 2021.



Fuente: elaboración propia con base en la encuesta de PNUD 2021.

De acuerdo con los datos de la Gráfica 1, el grupo etario que presenta mayor vulnerabilidad son las personas entre 18 y 24 años, pues son quienes reportan haber sido víctimas de ciberdelitos en más casos. El ciberdelito del que se reportan más casos es malware, con 313 personas que respondieron ser víctimas, en segundo lugar el hackeo en redes y en tercer lugar ciberacoso. Al ser el grupo etario nacido en la era digital, se observa un bajo nivel en el conocimiento de seguridad digital, falta de alfabetización digital y de mecanismos adecuados para identificar riesgos y vulnerabilidades. La carencia de habilidades de ciudadanía digital hace que no se cuente con mecanismos eficaces de prevención.

Situación jurídica

En Costa Rica la Ley No. 8148 del 2001 de la Asamblea Legislativa de la República de Costa Rica generó una adición al código penal, incluye los artículos 196 bis, 217 bis y 229 bis, promulgados para reprimir y sancionar los delitos informáticos, a continuación, sus textos:

> Artículo 196 bis. -Violación de comunicaciones electrónicas. Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese (sic.), modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones des-

critas en el párrafo anterior son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos (Asamblea Legislativa de la República de Costa Rica, 2022).

Artículo 217 bis. -Fraude informático. Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema (Asamblea Legislativa de la República de Costa Rica, 2022).

Artículo 229 bis. -Alteración de datos y sabotaje informático. Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese (sic.), borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.

Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años (Asamblea Legislativa de la República de Costa Rica, 2022).

Convenios

Costa Rica en 2017, fue el segundo país de Centroamérica en adherirse al Convenio de Budapest.

Desafíos

- El uso de lenguaje muy técnico en el Código Penal de Costa Rica, puede hacer que los ciudadanos, al ser víctimas, no reconozcan la conducta como un delito. Con lo cual se debe mediar la información para conseguir que llegue a la ciudadanía en general.
- Promover que los proveedores de servicios electrónicos e internet, sean aliados clave para facilitar, en el marco de la investigación de delitos informáticos, que se comprenda la importancia de la evidencia digital, así como su cadena de custodia, máxime en casos de acoso cibernético o pornografía infantil.
- Estructurar y fortalecer al personal que investiga y persigue delitos informáticos para la atención de delitos vinculados con la tecnología.
- Lograr que, en el sistema de justicia, se comprenda la importancia de la evidencia digital, su cadena de custodia y la importancia de salvaguardar la información.
- Desarrollar la ciudadanía digital de los ciudadanos en general, para conseguir que tengan una alfabetización digital, la cual ayude a prevenir el ciberdelito.

- La conectividad ha aumentado en los últimos años, sin embargo, se deben concretar y aligerar proyectos de infraestructura que amplíen la cobertura territorial y el ancho de banda.
- Impulsar mecanismos para conseguir que las personas puedan saber qué hacer al momento de ser víctimas de ciberdelitos.

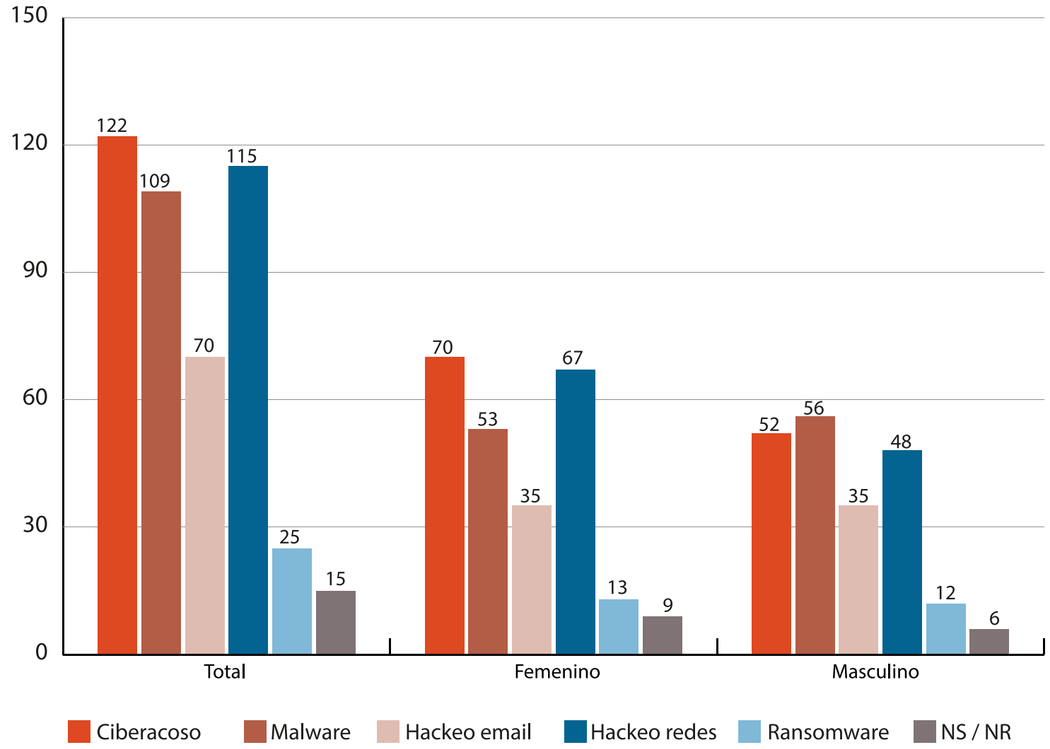
5.2 **El Salvador**

En la encuesta participaron 600 personas, con una paridad en la participación por género. El 82% de las personas encuestadas eran del área urbana y 18% del área rural, el 68% fueron nativos digitales personas menores de 34 años y 32% migrantes digitales de 35 años y más. La mayor participación fue del rango de edad 18 hasta 44 años, que se han adaptado a los procesos de hiperconectividad aumentado por el Covid-19, donde la virtualidad de los procesos para responder a necesidades básicas como el trabajo, estudio, salud y comercio se agilizó.

En relación con el nivel educativo, participaron 48% con nivel superior, 47% con el nivel secundario y 5% con nivel primario. Las principales ocupaciones de las personas participantes fueron: 31% estudiantes, 16% profesionales/técnicos/gerentes, 15.5% empleados de oficina y afines y 15% no identificado/desempleado, 9.1% amas de casa, 8.6% comerciantes y vendedores, principalmente. El 96% de las personas encuestadas utilizan como dispositivo el smartphone. El 19% utilizan mensajería instantánea (WhatsApp, Telegram, Viber, WeChat) y el 18% de las personas dijeron usar plataformas de redes sociales como Facebook, Instagram o Twitter.

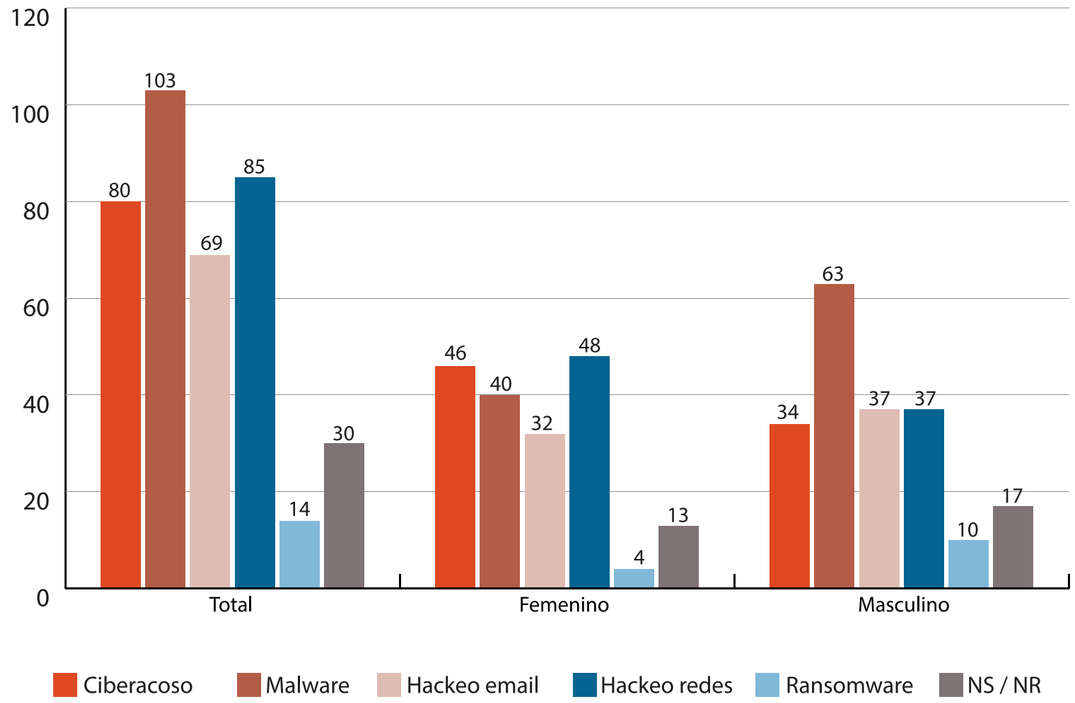
Gráfica 2. El Salvador. Víctimas de ciberdelitos por rango de edad, 2021.

Gráfica 2.1. El Salvador. Víctimas de ciberdelitos de 18 a 24, 2021.

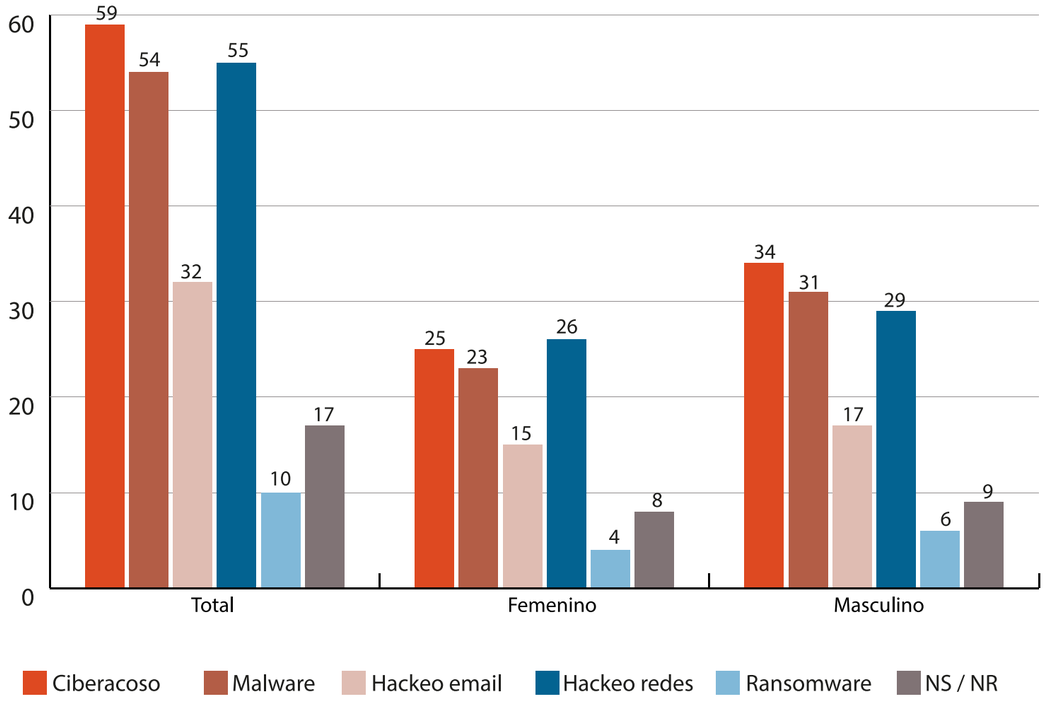


Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Gráfica 2.2. El Salvador. Víctimas de ciberdelitos de 25 a 34, 2021.

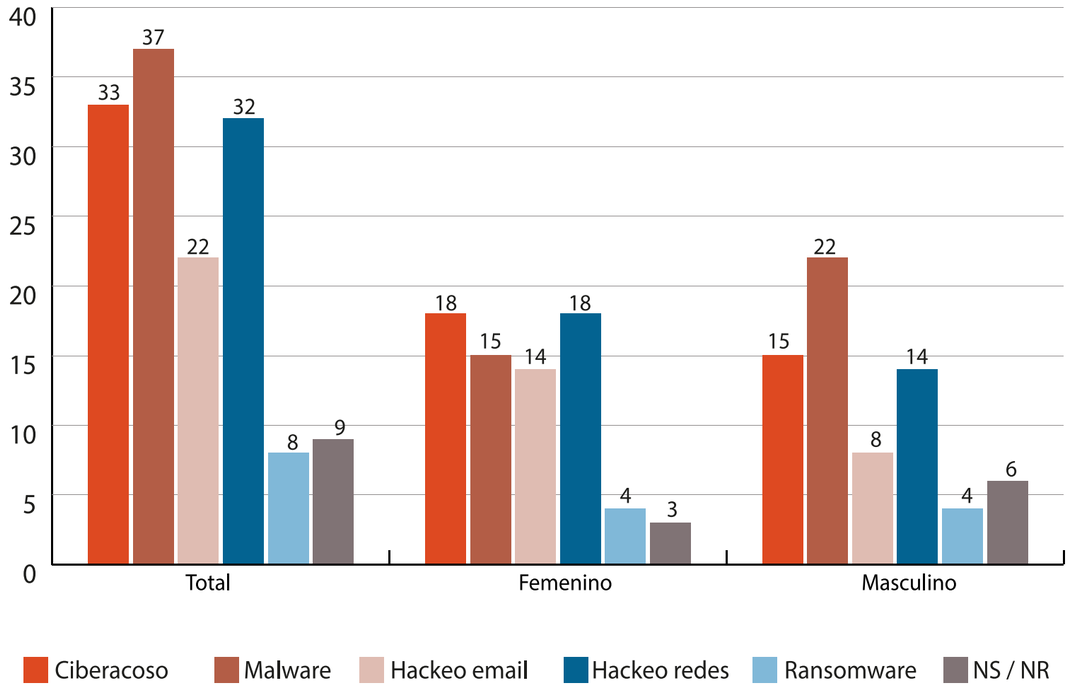


Gráfica 2.3. El Salvador. Víctimas de ciberdelitos de 35 a 44, 2021.

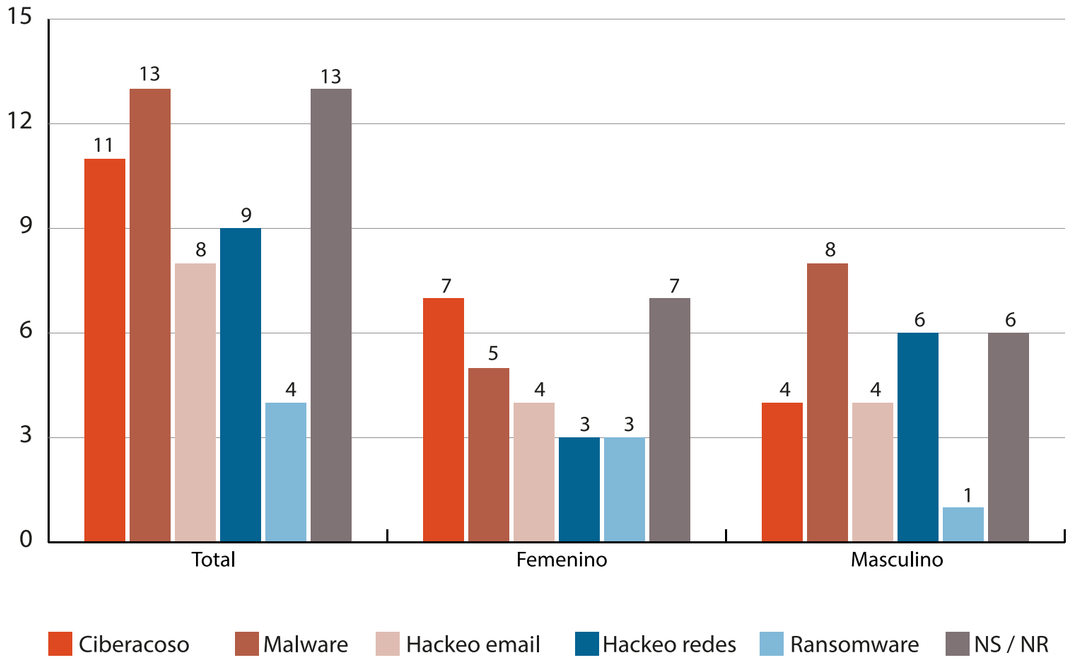


Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Gráfica 2.4. El Salvador. Víctimas de ciberdelitos de 45 a 54, 2021.



