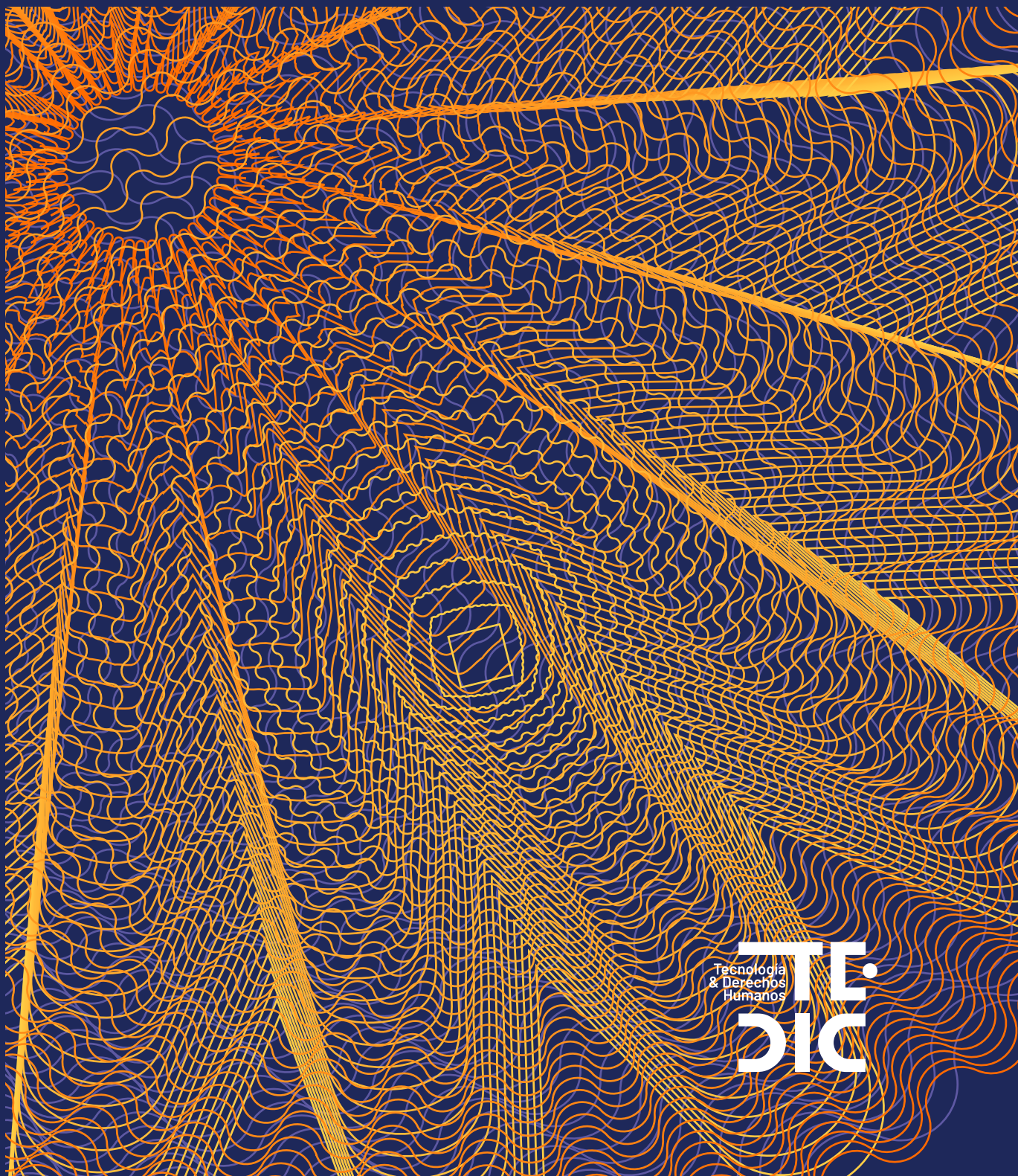
CIBERSEGURIDAD EN DEFENSORAS Y DEFENSORES DE DERECHOS HUMANOS EN PARAGUAY



Tecnología & Derechos Humanos

CIBERSEGURIDAD EN DEFENSORAS Y DEFENSORES DE DERECHOS HUMANOS EN PARAGUAY

Tecnología & Derechos Humanos

Digital Defenders Partnership (DDP, por sus siglas en inglés) es un programa internacional destinado a fortalecer la resiliencia de las personas y organizaciones defensoras de derechos humanos mediante la mejora de su seguridad digital a través de un enfoque holístico y sostenible.

Esta investigación fue posible gracias al Fondo de Alianza Regional de DDP, que apoya iniciativas que promuevan la libertad en línea y la protección digital para las personas defensoras de los derechos humanos que operan en un solo país o región.