Gráfica 2.5. El Salvador. Víctimas de ciberdelitos de +55, 2021.



Fuente: elaboración propia con base en la encuesta de PNUD 2021.

En El Salvador los ciberdelitos de los cuales han sido víctimas más personas, en relación con la Gráfica 2, son: primero el malware con 316 casos reportados, segundo ciberacoso con 305 resultados y el tercer lugar hackeo en redes con 296. Las víctimas se concentran en las personas entre 18 y 34 años, donde los menores de 24 presentan mayor vulnerabilidad, pues son quienes más casos reportan. El hecho que el malware sea el delito más frecuente denota la carencia de alfabetización digital en relación con los virus, ciberseguridad y mínimos de seguridad para navegar y analizar los riesgos cibernéticos a los que se puede estar expuesto. En general, es necesario trabajar procesos donde la ciudadanía digital se desarrolle en su integralidad.

Situación jurídica

El Salvador cuenta con una Ley Especial Contra los Delitos Informáticos y Conexos, tiene como objetivo proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las TIC, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas en los términos aplicables y previstos en la presente ley.

Se clasifican dentro de la ley aludida:

- Delitos contra los sistemas tecnológicos de información.
- Delitos informáticos.
- Delitos informáticos relacionados con el contenido de los datos.
- Delitos informáticos contra niñas, niños y adolescentes o personas con discapacidad.
- Delito contra el orden económico.

Convenios

Las autoridades han planteado su intención de adherirse al Convenio de Budapest. En una reunión reciente del Foro de Presidentes de Poderes Legislativos de Centroamérica y la Cuenca del Caribe (Foprel), sus miembros se comprometieron a priorizar en sus agendas la adhesión al Convenio y a legislar por la adaptación de las leyes nacionales a los estándares internacionales.

Desafíos

El Salvador ha experimentado una mayor cobertura de internet y, con ello, la ciudadanía emplea con mayor intensidad las TIC. Esto implica una corresponsabilidad en generar herramientas que fortalezcan la ciudadanía digital, en pro de disminuir el número de víctimas de ciberdelitos.

A medida que le nivel de cobertura de internet avanza en el país, también se incrementa el número de ilícitos facilitados por Internet, es impor-

tante lograr que el avance sea proporcional en la alfabetización digital y en las herramientas digitales.

Es importante que el Código Procesal Penal desarrolle e integre todo el contenido de evidencia digital, de cara a que todos los actores de la línea de justicia estén familiarizados con la preservación y el tratamiento de dicha evidencia. Así como capacitar a la línea de justicia en el adecuado tratamiento de las evidencias digitales y su cadena de custodia.

Asegurar que los funcionarios de las instituciones de seguridad y justicia cuenten con los recursos necesarios para aplicar la ley.

Lograr que los nativos y migrantes digitales conozcan la ley y cómo proceder si son víctimas de ciberdelitos.

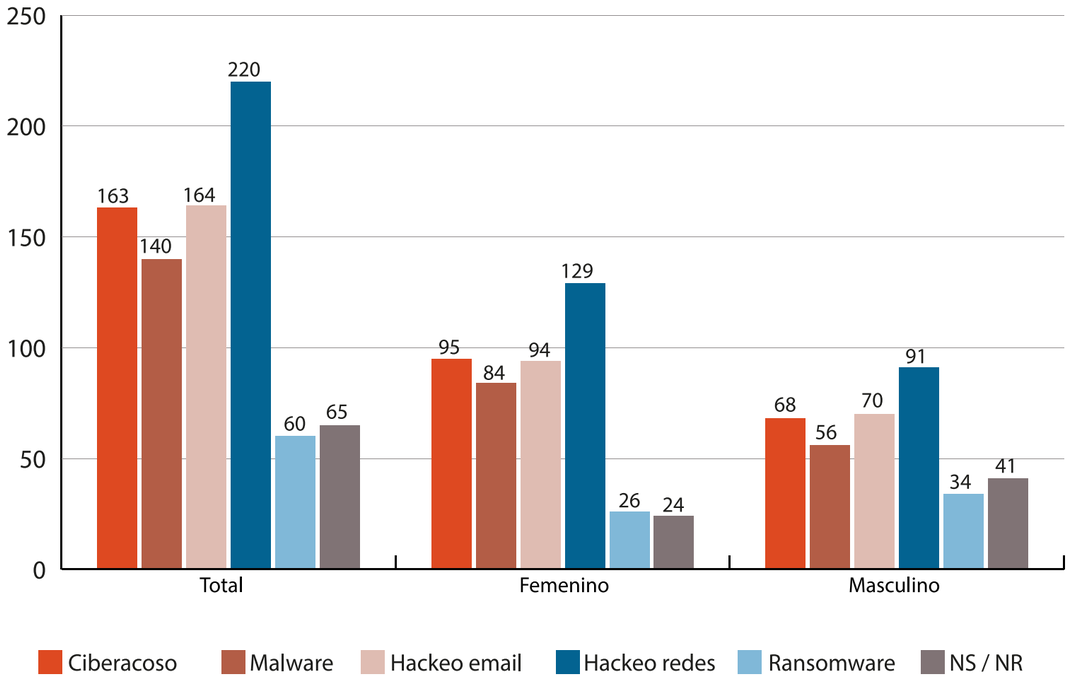
5.3 **Guatemala**

En la encuesta participaron 600 personas, de las cuales el 56% eran femeninas y 44% masculinas, el 70% población del área urbana y 30% del área rural. El 46% fueron personas de 18 a 24 años, el 28% personas de 25 a 34 años, con lo cual el 74% de la muestra son nativos digitales y el 26% migrantes digitales (personas de 35 años o más). La mayor participación fue del rango de edad 18 a 44 años, quienes se han adaptado a los procesos de hiperconectividad generados en parte por la pandemia de Covid-19, lo que llevó a una acelerada virtualización de bienes y servicios. En relación con el nivel educativo de las personas encuestadas el 74% cuenta con nivel secundaria, 21% nivel superior y 5% en el nivel primario. Las principales ocupaciones de las personas participantes son: 21% estudiantes, 21% amas de casa, 15% empleados de oficina y afines, 12.5% comerciantes y vendedores. En relación con el tipo de dispositivo, el 90% utiliza un smartphone. Las principales redes sociales utilizadas son Facebook, Instagram y Twitter.

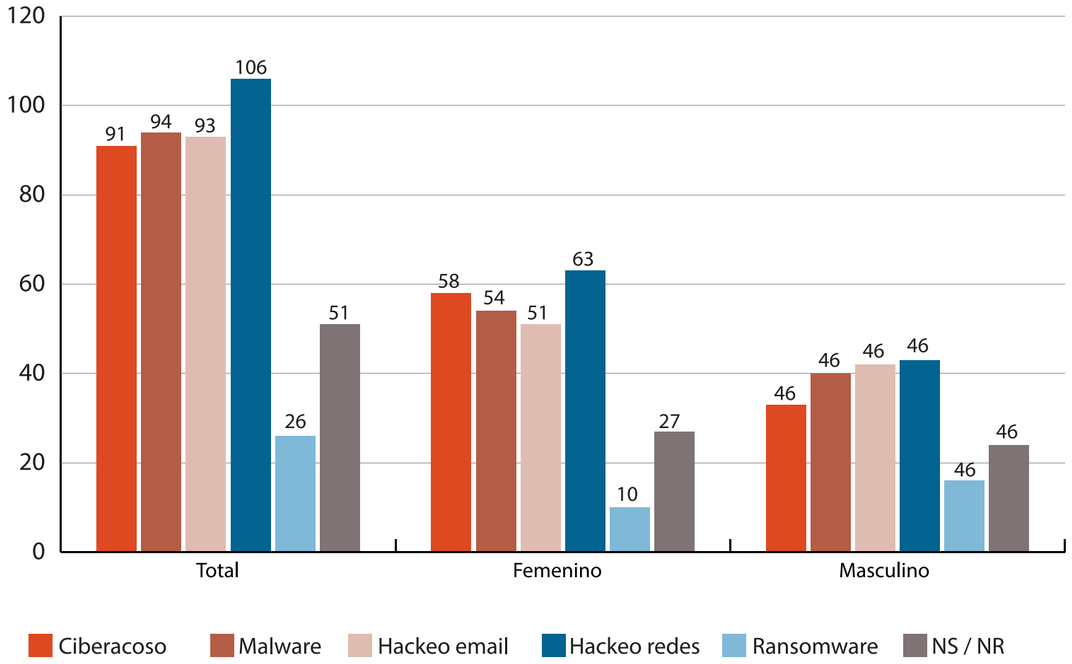
Guatemala es el país donde se reportaron más casos de ciberdelitos, (ver Gráfica 3) en la encuesta 416 expresaron haber sido víctimas de hackeo en redes, 333 personas fueron víctimas de ciberacoso y 327 personas sufrieron hackeo email. Además, a diferencia de los países anteriores, la violencia digital de género muestra una diferencia constante en la incidencia de victimización. Lo cual insta a poner atención e indagar los niveles de riesgo y brechas de seguridad entre los géneros, ya que la violencia basada en género, la cual se da en el entorno comunidad, se traslada a la esfera digital. Aunado a ello, los 5 ciberdelitos priorizados en la encuesta no cuentan con una tipificación especifica en el país, también existe una carencia de datos estadísticos institucionalizados, como en el caso del ciberacoso, esta falta de información sobre estos ciberdelitos a nivel de país hace que el desarrollo de procesos de minimización de riesgos y acceso a la información para desarrollar la ciudadanía digital de los jóvenes se constituya en un obstáculo.

Gráfica 3. Guatemala. Víctimas de ciberdelitos por rango de edad, 2021.

Gráfica 3.1. Guatemala. Víctimas de ciberdelitos de 18 a 24, 2021.

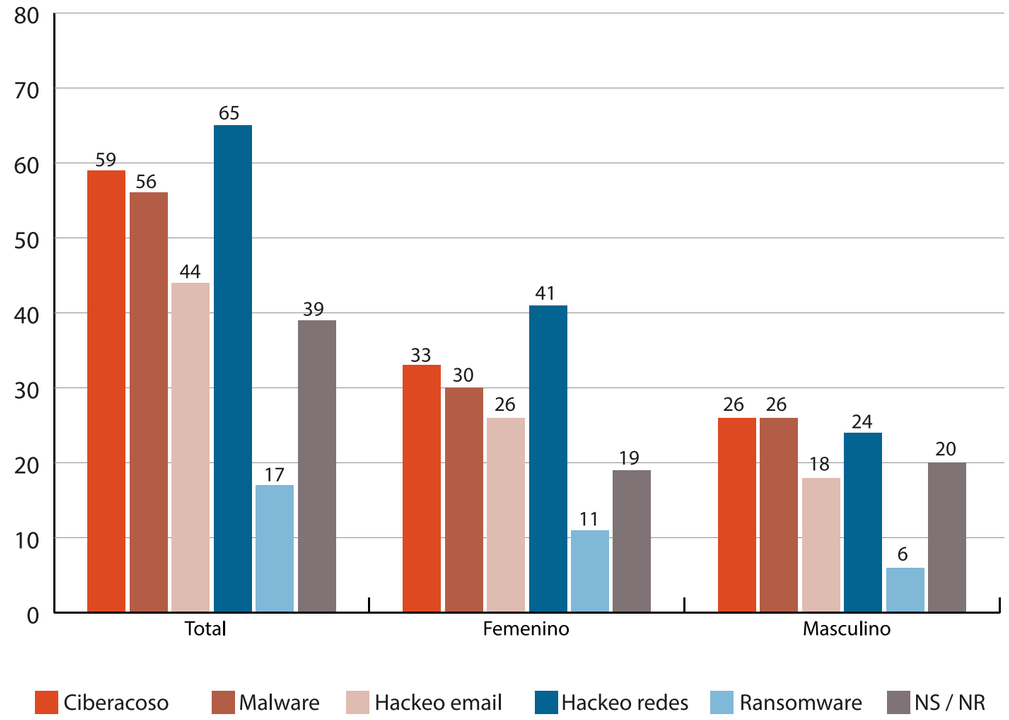


Gráfica 3.2. Guatemala. Víctimas de ciberdelitos de 25 a 34, 2021.

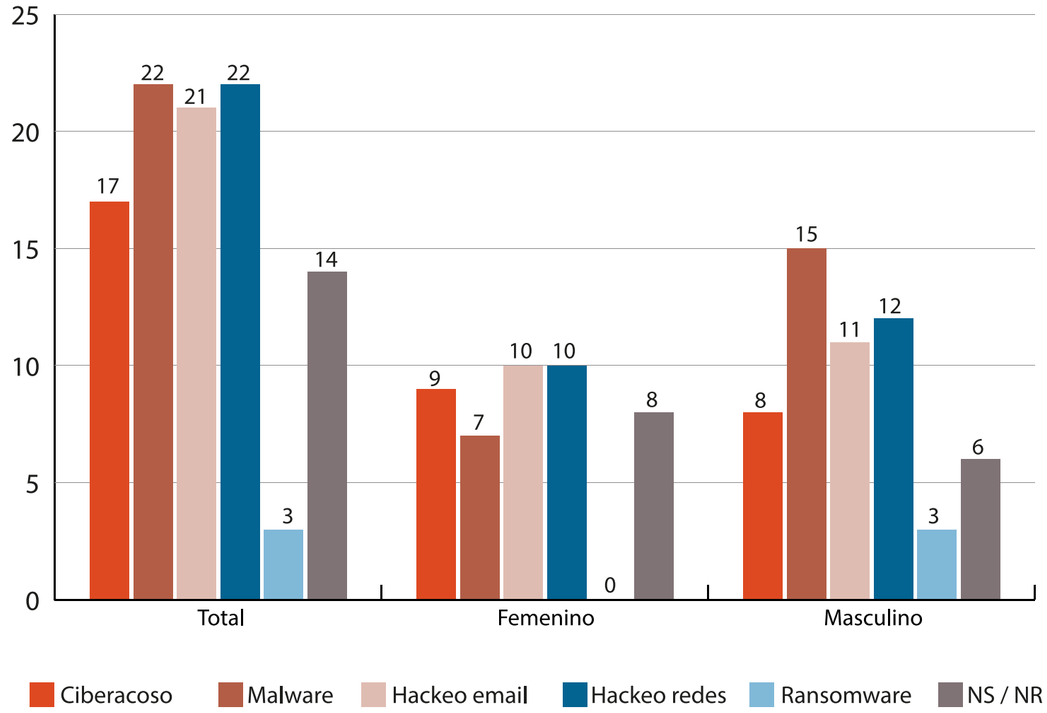


Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Gráfica 3.3. Guatemala. Víctimas de ciberdelitos de 35 a 44, 2021.

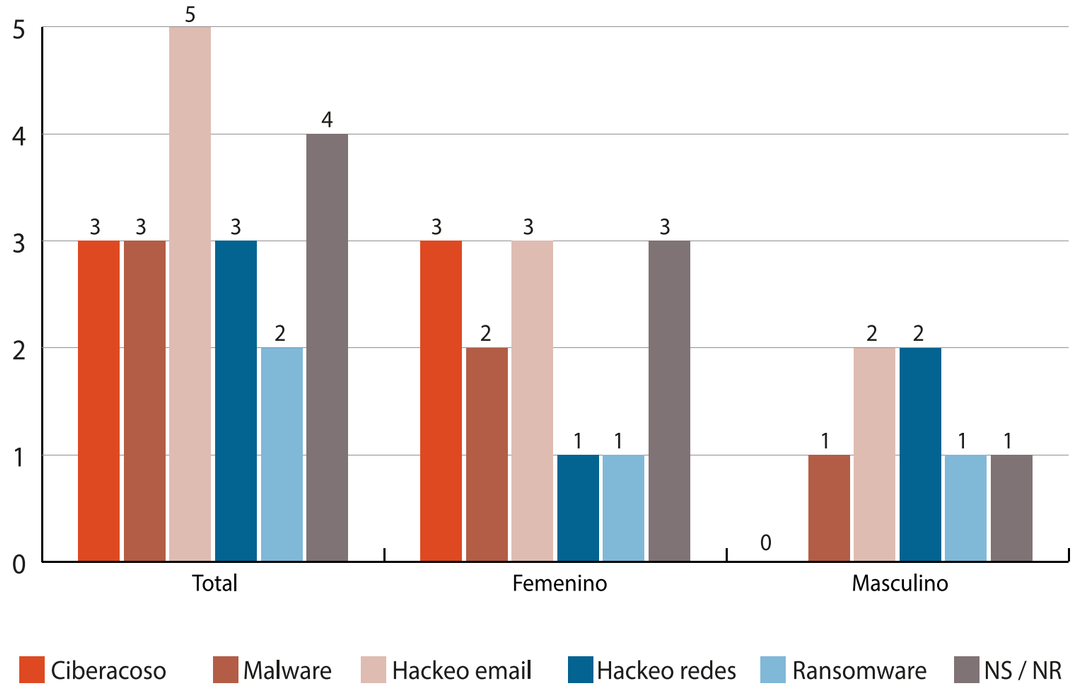


Gráfica 3.4. Guatemala. Víctimas de ciberdelitos de 45 a 54, 2021.



Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Gráfica 3.5. Guatemala. Víctimas de ciberdelitos de +55, 2021.



Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Situación jurídica

El 4 de agosto de 2022, el Congreso de la República emitió el Decreto Número 39-2022 en el que aprobó la Ley de Prevención y Protección contra la Ciberdelincuencia, que creaba figuras delictivas y adecuaba normas penales frente a delitos cibernéticos, pero recibió varias objeciones de diversos sectores, motivo por el cual no se convirtió en ley.

En el año 2022, con el Decreto 11-2022, se realizan reformas al Código Penal, que persiguen y castigan los hechos en contra la niñez y adolescencia. Entre las modificaciones fue añadido el Artículo 190 Bis al Código Penal, para tipificar el delito de seducción mediante el uso de las tecnologías de información contra niños, niñas y adolescentes, con penas de seis a doce años de prisión a quienes utilicen cualquier ardid, engaño, argucia, presión o amenaza, para contactar a un menor o a una tercera persona, con la finalidad de obtener material con contenido sexual o pornográfico donde participen menores de edad.

Se cuenta con legislación conexa que regula algunos ciberdelitos. En el código penal, decreto 17-73, en el artículo 274 de la literal "A" a la "H", se encuentra tipificado el delito de destrucción de registros informáticos, alteración de programas, reproducción de instrucciones o programas de computación, registros prohibidos, manipulación de información, uso de información, programas destructivos, entre otros. También la ley contra la violencia sexual, explotación y trata de personas, contempla que ciertos delitos sobre indemnidad sexual puedan ser utilizados medios, incluidos los tecnológicos, para ubicar o comunicarse con la víctima.

Convenios

Guatemala realizó la solicitud de adhesión al convenio de Budapest con el objetivo de establecer una política penal común y alineada entre países, orientada a la protección de la sociedad contra la ciberdelincuencia. Esto se alcanza al tipificar los delitos informáticos de forma similar en todas las naciones, de tal manera que se unifiquen las normas procesales y se implementen.

Guatemala cuenta con una Estrategia Nacional de Seguridad Cibernética. El documento data del año 2018 y fue elaborado por el Ministerio de Gobernación con la colaboración con más de 160 representantes de los distintos sectores de la sociedad guatemalteca (Ipandetec, 2020).

Desafíos

- Alto nivel de oposición a la Ley de Prevención y Protección contra la Ciberdelincuencia, por lo cual se requiere analizar y trabajar con varios sectores, de forma articulada, para evitar ir contra otros derechos y libertades.
- La carencia de una ley de ciberdelitos que contemple todas sus formas hace que muchas conductas delictivas queden en la impunidad.
- Aun cuando existen unidades ciber en el país, una en la Policía Nacional y otra en el Ministerio Público, las rutas de denuncia son poco sociabilizadas y están naturalizadas muchas formas de violencia y delitos cibernéticos dentro de la población, además de la baja cultura judicial de manejo de la cadena de custodia de la evidencia digital.
- Desarrollar una ciudadanía digital plena y priorizar el alfabetismo digital para toda la población, pero principalmente para los nativos digitales que según los datos parecen ser huérfanos digitales.
- En relación con el acceso a la seguridad y justicia, existen carencias en los procesos de investigación y judicialización de casos de ciberdelitos y manejo de la evidencia digital.
- El personal de investigación, fiscales y jueces se encuentran limitados con la legislación actual para la persecución penal de los ciberdelitos, además de una resistencia a utilizar la evidencia digital.

5.4 **Honduras**

En la encuesta realizada participaron 600 personas, se contó con más participación de personas de género masculino (53% versus 47% femenino), 86% de las personas que forman parte de la muestra fueron del área urbana y 14% del área rural.

En relación con la participación etaria, 38% fueron personas que tenían entre los 18 y 24 años, 34% de 25 a 34 años, con lo cual los nativos digitales que participaron fueron 72% y los migrantes digitales del 28% (personas de 35 años o más). El rango etario de mayor participación fue de personas entre los 18 y 44 años, lo cual evidencia los procesos acelerados de virtualización durante la pandemia Covid-19. El nivel educativo de las personas encuestadas es: 58% con nivel secundaria, 28% en el nivel superior y 14% nivel primario. El 94% utiliza

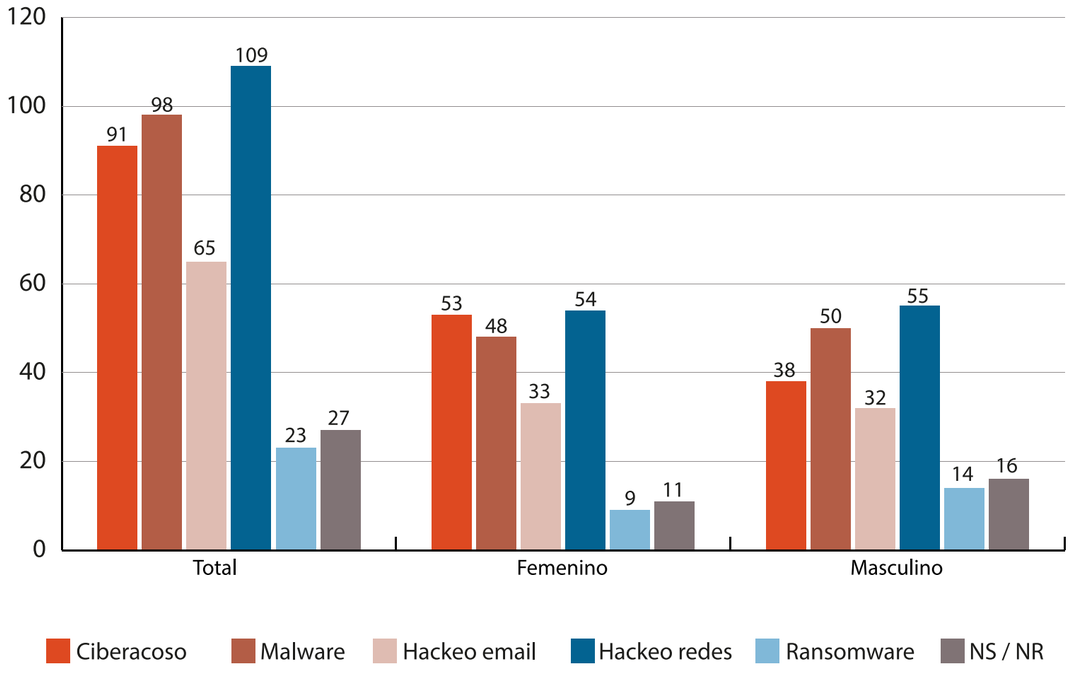
como dispositivo digital un smartphone. Las redes sociales más utilizadas son Facebook, Instagram y Twitter.

Las principales ocupaciones de las personas participantes fueron: 26% comerciantes y vendedores, 16% estudiantes, 15% amas de casa, 11% profesional/ técnicos/gerentes y afines, 10% empleados de oficina y afines, 9% otros no identificaron/desempleado, 7% artesanos/operarios especiales, 5% obreros y jornaleros.

En Honduras los ciberdelitos más reportados, en concordancia con la Gráfica 4, fueron malware con 274 personas víctimas, el segundo con más frecuencia fue hackeo de redes con 266 casos y el tercer lugar ciberacoso con 220 reportes. En Honduras, a diferencia de los países anteriores, la vulnerabilidad es similar en número de las personas de 18 a 44 años, lo que hace que, sin una diferencia muy amplia entre nativos digitales y migrantes digitales, se evidencia la carencia de desarrollo de ciudadanías digitales plenas. En el caso de ciberacoso en población de 18 a 24 años se ve una diferencia sustancial en cuanto a la violencia de género digital hacia la población femenina en las plataformas digitales. La interacción en redes es alta, pero sin seguridad digital, lo que genera mayor riesgo de hackeo de redes, máxime cuando la inmersión digital por el Covid-19 se generó de forma acelerada, con lo cual muchas personas, sin alfabetización digital, interactúan a diario en las redes sociales sin ser conscientes de los peligros y, en algunos casos, sin tomar medidas de seguridad en su actuar.

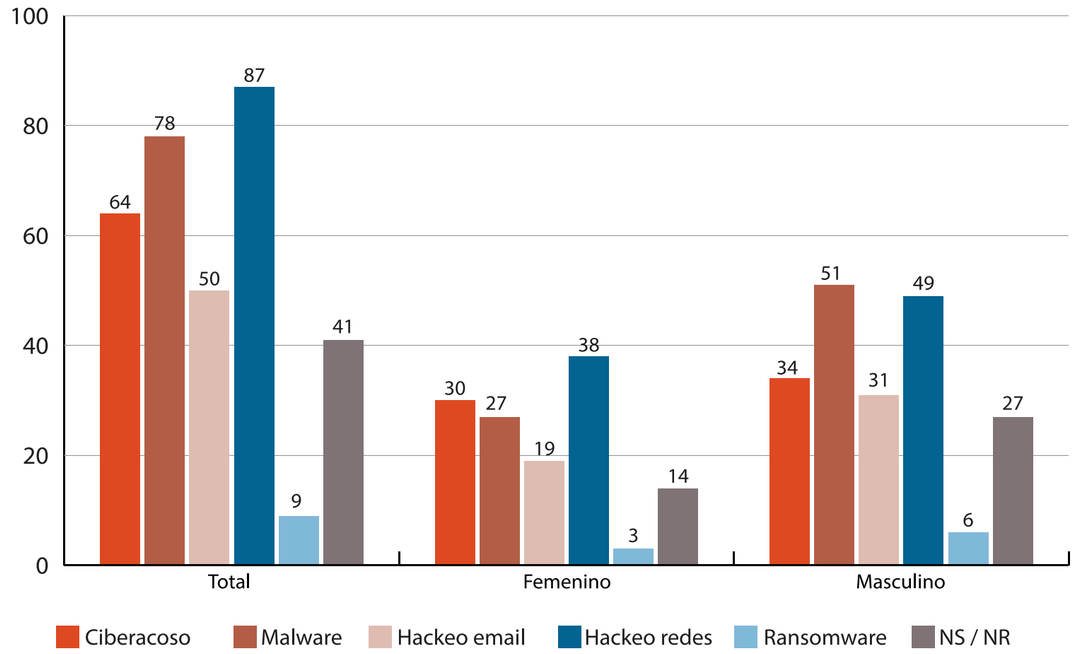
Gráfica 4. Honduras. Víctimas de ciberdelitos por rango de edad, 2021.

Gráfica 4.1. Honduras. Víctimas de ciberdelitos de 18 a 24, 2021.

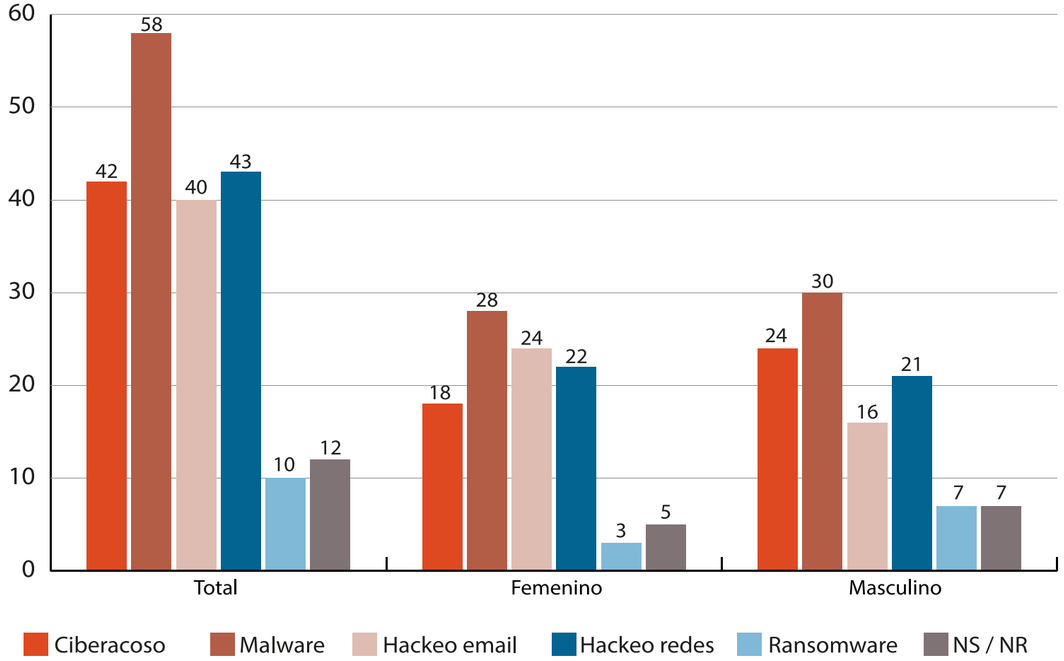


Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Gráfica 4.2. Honduras. Víctimas de ciberdelitos de 25 a 34, 2021.