TEDIC es una Organización No Gubernamental fundada en el año 2012, cuya misión es la defensa y promoción de los derechos humanos en el entorno digital. Entre sus principales temas de interés están la libertad de expresión, la privacidad, el acceso al conocimiento y género en Internet.

CIBERSEGURIDAD EN DEFENSORAS Y DEFENSORES DE DERECHOS HUMANOS EN PARAGUAY

SETIEMBRE 2024

INVESTIGACIÓN
Mariela Cuevas

COORDINACIÓN
Leonardo Gómez Berniga

DISEÑO METODOLÓGICO
Fundación Karisma - Colombia

MAPEO DE DEFENSORAS Y DEFENSORES
Coordinadora de Derechos Humanos del Paraguay (CODEHUPY)

EDICIÓN Y REVISIÓN
Maricarmen Sequera

DIAGRAMACIÓN
Horacio Oteiza

COMUNICACIÓN
Araceli Ramírez

TABLA DE CONTENIDOS

GLOSARIO

CERT-PY	Centro de Respuestas ante incidentes cibernéticos del Paraguay.
CICTE	Comité Interamericano Contra el Terrorismo.
CISA	Agencia de Seguridad de Infraestructura y Ciberseguridad. (Cybersecurity and Infrastructure Security Agency por sus siglas en inglés).
CSIRT	Equipo de Respuesta ante Incidencias de Seguridad Informáticas. (*Computer Security Incident Response Team* por sus siglas en inglés).
CODEHUPY	Coordinadora de los Derechos Humanos del Paraguay.
DDHH	Derechos Humanos
DGCPI	Dirección General de Ciberseguridad y Protección a la Información.
DDOS	Ataque de denegación de servicio distribuido. (*Distributed Denial-of-Service*, DDoS por sus siglas en inglés)
ENC PY	Estrategia Nacional de Ciberseguridad de Paraguay.
EPH	Encuesta Permanente de Hogares.
FGE	Fiscalía General.
LGTBIQ+	Lesbianas, Gays, Personas Trans, Bisexuales, Intersexuales y Queer. El signo más hace referencia a inclusión de todas las identidades de género y orientaciones sexuales.
MITIC	Ministerio de Tecnologías de la Información y Comunicación.
MITM	Ataque de Intermediario. (*Man-in-the-Middle* por sus siglas en inglés).
OEA	Organización de los Estados Americanos.
OEE	Organismos y Entidades del Estado.
ONU	Organización de las Naciones Unidas.
SENATICS	Secretaría Nacional de Tecnologías de la Información y Comunicación.
SICOM	Secretaría de Información y Comunicación.
SQL	Lenguaje de Consulta Estructurada. (*Structured Query Language* por sus siglas en inglés).
TIC	Tecnología, Información y Comunicación.
XSS	Secuencia de comandos en sitios cruzados. (*Cross-site scripting*).

RESUMEN DE LA INVESTIGACIÓN

La investigación analiza la situación de ciberseguridad en defensores y defensoras de derechos humanos en Paraguay, enfocándose en comprender las dinámicas de utilización de la herramienta digital, internet y su ciberseguridad.

Los defensores y defensoras referidos buscan la protección y promoción de los derechos humanos desde diferentes dimensiones y son sujetos medulares para combatir situaciones de injusticias y arbitrariedades en los diferentes temas, por lo que también robustecen la calidad democrática y la salvaguarda de derechos. En atención al rol que desempeñan en general se encuentran en situación de riesgo y vulnerabilidad en cuanto a su seguridad y de manera particular en lo que compete a la exposición en materia de ciberseguridad.

Ante esta situación, se llevó adelante esta investigación desde TEDIC de Paraguay en articulación con la Fundación Karisma de Colombia, con el fin de conocer y disponer de información sobre el estadio, los riesgos, debilidades, amenazas y fortalezas de seguridad digital y con ello, encaminar la toma de decisiones sobre medidas de protección para las organizaciones y personas defensoras de derechos humanos.

La investigación utilizó una metodología cuanti-cualitativa, y por ello se valió de un mapeo de defensores de derechos humanos y la aplicación de una encuesta sobre seguridad digital a 130 defensores y defensoras de derechos humanos en Paraguay, el desarrollo de grupos focales y entrevistas en profundidad que posibilitaron conocer con mayor claridad las percepciones y conocimientos en general sobre la ciberseguridad.

PALABRAS CLAVE: *ciberseguridad, vulnerabilidad, amenazas, ataque informático, violencia digital, defensoras y defensores, derechos humanos.*

METODOLOGÍA

Esta investigación realiza un estudio exploratorio que permite construir una línea de base para disponer de datos relacionados a la ciberseguridad de las defensoras y defensores de los Derechos Humanos en Paraguay.

El trabajo tiene como referencia el estudio “Fortaleciendo la garantía de los derechos de las personas defensoras y defensores de DDHH, líderes y lideresas, sus organizaciones y colectivos en Colombia” desarrollado por la Fundación Karisma durante los años 2023 y 2024.

Metodológicamente, se utilizaron técnicas de investigación cuantitativa y cualitativa. Para el abordaje de la metodología cuantitativa se aplicaron 130 encuestas a defensoras y defensores de derechos humanos del Paraguay, diligenciadas de manera sincrónica y asincrónica. El mapeo de defensores y defensoras de derechos humanos fue proporcionado por la Coordinadora de Derechos Humanos del Paraguay (CODEHUPY). La selección consideró las diferentes locaciones territoriales de las personas y que correspondieron a diversos puntos del país.

Las encuestas asincrónicas fueron distribuidas a las personas seleccionadas de la red de DDHH vía canal de mensajería WhatsApp y las encuestas sincrónicas fueron aplicadas de forma asistida vía telefónica. Por otro lado, se realizaron dos grupos focales con referentes de diferentes temas de los derechos humanos y fueron aplicadas tres entrevistas en profundidad con personas informantes clave, reconocidas por su trayectoria y conocimiento en el ámbito de la ciberseguridad y/o derechos humanos.

HERRAMIENTAS DE RECOLECCIÓN DE DATOS

A continuación, se detallan los mecanismos considerados según cada tipo de herramienta de recolección de datos:

Encuesta

El tipo de encuesta aplicado fue de carácter descriptivo al recolectar información de ciento treinta (130) defensores y defensoras de derechos humanos del Paraguay. Las encuestas asincrónicas se aplicaron a ciento quince (115) perfiles y las sincrónicas a quince (15) perfiles. La composición de los perfiles encuestados fue el siguiente: referentes campesinos, referentes indígenas, referentes del derecho a la ciudad, referentes ambientalistas, referentes de la libertad de expresión, referentes del derecho a la identidad: Feministas y LGTBIQ+, -Referentes de la educación, referentes de la salud y referentes de los derechos de niños, niñas, adolescentes. El cuestionario de la encuesta estuvo disponible a través de la herramienta de Google forms.

Grupos focales

Se realizaron dos (2) grupos focales con la participación de 8 (ocho) personas por cada grupo. Se contó con la participación de defensores y defensoras de organizaciones que trabajan diferentes temas de derechos humanos (derecho a la ciudad, campesinado, LGTBIQ+, Educación, ambiente, entre otros). El instrumento aplicado para relevar información fue en atención a las categorías y preguntas organizadas por la Fundación Karisma.

Entrevistas

Para desarrollar las tres (3) entrevistas en profundidad con informantes clave por su trayectoria en los ámbitos de actuación de ciberseguridad y/o derechos humanos. Se identificó a personas con el siguiente perfil: Como mínimo cinco (5) años de trabajo en el ámbito de derechos humanos; un reconocido desempeño en la defensa de los derechos; personas pertenecientes a plataformas de derechos humanos, equipos de monitoreo de entidades de cooperación y/o actores de la sociedad civil. El instrumento aplicado para relevar información fue en atención a las categorías y preguntas organizadas por la Fundación Karisma.

Revisión de fuentes secundarias

Para recabar la información de fuentes secundarias se consultaron investigaciones relacionadas a ciberseguridad y derechos humanos, como así también documentaciones públicas relacionadas al tema disponible en repositorios en línea y aquellos relacionados a las relatorías de las Naciones Unidas en materia de Derechos Humanos y Ciberseguridad.

MARCO TEÓRICO

CONTEXTO DE USO DE INTERNET

La utilización cotidiana de la tecnología por gran parte de la población y el hecho de que las personas estén conectadas a dispositivos e Internet es una característica de este tiempo y que se dio como fenómeno en todo el mundo desde finales del siglo XX. En Paraguay, según la Encuesta Permanente de Hogares (EPH, 2023), la población paraguaya que utiliza internet es de 76.3 %, lo que representa aproximadamente 4.556.000 personas. El crecimiento porcentual del año 2015 al 2022 ha sido de 26.6 % (De 49.7 % a 76.3 %).

El impacto que ha generado Internet en la vida de las personas es de una magnitud muy alta y sin precedentes, puesto que se ha creado un nuevo lugar de interacción y relacionamiento que se denomina el ciberespacio, donde las distancias se acortan y las fronteras se desdibujan. Hoy día disponer de informaciones se caracteriza por la facilidad y rapidez en el acceso.