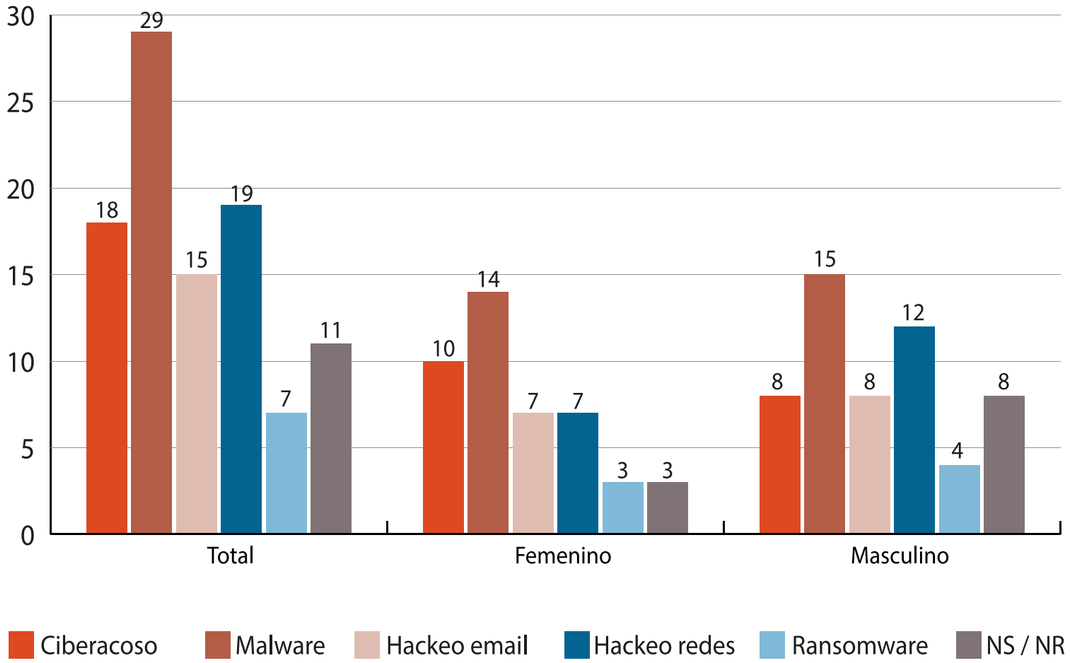


Gráfica 4.3. Honduras. Víctimas de ciberdelitos de 35 a 44, 2021.

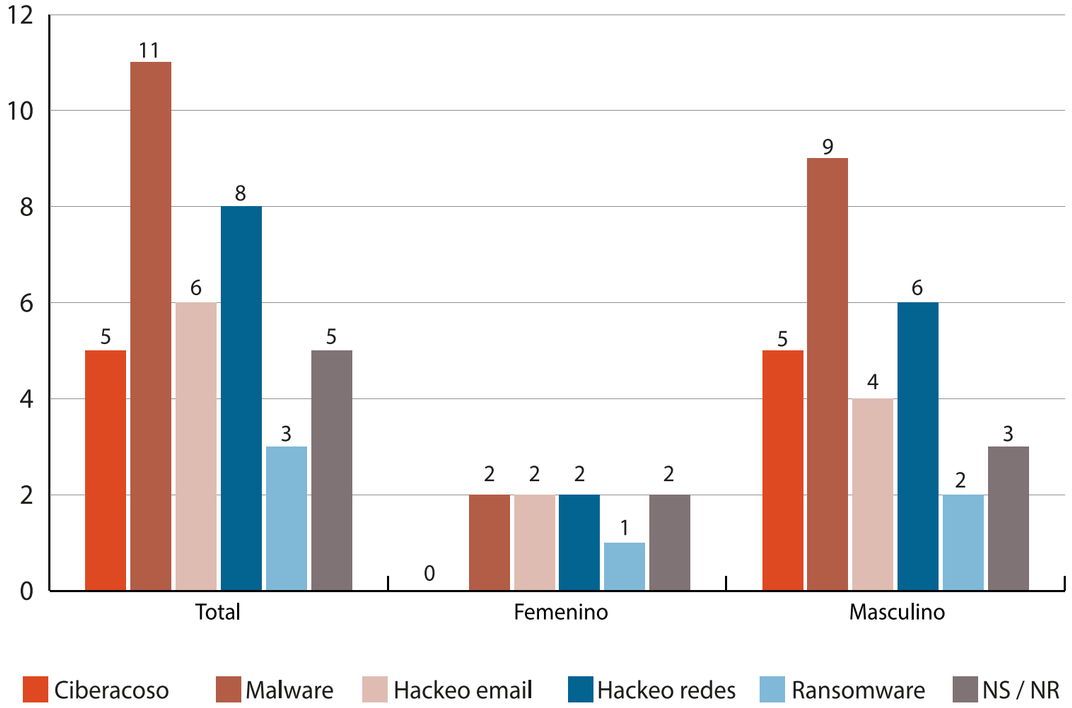


Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Gráfica 4.4. Honduras. Víctimas de ciberdelitos de 45 a 54, 2021.



Gráfica 4.5. Honduras. Víctimas de ciberdelitos de +55, 2021.



Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Situación jurídica

En Honduras el Código Penal Decreto No. 130-2017 Vigente a partir del 25 de junio de 2020, contiene legislación aplicable en materia de seguridad informática, el cual regula los delitos de incitación a la discriminación, amenazas, chantajes, contacto con finalidad sexual con menores de edad por medios electrónicos, hostigamiento sexual, elaboración y utilización de pornografía infantil, provocación sexual, descubrimiento y revelación de secretos, revelación de secreto profesional, extorsión, delitos contra el derecho de autor y los derechos conexos, descubrimiento y revelación de secreto industrial y comercial, acceso no autorizado a sistemas informáticos, daños a datos y sistemas informáticos, suplantación de identidad, difusión de noticias o rumores falsos, falsificación de tarjetas bancarias y cheques de viaje, usurpación de la personalidad de otro, solicitud de actos de contenido sexual, espionaje y ciberterrorismo o terrorismo electrónico.

Se regula mediante un Comité Interinstitucional de Ciberseguridad, el cual es encargado de desarrollar e implementar la Estrategia Nacional de Ciberseguridad.

Convenios

Honduras cuenta con recomendaciones del Congreso Nacional para la adhesión al convenio de Budapest.

Desafíos

- Lograr el desarrollo de una ciudadanía digital en las personas de 18 a 55 años.
- Se requiere que el sistema de justicia logre incorporar mecanismos de práctica forense digital y evidencia digital como parte de los procesos judiciales.
- Capacitar al personal de investigación, fiscales y jueces para la debida aplicación de la reforma del Código Penal Decreto No. 130-2017 Vigente a partir del 25 de junio de 2020.
- Socializar con la población en general tanto la ruta de denuncia como los mecanismos de prevención para evitar ser víctima de ciberdelitos.
- Implementar estrategias de atención diferenciadas y especializadas para víctimas de ciberdelitos.

5.5 República Dominicana

En la encuesta participaron 600 personas, se contó con una participación mayor de personas con género femenino (51% versus 49% masculino), el 89% de la muestra es de área urbana y el 11% de área rural.

De las personas participantes el 35% se encontraban en el rango de 18 a 24 años, el 32% de 25 a 34 años, con lo cual el 67% de la población parte de la muestra eran nativos digitales. El 33% de las personas participantes fueron migrantes digitales (personas de 35años o más). Respecto al nivel educativo de las perso-

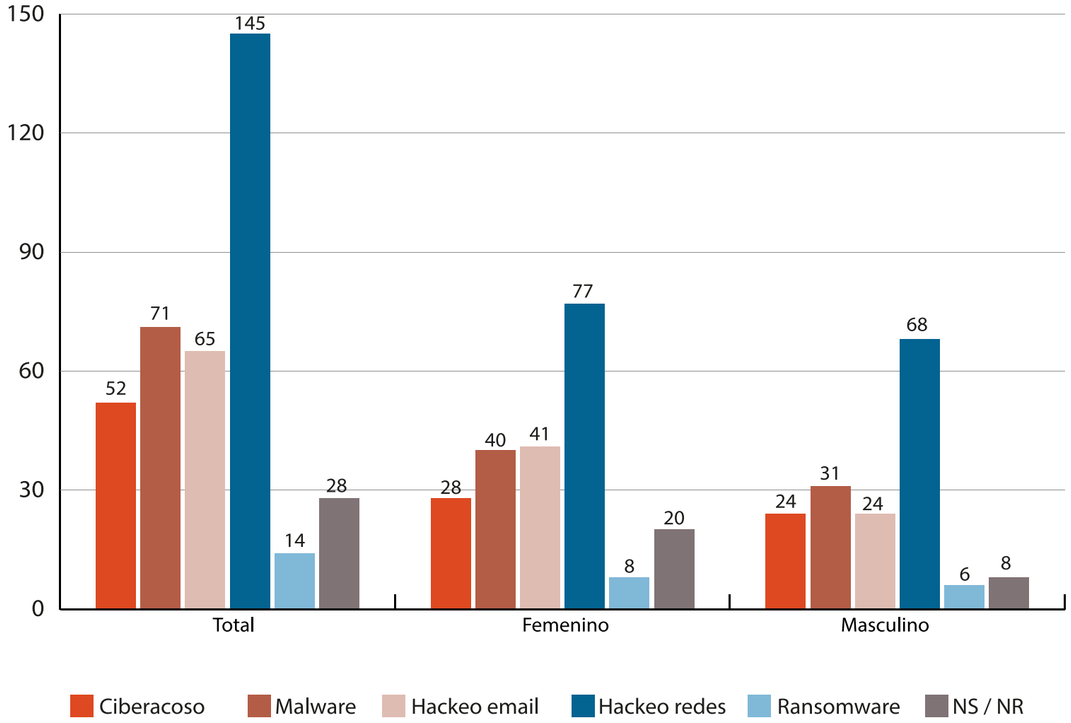
nas participantes, se observa que 62% contaba con nivel secundaria, el 33% con nivel superior y 5% con nivel primario.

Las principales ocupaciones de las personas participantes fue 21% otros no identificado/desempleado, 19% estudiantes, 17% amas de casa, 16% comerciantes y vendedores, 14% empleados de oficina y afines, 7% profesional/ técnicos/gerentes y afines, 3% obreros y jornaleros. El 96% utiliza como dispositivo digital un *smartphone*.

En República Dominicana, la frecuencia más alta de ciberdelito reportado fue la de hackeo de redes con 373 víctimas, los grupos etarios más vulnerables son las personas de 18 a 24 años y de 25 a 34 años, lo cual está correlacionado con la interacción en redes sociales. El segundo ciberdelito más reportado es malware con 211 casos reportados, seguido de hackeo de email con 188 reportes. (ver Gráfica 5) La muestra indica una interacción desde la huerfanidad digital, donde la mayoría utilizan herramientas digitales, pero no son conocedores de las implicaciones de las interacciones, de la seguridad, sus riesgos y vulnerabilidades.

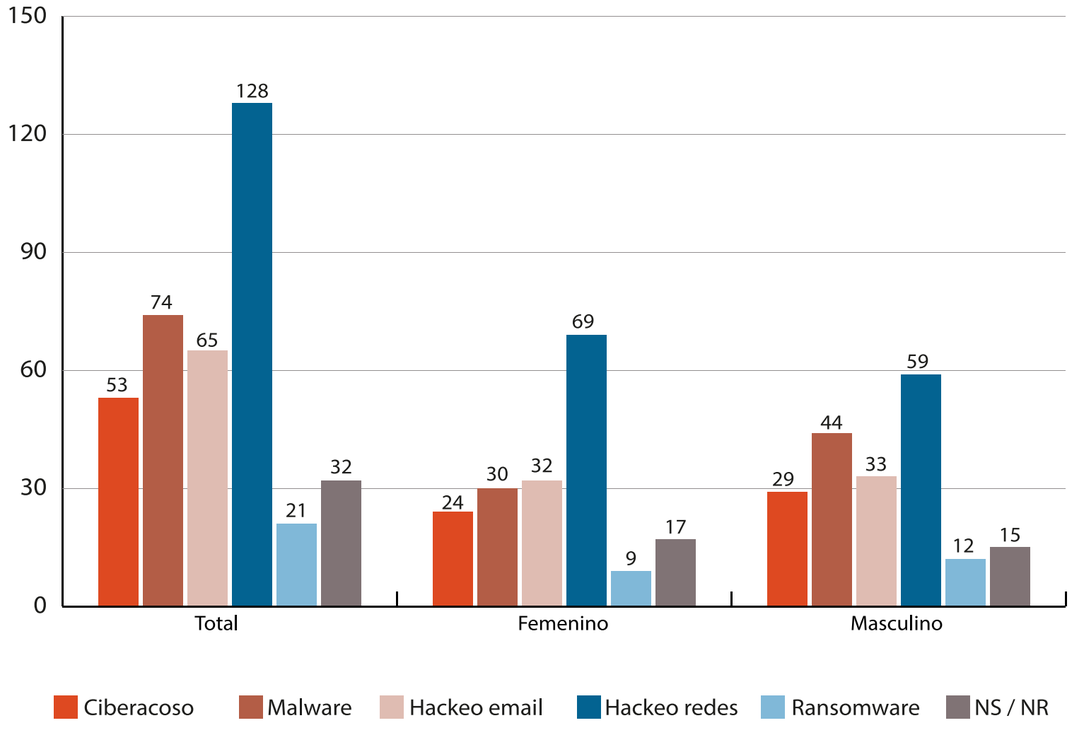
Gráfica 5. República Dominicana. Víctimas de ciberdelitos por rango de edad, 2021.

Gráfica 5.1. República Dominicana. Víctimas de ciberdelitos de 18 a 24, 2021.

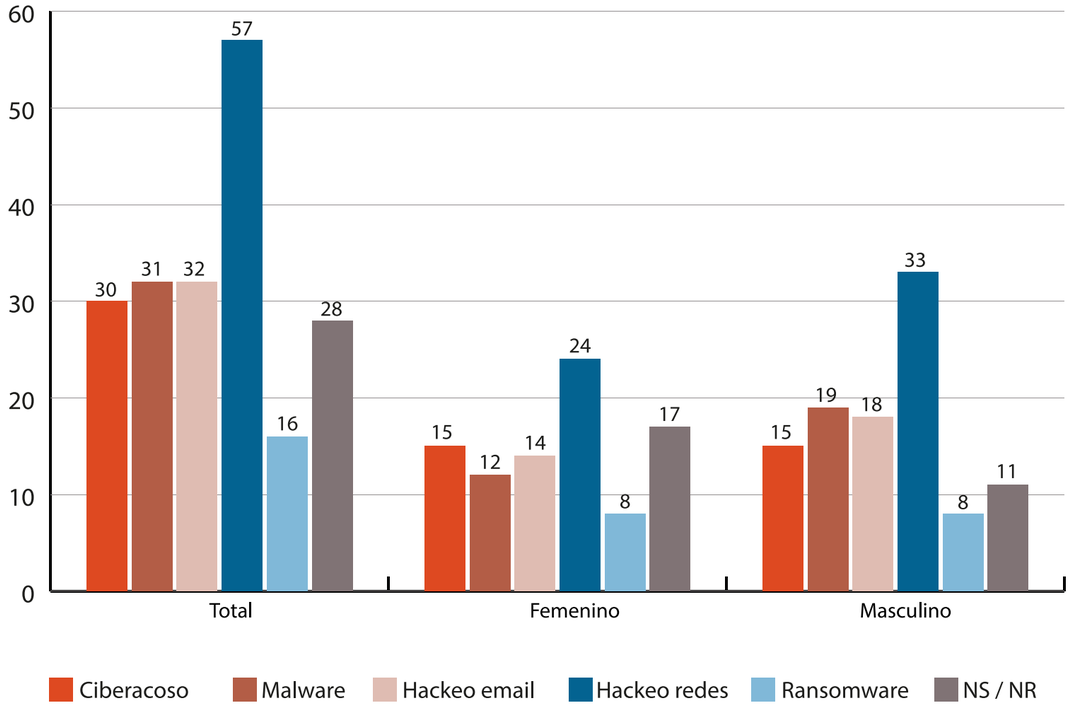


Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Gráfica 5.2. República Dominicana. Víctimas de ciberdelitos de 25 a 34, 2021.

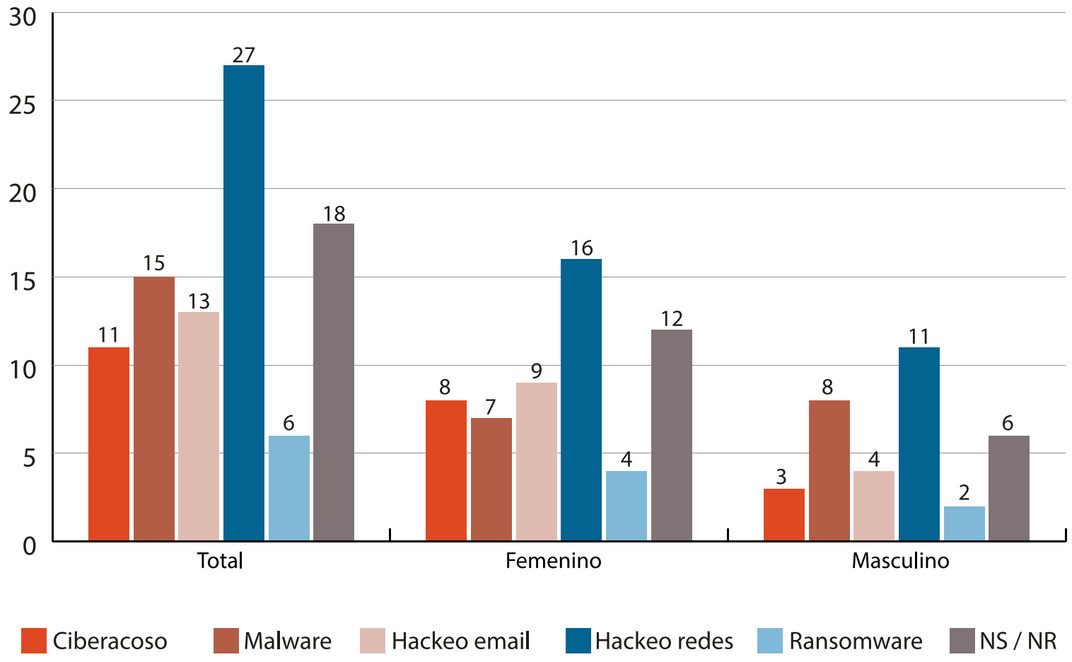


Gráfica 5.3. República Dominicana. Víctimas de ciberdelitos de 35 a 44, 2021.

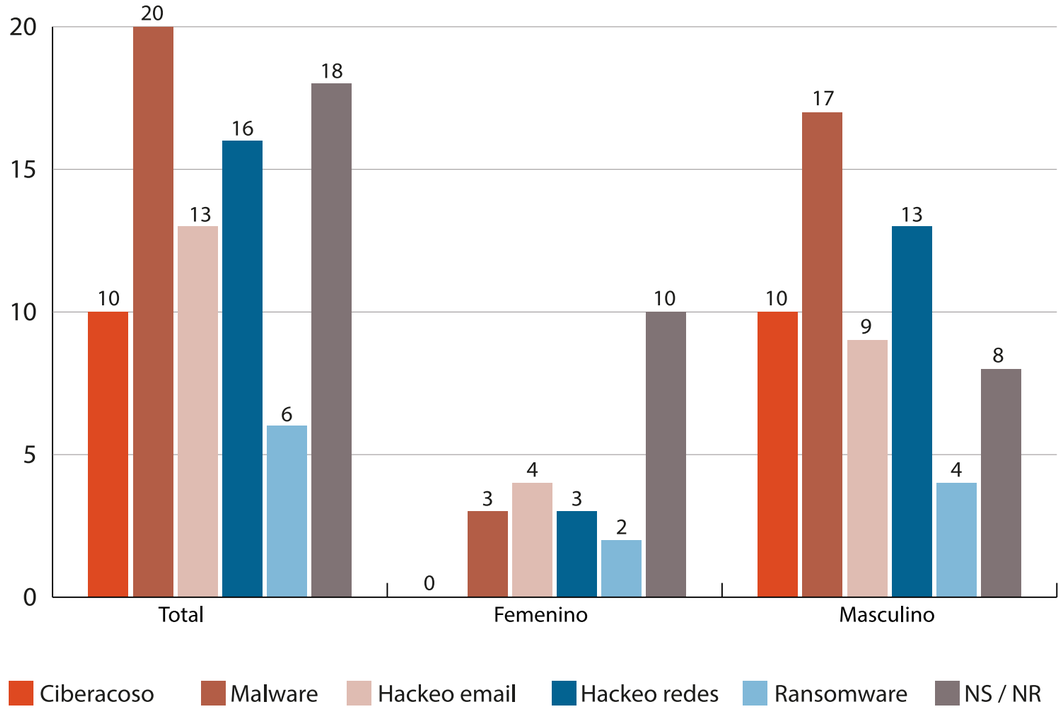


Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Gráfica 5.4. República Dominicana. Víctimas de ciberdelitos de 45 a 54, 2021.



Gráfica 5.5. República Dominicana. Víctimas de ciberdelitos de +55, 2021.



Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Situación jurídica

República Dominicana cuenta con la Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología. La ley tipifica delitos de contenido, delitos de propiedad intelectual, delitos contra las telecomunicaciones.

Disposiciones específicas:

- Acceso ilícito: Artículo 6
- Interceptación ilícita: Artículo 9
- Interferencia en los Datos: Artículo 10
- Interferencia en el Sistema: Artículo 11
- Abuso de Dispositivos: Artículo 8
- Falsificación Informática: Artículo 18
- Fraude Informático: Artículos 13 - 16
- Pornografía Infantil: Artículo 24
- Infracciones de la Propiedad Intelectual y de los Derechos afines: Artículo 25

Convenios

República Dominicana es signataria del Convenio sobre Ciberdelincuencia del Consejo de Europa. Fue el primer país de la región centroamericana en formar parte de este tratado internacional. Por otro lado, se adhirió al llamamiento de París para la confianza y la seguridad en el ciberespacio. Se propone una visión multisectorial de la regulación en el ciberespacio y de los grandes principios relacionados a ella. Cabe destacar que República Dominicana es uno de los 75 países firmantes, uno de los pocos de América Latina.

Desafíos

- Fomentar la denuncia para conseguir que los ciberdelitos sean investigados, entre ellos los casos más comunes, tales como chantajes y ciberacosos.
- Aplicar una política penal común, encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.
- Fortalecer a la ciudadanía con información de ciberseguridad, con el fin de no ser víctimas en el uso de sus dispositivos digitales y reducir la brecha digital.

6. **Análisis Victimológico**

Las personas que participaron en la encuesta muestran un bajo nivel de desarrollo de su ciudadanía digital, por lo cual la mayoría carece de alfabetización digital. Para muchos su relación con la tecnología corresponde a la necesidad de cubrir funciones de relacionamiento, trabajo, estudio y se omiten e se ignoran los riesgos en las plataformas digitales.

Es importante establecer que, como en el mundo físico, la intersección de categorías protegidas[2] puede generar más vulnerabilidad. En las plataformas digitales la violencia puede ser diferenciada y en algunos casos, como la violencia digital de género, es una réplica de las formas de violencia y dominación de la sociedad.

Aunado a lo anterior, la brecha digital marca una serie de desigualdades entre las personas que acceden a la tecnología y a las plataformas digitales, en la mayoría de países las personas que viven en zonas rurales carecen de conectividad, acceso a la tecnología, en los 5 países el dispositivo más utilizado es un smartphone.

Así como existen desigualdades en relación con la zona del país donde se encuentre, se presentan disparidades en razón del género, etnia, nivel de educación y situación económica. El acceso a internet, aunque se transformó con la pandemia Covid-19 en un servicio esencial, el acceso y conectividad no es accesible para toda la población debido a los costos. Cuando se entrecruzan factores como la brecha digital, los índices de pobreza y género se denota cómo las mujeres en el sector TIC son mucho menos en proporción a los hombres. La tecnología, su acceso y conectividad depende mucho de la situación económica individual, la primera barrera para lograr que se desarrolle la ciudadanía digital plena y, con ello, la participación e interacción en el mundo digital.

Romper la brecha digital de género requiere que la mayoría de las mujeres tengan acceso a información veraz y accesible sobre los nueve aspectos de la ciudadanía digital, además de estar informadas de cómo hacer frente a situaciones de violencia y criminalidad en las plataformas digitales.

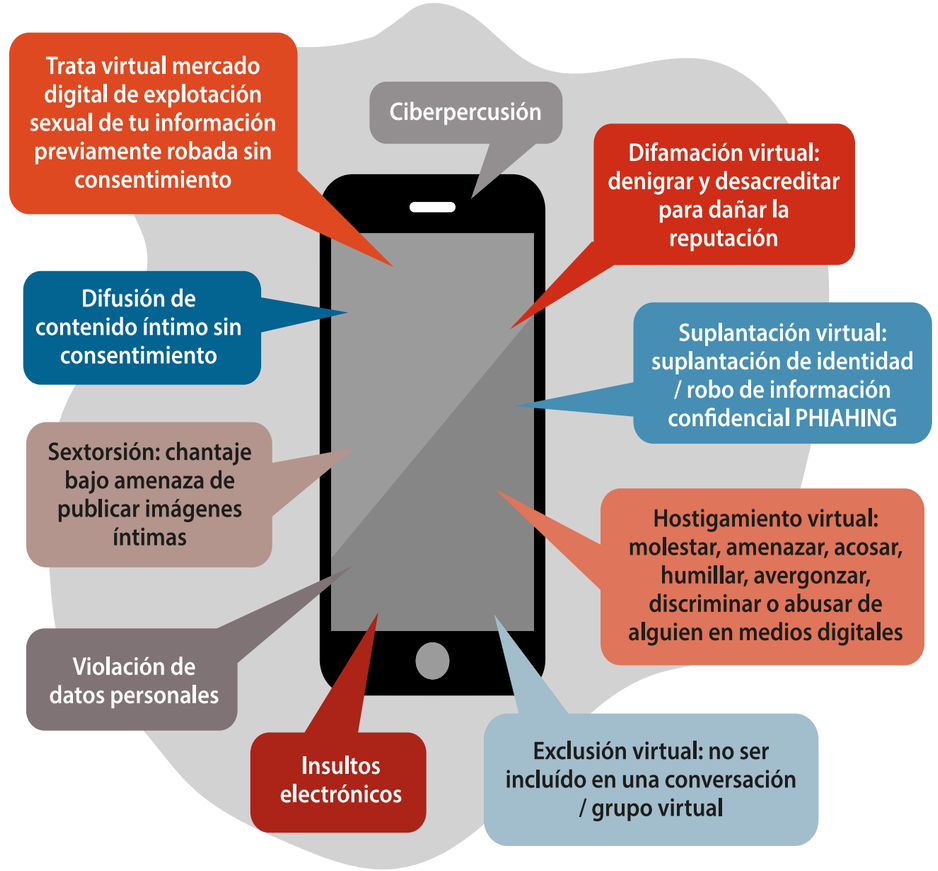
2 Categoría protegida: son categorías reconocidas por los derechos humanos basadas en el principio de no discriminación, las que protegen a las personas en sus derechos frente a cualquier distinción que se haga con base en raza, género, sexo, origen étnico, nacionalidad, religión, lengua, orientación sexual, identidad de género, expresión de género discapacidad, edad y cualquier otra categoría reconocida por el DDHH.

Es necesario comprender que todas las personas, máxime en época de Covid-19, se han vuelto ciudadanos digitales. Por tanto, disminuir los niveles de vulnerabilidad en las plataformas, sobre todo de la población más joven, exige que se tenga acceso a todos los elementos de la ciudadanía digital y que se pueda comprender el internet de las cosas y el mundo hiperconectado en el que actualmente se desenvuelven.

Comprender los riesgos en internet precisa lograr ver cuándo las situaciones de violencia van en aumento y es necesario buscar mecanismos para salir de esos espacios de violencia. Sin embrago, también es importante comprender que estas conductas en las redes son un espejo de las realidades sociales.

Por ello es importante que las personas desnaturalicen las violencias digitales (ver Ilustración 2) y adquieran herramientas para identificar todos estos mecanismos de violencia y control que pueden darse en relación con los dispositivos y el Internet.

Ilustración 2. Violencias digitales



Fuente: elaboración propia.

Pero además de estas violencias existen riesgos que afectan la salud física y psicológica de las personas, así como la perspectiva del mundo:

Ilustración 3. Riesgos psicológicos

Fuente: elaboración propia.

Como se muestra en la Ilustración 3, existen diversidad de riesgos psicológicos, desde la ansiedad por perderse algo en el ciberespacio, la dependencia al teléfono y perderse de los momentos por prestar más atención al teléfono que a las personas, la adicción a la tecnología priorizada sobre acciones básicas para la vida como comer o dormir, así como la vigilancia a otras personas; son todas modificaciones conductuales que pueden afectar las habilidades psicosociales de las personas.

De similar forma, el cuerpo (ver Ilustración 4) siente los efectos del uso desproporcionado de la tecnología, de forma que existe una exposición prolongada a la luz azul. El uso de dispositivos en la noche repercute en la calidad del sueño de las personas, aunado a la mala postura debido al descuido de la ergonomía mientras se utilizan dispositivos electrónicos, lo cual afecta la salud, principalmente el cuello y la espalda. Cuidar la salud física, tanto como la mental mientras se interactúa con la tecnología, es fundamental para desarrollar el bienestar digital.

Ilustración 4. Riesgos físicos

Fuente: elaboración propia.

Los riesgos relacionados con la información, como lo muestra la Ilustración 5, están relacionados al registro de intereses que la huella digital de una persona deja en el ciberespacio, con lo cual, la información a la que tiene acceso de forma directa y filtrada es aquella que se relaciona con sus intereses propios, por lo cual dos personas que buscan la misma información tendrán acceso a diferentes fuentes, aquellas que se identifiquen más con sus hábitos de navegación, lo cual implica pérdida de objetividad, normalmente las personas en el ciberespacio se relacionan con aquellas fuentes y referencias más afines a su imaginario social, lo que conlleva a perder información de aquellos que no comparten sus mismos intereses. Otro riesgo es el acceso a información falsa, carente de sustento científico, que se viraliza y, en muchas ocasiones, condiciona el imaginario social en relación a un tema determinado.

Ilustración 5. Riesgos relacionados con la información

Fuente: elaboración propia.

Establecer cómo son las víctimas y los victimarios en los ciberdelitos, debido a las diversas conductas delictivas en la plataforma digital, sumado a la hiperconectividad que intercepta múltiples factores, es un trabajo complejo y los datos no dan les acceso a información de perfilación, no existe un perfil de víctima y agresor estándar, depende mucho de cada caso.

En relación con la violencia digital de género estudios de la OEA, han establecido que los agresores tienen por lo general una identidad masculina en la mayoría de los casos la víctima conoce o identifica a su agresor que le crea un ambiente hostil en línea (OEA, 2021;OEA y Cicte, 2020).

Parte de la dificultad para caracterizar tanto a la víctima como al agresor se estructura a partir del hecho que la mayoría de personas carece de ciudanía digital, muchas tienen vulnerabilidades de seguridad en sus dispositivos, por ejemplo no utilizan antivirus, usan la misma contraseña para varias cuentas o redes, existe una proliferación del internet de las cosas y las personas carecen de alfabetización digital en el uso de dispositivos inteligentes en el hogar, vehículo u oficina, lo cual provoca que se genere una masificación de víctimas debido a la conectividad mundial. De manera que casi cualquier individuo huérfano digital puede ser una potencial víctima.

Tabla 7. Víctimas ciberdelitos por país 2021

Cantidad de víctimas de ciberdelitos por país						
Víctimas de ciberdelito	**Costa Rica**	**El Salvador**	**Guatemala**	**Honduras**	**República Dominicana**	**Total**
No	399	293	265	378	441	1776
No sabe/ No responde	2	2	2	2	3	11
Si	199	305	333	220	156	1213
Total	**600**	**600**	**600**	**600**	**600**	**3000**

Fuente: elaboración propia con base en la encuesta de PNUD 2021.

De conformidad con la Tabla 7, 1213 personas que conforman la muestra, de un total de 3000 de los 5 países, afirmaron haber sido víctimas de ciberdelitos, el 27% de Guatemala, el 25% de El Salvador, 18% Honduras, 17% Costa Rica y 13% de República Dominicana, en términos de seguridad ciudadana el triángulo norte sigue registrando mayor incidencia victimológica.

Se preguntó a las personas participantes en la encuesta si identificaron a su agresor, 273 víctimas identificaron al agresor. Con respecto a la relación con el agresor, del universo de 273, el 28% señaló que era amigo, 19% desconocidos, 10% esposo/a, pareja, 9% compañero/a de estudios (escuela, universidad, etc.), 8% exesposo/a, expareja, 6% vecino, 5% alguien con quien trabajaba y 1% un familiar. En estos casos los agresores cuentan con datos personales (correos, número telefónico o de WhatsApp) o son parte de las amistades en redes sociales de las víctimas. Los agresores pertenecen al círculo primario de las víctimas, (ver Tabla 8) lo que implica cierto grado de confianza a la hora de facilitar información sensible como las claves de acceso a correos, acceso a dispositivos digitales y números de cuentas de tarjetas o cuentas bancarias.

Tabla 8. Identificación y relación con el agresor 2021

Identificación y relación del agresor	Cantidad
Amigo (en ese momento)	78
No tenía/tengo ninguna relación (desconocido)	52
Otro (específica)	30
Esposo/a, pareja (en ese momento)	26
Compañero/a de estudios (escuela, universidad, etc.) (en ese momento)	24
Ex-esposo/a, ex-pareja (en ese momento)	23
Vecino (en ese momento)	17
Alguien con quien trabajaba (en ese momento)	14
Familiar	4
Ninguna	4
No sabe / no contesta	1

Fuente: elaboración propia con base en la encuesta de PNUD 2021.

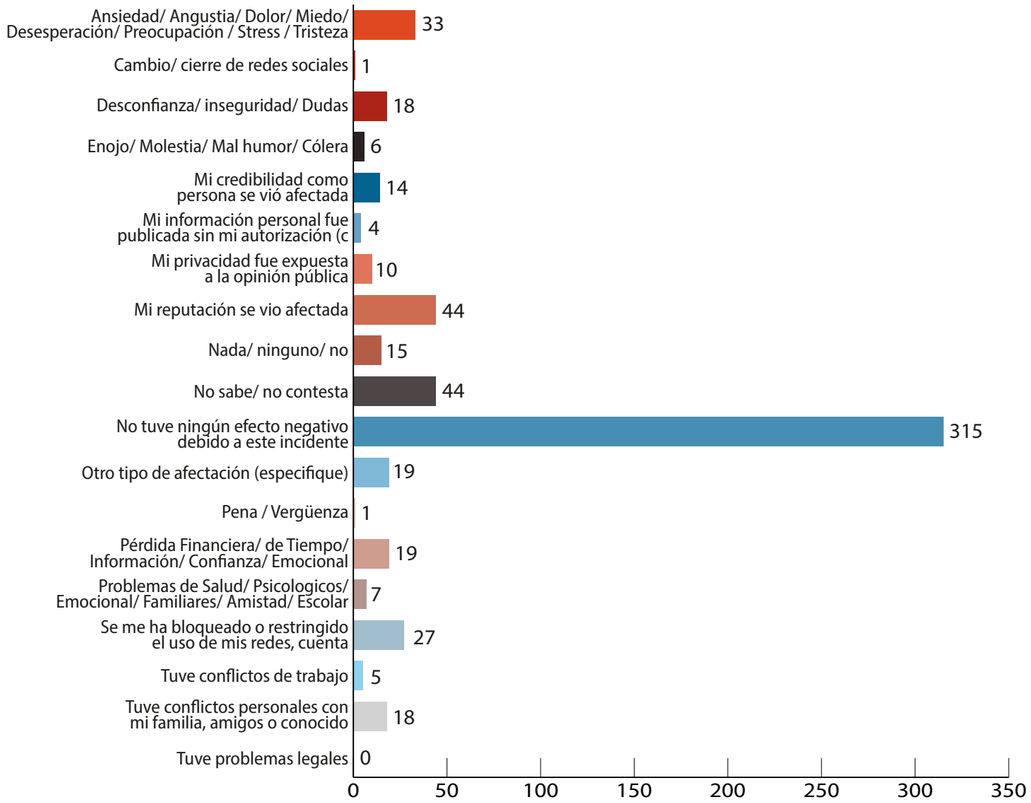
En relación con el daño que generó el ciberdelito, del total de personas que participaron en la encuesta en los 5 países priorizados, 555 expresaron que el ciberdelito generó un daño financiero, también informaron que generó daño en relación a la salud emocional y física, de manera que 686 personas viven con ansiedad, 411 sienten miedo, 226 les provocó tristeza y depresión, 153 manifestaron que sintieron desesperación y 119 de las personas que participaron sintieron enojo / cólera / molestia.

Las repercusiones de ser víctima de ciberdelitos pasan por el ámbito psicosocial, como lo muestra la Gráfica 6, con lo cual es importante que se brinde atención diferenciada y especializada a este grupo de víctimas, desde un enfoque de derechos humanos e interseccionalidad.

Los otros daños expresados, por las personas participantes en la encuesta, fueron principalmente: ansiedad, angustia, dolor, miedo, desesperación, preocupación, stress, enojo, mal humor, cólera, tristeza, desarrollaron desconfianza, inseguridad, dudas, su reputación se vio afectada, tuvieron perdida financiera, de tiempo, información, confianza y emocional.

Gráfica 6. Daños en la salud emocional y física por país, 2021

Gráfico 6.1. Daños en la salud emocional y física en República Dominicana, 2021



Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Gráfico 6.2. Daños en la salud emocional y física en Honduras, 2021

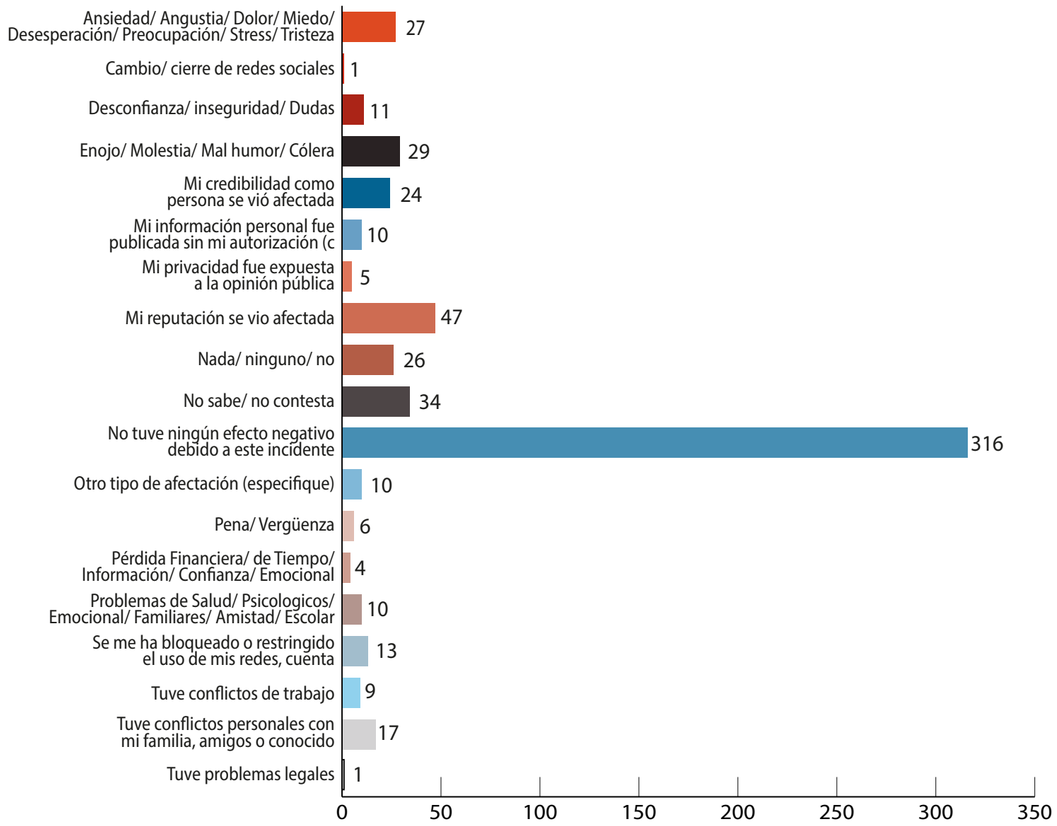
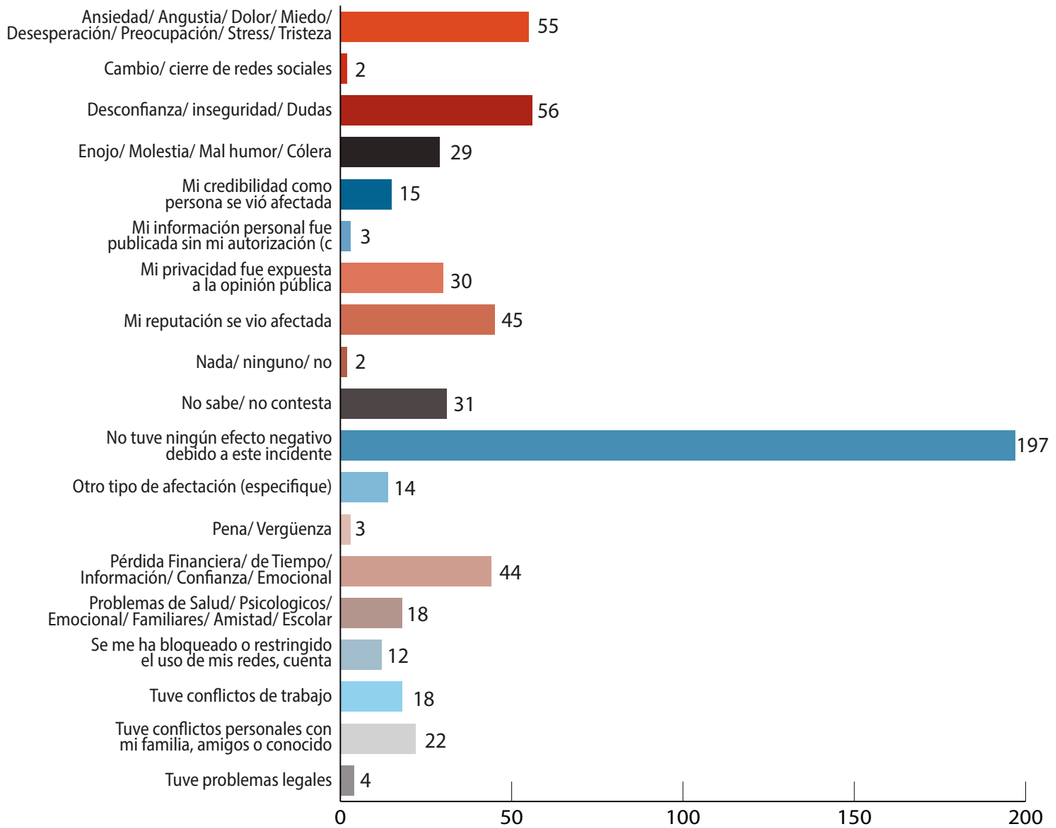


Gráfico 6.3. Daños en la salud emocional y física en Guatemala, 2021



Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Gráfico 6.4. Daños en la salud emocional y física en El Salvador, 2021

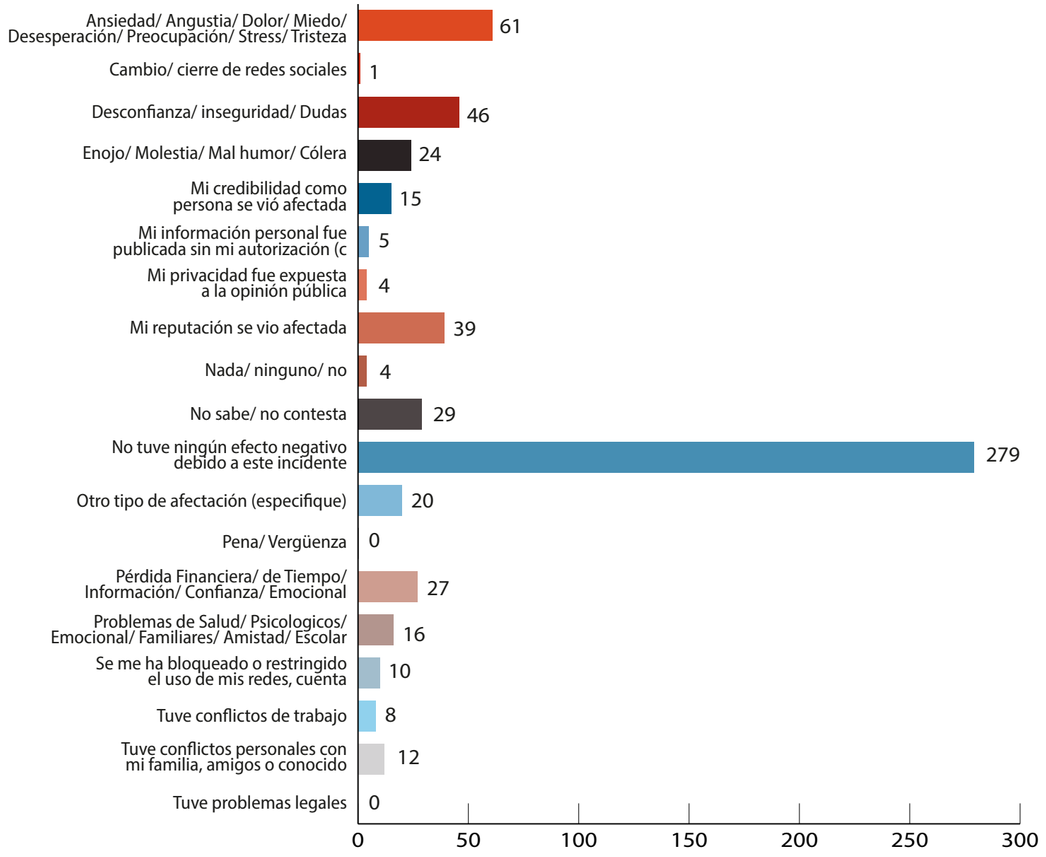
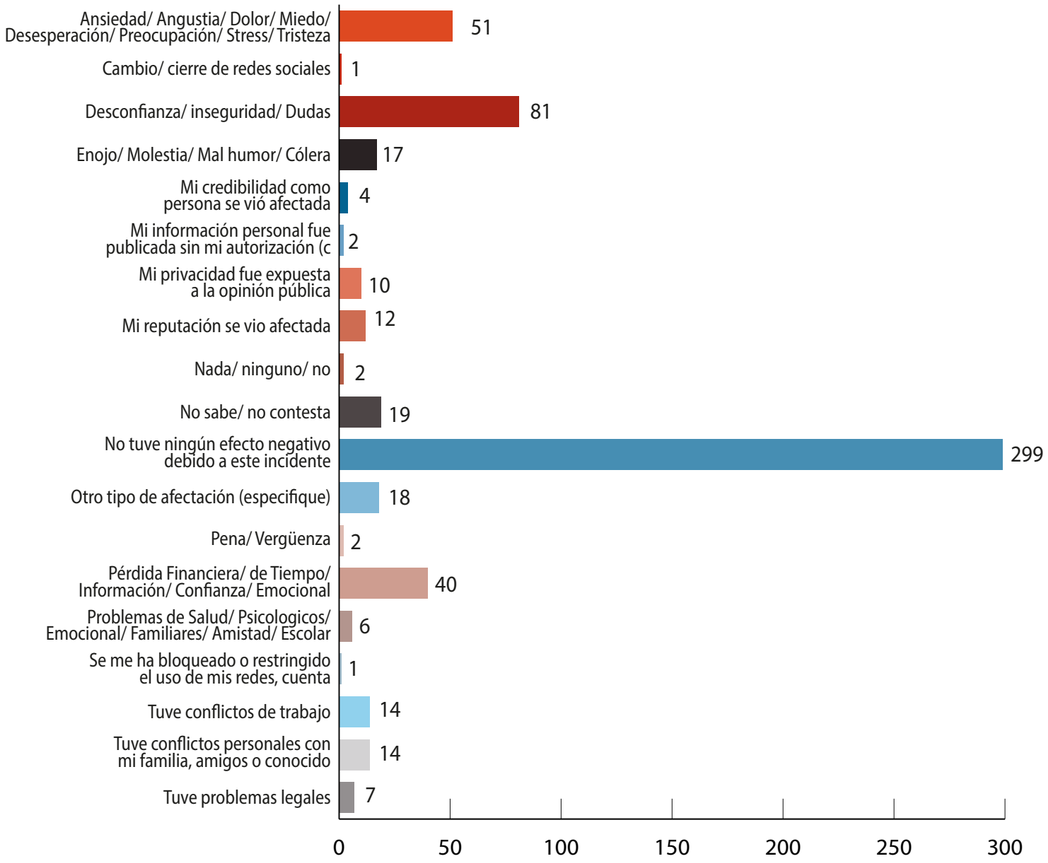


Gráfico 6.5. Daños en la salud emocional y física en Costa Rica, 2021



Fuente: elaboración propia con base en la encuesta de PNUD 2021.

En relación con la denuncia del hecho delictivo, solamente 550 personas realizaron la denuncia, el país donde más se denunció fue Costa Rica con 139 personas, seguido de Guatemala con 124 personas, en tercer lugar, República Dominicana con 120 personas, seguido de Honduras con 105 y, en último lugar, El Salvador con 62 personas. Estos datos reflejan que se carece de una cultura de denuncia para los ciberdelitos. Es relevante elaborar, con las instituciones encargadas de las seguridad y acceso a la justicia, las rutas de denuncia de ciberdelitos y violencias digitales.

De las 550 personas que presentaron su denuncia conforme a la Tabla 9, 189 denunciaron en Policía Nacional o Policía Judicial, 139 denunciaron en las entidades bancarias y en tercer lugar con 84 en Ministerio Público / Fiscalía. Se observa que muchas, aunque denunciaron, no lo hicieron en la línea de seguridad y justicia del país.

Tabla 9. Lugar donde denunciaron las víctimas 2021

Cantidad de personas que denunciaron por país						
Lugar de denuncia	**Costa Rica**	**El Salvador**	**Guatemala**	**Honduras**	**República Dominicana**	**Total general**
El Departamento de Investigaciones de Crímenes y Delitos Alt	2			2	14	18
Empresas telefónicas	1			2	3	6
Entidades bancarias	49	19	19	13	39	139
Ministerio Público / Fiscalía	11	11	39	18	5	84
Ninguna	2		1			3
NS/NR	2			2	2	6
Organismos Judiciales	54			2		56
Otro	2	6	1	4	2	15
Policía Nacional ó Policía Judicial	10	16	59	58	46	189
Redes sociales	6	10	4	3	5	28
Supermercados / Plazas / Establecimientos			1	1	4	6
Total general	**139**	**62**	**124**	**105**	**120**	**550**

Fuente: elaboración propia con base en la encuesta de PNUD 2021.

En relación con la medición del servicio al momento de hacer una denuncia, conforme a la Tabla 10, se reporta que 185 personas comentaron que el servicio fue satisfactorio, 154 indicaron que el servicio fue insatisfecho y 118 comentaron que fue muy insatisfecho. Esta información refleja una necesidad de evaluar los servicios que prestan las instituciones, específicamente, cuando se trata de interponer una denuncia de ciberdelito que es un delito poco conocido con las y los funcionarios públicos. Esto evidencia que también hay que trabajar en las instituciones con el mandato de atención a víctimas en capacitación sobre los ciberdelitos, ciberviolencias, causas y efectos en las víctimas.

Tabla 10. Nivel de satisfacción de los servicios al momento de colocar la denuncia 2021

Cantidad de personas por país						
Nivel de satisfacción	**Costa Rica**	**El Salvador**	**Guatemala**	**Honduras**	**República Dominicana**	**Total general**
Insatisfecho	34	15	37	26	42	154
Muy Insatisfecho	25	14	27	19	33	118
Muy satisfecho	24	11	14	16	21	86
NS/NR	5			2		7
Satisfecho	51	22	46	42	24	185
Total general	**139**	**62**	**124**	**105**	**120**	**550**

Fuente: elaboración propia con base en la encuesta de PNUD 2021.

La mayoría de las personas, de acuerdo con la Tabla 11, no denuncian los ciberdelitos porque consideran que es una cosa de poca importancia, porque los resuelven a su manera o no creen que las autoridades pueden ser eficaces y eficientes a la hora de resolver su caso. Ello reafirma que existe una naturalización de la violencia y criminalidad en las plataformas digitales, donde las víctimas carecen de mecanismos de protección ante estas amenazas.

Las respuestas de "no conozco el procedimiento", reflejan una oportunidad para establecer estrategias de comunicación e información. En relación con la falta de pruebas es importante educar a la ciudadanía, e informar que actualmente en este tipo de delitos se maneja evidencia digital. Las instituciones encargadas de recibir las denuncias deben tener mecanismos y procesos de atención que tomen en cuenta el principio de "no revictimización" para generar confianza en las personas de realizar denuncias de este tipo. La respuesta "lo resolví a mi manera" es una de muchas percepciones de la ciudadanía por la falta de credibilidad en la institucionalidad Estatal de abordaje integral de los ciberdelitos. Se debe buscar alternativas para conseguir que el proceso de acceso a la seguridad y justicia no siga recayendo en costos, tiempo y garantías de seguridad en la víctima.

Tabla 11. Motivos para no denunciar estos tipos de delitos 2021

Cantidad de personas por país						
Razón de no denuncia	**Costa Rica**	**El Salvador**	**Guatemala**	**Honduras**	**República Dominicana**	**Total general**
Acudí/contacté a la plataforma en la que sucedió el incidente	20	26	13	2	12	**73**
Conocía al agresor (o a los agresor(es)	3	8	2	7	4	**24**
Cosa de poca importancia	112	146	139	146	164	**707**
Desprecio o miedo a la policía/autoridad		3	2	1	2	**8**
El costo del procedimiento es elevado (transporte, abogados, etc)			5			**5**
El proceso burocrático es muy complicado y tardado	8	8	8	6	6	**36**

Cantidad de personas por país						
Razón de no denuncia	**Costa Rica**	**El Salvador**	**Guatemala**	**Honduras**	**República Dominicana**	**Total general**
Esta situación no está considerada como una conducta castigada	23	26	21	13	21	**104**
Falta de pruebas	10	14	8	12	13	**57**
Falta de tiempo/ información	6	10	25	1	1	**43**
Fue mi culpa / Fui descuidado	9	2	5	25	18	**59**
La policía / autoridad competente no habría hecho nada	38	65	55	86	28	**272**
Lo resolví a mi manera	80	60	34	53	57	**284**
Miedo a las represalias	7	30	30	31	13	**111**
Ninguno/ Nada/ No	2	2	1	3	1	**9**
No conozco el procedimiento para reportar delitos	15	27	11	22	11	**86**
No era apropiado que la policía o la autoridad competente interviniera	21	5	17	6	7	**56**
No sabe / no contesta	48	30	9	33	77	**197**
No sabía que esta situación era un delito	26	50	47	37	42	**202**
No tenía seguro	5	1	3	6		**15**
Otro motivo (especifique)	22	21	32	4	3	**82**
Total General	**455**	**534**	**467**	**494**	**480**	**2430**

Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Si se toman en cuenta los delitos priorizados en la encuesta, las personas participantes, antes de un ataque cibernético de acuerdo con la Tabla 12, contaban con medias de seguridad como: 637 personas cambiaban las contraseñas y consideraban las recomendaciones de utilizar más de 6 caracteres el uso de mayúsculas y minúsculas para hacer contraseñas más fuertes y menos vulnerables a los ataques. 271 personas usaban antivirus como una medida de protección a sus dispositivos digitales y generación de alertas de virus. 257 personas no tomaron ninguna medida de protección o prevención, y 154 registraron un patrón de bloqueo a sus dispositivos digitales.

Tabla 12. Medidas tomadas antes de ser víctimas de ciberdelito 2021

Cantidad de personas por país						
Medidas de protección smartphone	**Costa Rica**	**El Salvador**	**Guatemala**	**Honduras**	**República Dominicana**	**Total general**
Acceso remoto al dispositivo para bloquear o eliminar información	3	1			1	**5**
Antivirus	96	34	84	42	15	**271**
Aplicaciones/ avisos o alertad de plataforma	1	2	3			**6**
Cambio de las preguntas de seguridad	1		1			**2**
Cambio periódico de la contraseña (al menos una vez al mes)	1	4		6	2	**13**
Contraseña de acceso (de al menos 6 caracteres, mayúsculas/m	91	213	75	126	132	**637**
Encriptación de dispositivos	1		1	1		**3**
Establecimiento de la verificación o autenticación en dos pasos	1	3	1	2		**7**

Cantidad de personas por país						
Medidas de protección smartphone	**Costa Rica**	**El Salvador**	**Guatemala**	**Honduras**	**República Dominicana**	**Total general**
Firewall					1	1
Huella digital / Reconocimiento facial	1		5	2		8
Ninguna medida de protección o prevención	78	23	94	37	25	257
No sabe / no contesta	20	2	12	2	3	39
Otras medidas de protección o prevención (especifique)	4	2	5			11
Patrón de bloqueo	12	26	30	55	31	154
Respaldo regular de la información (al menos una vez al mes)	1	3	3	1		8
Sistema operativo actualizado	2	3			2	7
Verificación por correo electrónico			1			1
Total general	**313**	**316**	**315**	**274**	**212**	**1430**

Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Las víctimas de ciberdelitos toman otras medidas de seguridad o de protección, 251 personas dijeron utilizar un patrón de bloqueo, 154 antivirus y 42 personas actualizaron su sistema operativo (ver Tabla 13).

Tabla 13. Medidas tomadas después de ser víctimas de ciberdelito 2021

Cantidad de personas por país						
Medidas de protección smartphone	**Costa Rica**	**El Salvador**	**Guatemala**	**Honduras**	**República Dominicana**	**Total general**
Acceso remoto al dispositivo para bloquear o eliminar información	8	8		3	3	22
Antivirus	31	58	13	38	14	154
Aplicaciones/ avisos o alertad de plataforma		1			2	3
Cambio de las preguntas de seguridad	1	2	1	2	1	7
Cambio periódico de la contraseña (al menos una vez al mes)	1	1		2		4
Contraseña de acceso (de al menos 6 caracteres, mayúsculas/m				1		1
Encriptación de dispositivos	5	7		8	2	22
Establecimiento de la verificación o autenticación en dos pasos	3	1	2	2		8
Firewall			2			2
Huella digital / Reconocimiento facial		1	1	2	2	6
Patrón de bloqueo	35	126	5	55	30	251

Cantidad de personas por país						
Medidas de protección smartphone	**Costa Rica**	**El Salvador**	**Guatemala**	**Honduras**	**República Dominicana**	**Total general**
Respaldo regular de la información (al menos una vez al mes)	5	8	1	3	3	20
Sistema operativo actualizado	7	21	2	9	3	42
Verificación por teléfono			1			1
Total general	**96**	**234**	**28**	**125**	**60**	**543**

Fuente: elaboración propia con base en la encuesta de PNUD 2021.

Es necesario ver la seguridad digital como una herramienta orgánica que pasa desde lo conductual, hasta la seguridad del dispositivo que se utiliza. La necesidad de democratizar todos los componentes de la ciudadanía digital debe ser prioridad de los Estados, máxime cuando el nivel de victimización es elevado, la cultura de denuncia baja y los mecanismos de protección mínimos.

Minimizar los niveles de vulnerabilidad y las tasas de victimización requiere entre otras cosas:

- Lograr desarrollar empatía digital, lo que implica empatizar con las necesidades propias y de otros en el entorno digital,
- Construcción de pensamiento crítico, procurar que la persona tenga la capacidad de discernir la veracidad, credibilidad y salubridad del contenido que está consumiendo en sus interacciones digitales.
- Construir un nivel de ciudadanía digital eficiente que permita interacciones saludables y seguras tanto online como offline.
- Desarrollar un nivel de seguridad cibernética donde, además de proteger los dispositivos, se protejan los datos, se comprenda la etiqueta digital, se utilice claves seguras y se conozca la ruta a seguir en caso de ser víctima de algún ciberdelito. Acciones que lleven a tener mayor control de la privacidad para salvaguardar sus datos sensibles e información personal.
- Ser consciente de la huella digital, comprender el trasfondo de las decisiones y acciones que se generan en la virtualidad.
- Cuidar la salud digital, para evitar daños a la salud física y mental, desde número de horas de conexión, hasta ergonomía, cuidado de cuerpo físico.

- Capacidad de detección de ciberdelitos, desnaturalizar violencias cibernéticas, construir límites, conocer las rutas de denuncia y protección de la evidencia digital.
- Analizar la conducta de las personas en el ciberespacio, es necesario que las personas sean conscientes de los riesgos reales de ser víctimas en el ciberespacio, para que dejen de minimizarlos. Al mismo tiempo se debe dejar de ocultar la victimización por miedo a no exponerse públicamente a la vergüenza o a mostrarse vulnerables, por lo cual es esencial la atención diferenciada y especializada con enfoque de género e interseccionalidad.
- El anonimato y la asincronicidad que se da en los delitos cibernéticos implica comenzar a estructurar investigaciones donde se comience a analizar los procesos criminales organizados transicionales en las plataformas digitales, a fin de combatir el anonimato de los autores y la carencia de sistemas de seguridad.
- Las realidades y carencias en prevención integral del ciberdelito contribuyen de forma continua a la masificación de las víctimas, lo que se percibe a través de la falta de conciencia individual de los riesgos y vulnerabilidades en el entorno digital, la falta de estadísticas y data oficial, una cultura de no denuncia, la carencia de investigación continua y a gran escala, sistemas penales frágiles y sin recursos técnicos ni profesionales en la temática. Falta de políticas públicas de prevención con enfoque victimológico.

La cifra negra es muy elevada en ciberdelitos, la prevención se sigue haciendo desde enfoques criminológicos sin considerar los aspectos victimológicos, así como la heterogeneidad de las víctimas. Las víctimas tienen derecho a ser parte activa de los procesos, para ello requieren de una ciudadanía digital desarrollada y fuerte.

La percepción de inseguridad no suele coincidir con el riesgo de la víctima. Con la pandemia Covid-19 miles de personas se vieron obligadas a interactuar en plataformas digitales sin ciudadanía digital, lo cual elevó su riesgo de ser víctimas.

7. **Principales desafíos que los ciberdelitos plantean para los Estados de la región**

Además de los desafíos señalados específicamente por país a partir de los hallazgos de la encuesta, a continuación, se presentan algunos de los principales retos para la prevención, atención y judicialización de ciberdelitos, planteados más allá de las 5 modalidades priorizadas en la encuesta.

a. Lograr que la mayoría de los ciudadanos posean una ciudadanía digital, a través del desarrollo de la alfabetización digital y las herramientas básicas para procurar que las personas interactúen en plataformas digitales de forma segura.
b. Disminuir la brecha digital y dar acceso a conectividad a toda la población, y así garantizar el acceso a internet universal.
c. Los países que carecen de legislación, o marcos legales en la materia, deben lograr generarla de tal manera que protejan a sus ciudadanos de las ciberviolencia y ciberdelitos. Quienes ya cuentan con una, lograr socializarla para conseguir que las personas la conozcan y lograr su implementación a nivel país.
d. Establecer rutas de atención a las víctimas de ciberdelitos y ciberviolencias.
e. Los funcionarios públicos y juristas deben ser conocedores de tema, por lo cual las facultades de derecho de la región deben incluir en sus programas de estudio todo lo relativo a los ciberdelitos y aspectos procesales de la prueba informática.
f. Lograr que la evidencia digital adquiera cada vez más importancia en la investigación de cualquier delito, e implementar programas de capacitación que alcance no solamente a las unidades especiales de ciberdelitos, sino a todos los operadores del sistema penal.
g. Especializarse en el manejo de la cadena de custodia y prueba digital para manejar y garantizar la integridad de esta prueba.
h. Generar protocolos de investigación de ciberdelitos y cadena de custodia de evidencia digital.
i. Armonización legislativa para incluir temas de criminalidad trasnacional cibernética, en derecho procesal que incluya la prueba digital obtenida en el país y en otros países.
j. Coordinar el acceso, mediante un convenio con las empresas de servicios de internet (ej. Plataformas de redes sociales), para dar respuestas más ágiles y adecuadas a los requerimientos del sistema judicial.
k. Los sistemas informáticos de las instituciones de seguridad y justicia deben incluir las variables y catálogos los ciberdelitos legislados y como acción afirmativa incluir las ciber violencias.

8. **Conclusiones**

Para la academia

- Los cinco ciberdelitos priorizados en la encuesta, permiten un acercamiento al análisis de delitos vinculados al uso de dispositivos digitales.
- Existe poca oferta académica en temas de ciberseguridad, violencia digital de género orientados fortalecer la ciudadanía digital.
- Pocos estudios sobre el ciberdelito y violencia digital de género, los cuales fortalezcan la toma de decisión basada en evidencia.
- No hay estudios de evaluación de la implementación y reformas de los instrumentos legislativos en materia de ciberdelitos.

Para las instituciones de seguridad y justicia

- La percepción de la ciudadanía sobre los servicios que brindan las instituciones encargadas de la recepción de la denuncia es insatisfactoria.
- No existe una cultura de denuncia de ciberdelitos y violencias digitales, expresadas en las personas encuestadas.
- Las personas encuestadas comentaron no conocer los procedimientos para interponer una denuncia de ciberdelito.
- No se cuenta con perfiles de las víctimas y agresores de ciberdelitos y violencia digital, para el análisis del fenómeno criminal.
- La falta de información sobre los ciberdelitos analizados en este documento. Se requiere de un particular interés de generar acciones de prevención, atención e investigación para conocer más sobre los impactos que tienen en las víctimas.

Para las personas víctimas

- Existe muy poca información y estrategias de ciberseguridad que puede implementar la ciudadanía.
- Las personas encuestadas no cuentan con protocolos personales de ciberseguridad, lo cual los pone en una posición de vulnerabilidad ante el uso de plataformas de Internet.
- Falta de conocimiento del mandato de las instituciones de seguridad y justicia en materia de ciberdelitos.

9. Recomendaciones

Para la academia

- Realizar encuestas para generar información que facilite la toma de decisión basada en evidencia e informar a la ciudadanía de las vulneraciones y acciones realizadas en prevención del ciberdelito.
- La elaboración de encuestas debe tomar en cuenta otras variables de análisis de violencia digital y tipologías delictivas conexas al ciberdelito.
- Fomentar la oferta académica en temas de ciberseguridad, violencia digital de género; acciones orientadas a fortalecer la ciudadanía digital para reducir índices delictivos y reincidencias de ciberdelitos y violencias digitales.
- Realizar alianzas con la cooperación internacional que trabaja la prevención, atención, investigación y judicialización de ciberdelitos, para realizar estudios, encuestas de percepción y victimización de violencia digital y ciberdelitos.
- Realizar estudios sobre la implementación y retos que tienen los Estados en la prevención, investigación y judicialización de las nuevas figuras delictivas en materia de ciberdelitos en los países parte en esta encuesta.
- Trabajar, con las universidades, la oferta académica de las carreras jurídicas y otras carreras afines para conseguir que estén ligadas al trabajo con las instituciones de seguridad y justicia.

Instituciones de seguridad y justicia

- Para mejorar la percepción de la ciudadanía en la atención y recepción de denuncias de ciberdelitos y violencias digitales, se recomienda revisar la ruta de denuncia y actualizar los sistemas informáticos para realizar las denuncias de manera virtual.
- Establecer campañas de información sobre la importancia de la cultura de denuncia de los ciberdelitos y violencias digitales.
- Elaborar protocolos y rutas de denuncia para garantizar la atención diferenciada y especializada que implica abordar a las víctimas de ciberdelitos.
- Capacitar al personal que hace la recepción este tipo de denuncias con el principio de no revictimización.

- Caracterizar a la víctima de ciberdelitos y violencia digital y al agresor a partir del enfoque victimológico y criminológico.
- Revisar y actualizar los sistemas informáticos para integrar variables y catálogos de los ciberdelitos y violencia digital.

Para las personas víctimas

- Participar en campañas de información y sensibilización sobre la importancia de integrar la ciberseguridad en su cotidianidad y buscar establecer confianza en la institucionalidad para abordar los ciberdelitos y violencias digitales.
- Informarse sobre la ciberseguridad y ciudadanía digital para reducir factores de riesgo al momento de uso de dispositivos digitales y plataformas de Internet.
- Identificar los comportamientos de riesgos en el uso de las redes sociales y dispositivos, elaborar estrategias de prevención primaria.

10. **Referencias bibliográficas**

Agustina, J. R. 2014. “Cibercriminalida y perspectiva victimologica: un enfoque general explicativo de la cibervictimización”. Cuadernos de Política Criminal 3 (114): 143-178.

Asamblea Legislativa de la República de Costa Rica. 2022. Sistema Costarricense de información Juridica . (14 de noviembre) Obtenido de Ley N° 8148 para reprimir y sancionar los delitos informáticos: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=47430&nValor3=50318&strTipM=TC

Barahona, S. S. 2021. “Perfiles de ciberdelito: un campo de estudio inexplorado”. Revista de Derecho (30): 67-76.

Cicam. 2021. Riesgos y amenazas contra mujeres y jóvenas en uso de plataformas virtuales. Guatemala.

Cisco. 2022. Cisco. (14 de noviembre) Obtenido de https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

De la Cuesta Arzamendi, J. L., y Pérez Machio A. I. s.f. Ciberdelincuentes y cibervictimas.

Del Pino, S. A. s.f. Delitos Informaticos: Generalidades.

Digital Global Overview Report. 2022. Datareportal. Obtenido de https://datareportal.com/reports/digital-2022-global-overview-report

Federación de Mujeres Progresistas. 2021. Guía Informatica sobre ciberviolencias y delitos de odio por razón de género. España.

Fundación de la Innovación Bankinter. 2011. El internet de las cosas. En un mundo conectado de objetos inteligentes. Future Trends Forum.

Gamón, V. P. 2017. “Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad”. URVIO, Revista Latinoamericana de Estudios de Seguridad (20): 80-93.

Global Action on cibercrime extended. 2022. Desafíos para las autoridades de justicia penal en materia de ciberdelincuencia en América Latina y el Caribe 8 may 2020. (14 de noviembre) Obtenido de https://rm.coe.int/q-a-webinar3-latam-1-/16809e682d

IBM. 2022. IBM. (14 de noviembre) Obtenido de https://www.ibm.com/es-es/topics/cybersecurity

Ipandetec. 2020. Centroamerica Cibersegura.

Kanarek, J. 2021. Tracender el Reactivo. Uruguay: Debate.

López Gorostidi, J. 2020. "La Pluralidad De víctimas Derivada De La Elevada Lesividad En Los Ciberdelitos: Una Respuesta Penal Proporcional". Estudios de Deusto Revista de derecho público 68 (1): 201-221.

DOI: https://doi.org/10.18543/ed-68(1)-2020pp201-221

Llinares, F. M. 2011. "La Oportunidad Criminal". Revista Electrónica de Ciencia Penal y Criminología 7 (13):55.

Llinares, F. M. 2012. El Cibercrimen. fenomenologia y criminologia de la delincuencia en el ciberespacio. Madrid : Marcial pons.

MGS. 2022. Tu blog tecnológico. (14 de noviembre) Obtenido de http://tublogtecnologico.com/huella-digital-debes-cuidarla/

Muñoz, R. G. 2020). Decálogo Metodológico para el estudio del cibercrimen. Mexico: Universidad Guanajuato.

Organización de Estados Americanos (OEA). 2019. Alfabetismo y seguridad digital, mejores practicas en el uso de Twitter.

Organización de Estados Americanos (OEA). 2021. Alfabetización y seguridad digital, la importancia de mantenerse seguro e informado.

Organización de Estados Americanos (OEA). 2021. Ciberseguridad de las mujeres durante el covid 19.

Organización de Estados Americanos (OEA). 2020. La violencia de género en línea contra las mujeres y niñas : Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta. Comité Interamericano contra el Terrorismo / Comisión Interamericana de Mujeres.

Organización de Estados Americanos (OEA). 2018. Lineamientos para el empoderamiento y la protección de los derechos de los niños, niñas y adolescnetes en internet en Centroamérica y República Dominicana. Informe Regional. Instituto Interamericano del niño, la niña u adolescentes INN, SICA.

Organización de Estados Americanos (OEA). 2013. Tendencias en la seguridad cibernética . Washington, D.C.

Organización de Estados Americanos (OEA) y Cicte. 2020. Manual práctico de seguridad digital y estrategias de respuesta .

OEDI. 2022. Observatorio Español de Delitos Informaticos. (14 de noviembre) Obtenido de OEDI: https://oedi.es/ciberdelitos/

Rouhiainen, L. 2018. Inteligencia Artificial 101 cosas que debes saber hoy sobre nuestro futuro. Barcelona: Alienta.

Salazar, J. s.f. Internet de las cosas. Tech pedia.

Silva, J. M. 2018. “Los menores víctimas de la ciberdelincuencia”. Advocatus: 79-90.

Temperini, M., Borghello C., y Macedo M. 2014. La cifra negra de los delitos informaticos: Proyecto ODILA.

Tirado-Acero, M. 2021. “La politica criminal frente al ciberdelito sexual contra niños, niñas y adoslescentes en Colombia”. Revista Científica General José María Córdova 19 (36):1011-1033.

UNODC. 2022. Oficina de Naciones Unidas Contra la Droga y el Delito. (14 de noviembre) Obtenido de https://www.unodc.org/e4j/es/cybercrime/module-1/key-issues/cybercrime-in-brief.html

UNODC Ropan. 2021. Miniguía de seguridad en internet .

Vaca Trigo, I., y Valenzuela M. E. 2022. Digitalización de las mujeres en America Latina y el Caribe. Santiago: Cepal.

11. **Sobre las autoras**

Karen Vargas

Asesora en atención integral a las personas sobrevivientes de violencia, prevención de la violencia y el delito con un enfoque víctimo-criminológico, con énfasis en la prevención, atención e investigación criminal de la violencia en contra de personas en condición de vulnerabilidad. Especialista en abordaje de la prevención, atención a víctimas y facilitación de mecanismos de investigación en ciberdelitos y violencia digital de género. Brinda asistencia técnica en el fortalecimiento institucional para la preservación y manejo de la evidencia digital, así como la implementación de la ciudadanía digital y mecanismos de cierre de brechas digitales y ciberseguridad. Es facilitadora de espacios para la elaboración de rutas de denuncia del ciberdelito y elaboración de materiales didácticos con enfoque en derechos digitales de cuarta generación; además en el análisis, abordaje y prevención de los discursos de odio en redes sociales. Con experiencia de más de 15 años en fortalecimiento a instituciones del sector seguridad y justicia. Es máster en Criminología con enfoque victimológico y atención integral a sobrevivientes de violencia. Máster en Recursos Humanos. Posgrado en Psicología Forense. Licenciada en Comunicación Social. Ex becaria del programa Erradicar la violencia de género del Gobierno de Estados Unidos. Referente para Guatemala de Corpora en Libertad.

Patricia Vargas

Jurista en Derecho Internacional, ciberdelincuencia, victimología, justicia transicional, diversidad e inclusión de grupos en situación de vulnerabilidad. Con experiencia de más de 15 años a nivel internacional, en la defensa de los derechos humanos y prevención de la violencia y el delito con un enfoque victimo-criminológico, en el diseño de políticas públicas. Máster en comportamiento no verbal y detención del engaño, por la Universidad del Valle de Guatemala y Behavior and law en España. Abogada por la Universidad de la Sabana en Colombia. Comercio Internacional y Gestión de Empresas por la escuela de negocios HEC de la Universidad de Montreal, Canadá. Estudios en ciberseguridad en la Universidad Internacional de la Florida. Miembra de Alianza de Investigadores CARA: Central America Research Aliance, y de PIADH grupo para la promoción de la investigación aplicada en Derechos. Catedrática de la Universidad Landívar y FLACSO Guatemala, asesora en ciberseguridad y violencia digital de Género, capacitadora e investigadora en violencia de género en plataformas digitales, asesora en seguridad digital para organizaciones de sociedad civil en Guatemala y Perú, en prevención de ciberataques, discursos de odio, fraudes y mecanismos de ciberactivismo. Apoyó la construcción del eje de ciberviolencias y ciberdelitos de la PRONAPRE para ONUDC 2022.

El ciberdelito en **Centroamérica y el Caribe**

Autoras: Patricia Vargas y Karen Vargas

La Red Conose surgió en el año 2015, a partir del foro regional Gestión de conocimiento en seguridad ciudadana: una mirada desde la sociedad civil, como una respuesta a la necesidad de articular una serie de instituciones que abordan el tema de seguridad ciudadana. Dentro de uno de los ejes centrales de trabajo de la Red se encuentra el desarrollo de investigaciones que, preferencialmente, aborden fenómenos y procesos de carácter regional, en ese marco se estructura esta investigación sobre el tema de ciberseguridad y delito digital en América Central.

El punto de referencia principal para este estudio fue una base de datos perteneciente a una encuesta regional aplicada en cinco países centroamericanos por la casa encuestadora CID Gallup, a solicitud de las oficinas de PNUD, etn el primer cuatrimestre del año 2021. Con base en dicho insumo se generó un proceso de análisis de los datos con enfoque de género e interseccionalidad, a fin de tener una perspectiva más amplia sobre la ciberdelincuencia y las características victimológicas de las personas pertenecientes a la muestra de la base de datos que recabó información de Costa Rica, El Salvador, Guatemala, Honduras y República Dominicana.

conose
RED DE CONOCIMIENTO SOBRE **SEGURIDAD CIUDADANA**

infoSEGURA

USAID
DEL PUEBLO DE LOS ESTADOS UNIDOS DE AMÉRICA

PNUD

ISBN: 978-9977-68-346-1