El espacio digital es complejo y se encuentra en permanente evolución. Hablar de ello, implica la existencia de ciertos factores que según Machín y Gazapo 2016, se trata de los siguientes elementos:

1. Datos
2. Tecnologías de computación (Hardware, Software, Redes de ordenadores/Infraestructura, Protocolos de red, virtualización, computación en la nube)
3. Tecnologías de la información de análisis / Comprensión
4. Tecnologías de Interacción / Gestión (Interacción hombre-máquina, Tecnologías de agentes inteligentes, tecnologías de personalización, tecnologías de bases de datos)

Los citados autores indican que el ataque facilitada por la tecnología puede darse cuando se da alguna acción contra uno o más elementos que conforman el ciberespacio, se trata pues, de perpetrar una operación con el fin de tener acceso y manipular cierta información.

El ciberespacio y su vinculación con la seguridad hace que emerja la consideración de la misma desde una perspectiva armónica, como bien público, y desde una mirada del conflicto, como espacio de guerra. Acuña (2017) señala que “sin un enfoque centrado en las personas, la ciberseguridad sólo sirve para dar más poder al poder”. Por su parte, Sancho (2017) indica que el tratamiento de internet como un bien público, obliga al Estado a desarrollar acciones para garantizar condiciones mínimas de seguridad y así posibilitar que toda la población pueda usarla en forma confiable.

¿QUÉ ES CIBERSEGURIDAD?

Si bien, la ciberseguridad es un término que no ha conseguido consenso en torno a su definición, se puede decir de ella, que es un desafío económico y social, pues, no se limita sólo a la dimensión técnica. En este sentido hace referencia a un conjunto de medidas y prácticas que buscan minimizar los riesgos relacionados a la seguridad digital, y a través de ello, contribuir con el desarrollo socio-ecónomico, garantizando la protección de los derechos humanos y los valores democráticos OCDE (2016)[1].

Es importante contextualizar a la seguridad desde la mirada de los Derechos Humanos, pues, en este sentido, se la enmarca en la capacidad de las personas de actuar libremente de forma responsable. La política de seguridad en Internet no debe reducirse a un perfil defensivo, sino a actuar como facilitador en el cuidado y salvaguarda de los derechos de las personas. Así pues, se proporciona una perspectiva desde lo positivo con soluciones y con reducción de la mirada negativa, desde las amenazas (TEDIC, 2016).

La ciberseguridad consiste en garantizar la protección de las personas u organizaciones en el ciberespacio, de manera puntual, se trata de cuidar los datos personales o institucionales para mantenerlos fuera de amenazas en internet o en la red. Implica abordar el relacionamiento que se da entre humanos-máquinas. Las medidas de protección de ciberseguridad apuntan a resguardar la confidencialidad, la información (disponibilidad y autenticidad) y la integridad de los datos de las personas, organizaciones, empresas y las del Estado. Se vuelve medular la necesidad de incorporar el enfoque de Derechos Humanos, en particular desde los derechos de intimidad, privacidad, confidencialidad, disponibilidad e integridad de la información, y libertad de expresión (Fundación Karisma, 2024). En coincidencia con lo anterior, la publicación de expertos sobre Ciberseguridad (Sequera et al,. 2018), indican que la seguridad digital está estrechamente relacionada con las personas, pues la forma en cómo se implementan las políticas de regulación del comportamiento en línea y la seguridad de la información, tienen estrecha relación principalmente con los derechos fundamentales como el derecho a la privacidad, la libertad de expresión o la libre asociación (p. 5). Esto refuerza la necesidad de comprender la definición de ciberseguridad en atención a la relación de interdependencia existente entre la seguridad digital y los derechos humanos, y de esta manera pues, dar paso al cuidado efectivo de la seguridad de las personas en el campo *online* como *offline*.

La ciberseguridad está comprometida, vulnerable y amenazada cuando personas perpetradoras, atacantes o personas malintencionadas realizan actos para ingresar de manera no autorizada a las cuentas, equipos informáticos o sistemas para cometer algún tipo de ataque con distintos fines, ya sea robo de información, estafar, extorsionar, acosar, envío de *spam*, entre otros.

Es importante señalar que, la ciberseguridad también puede ser atacada por la vigilancia realizada por parte del Estado. Algunas de las maneras a través de las cuales se vulnerada la seguridad digital es a partir de mecanismos que puede utilizar la policía nacional, como por ejemplo: extracción de datos de teléfonos móviles (físicamente), hackeo de dispositivos móviles, extracción de datos de la nube, la utilización de cámaras de reconocimiento facial y corporal en espacios públicos, y el monitoreo de las redes sociales de personas activistas, entre otros (Sequera, 2022).

1 OCDE. (2016). Políticas de banda ancha para América Latina y el Caribe: Un manual para la economía digital. Disponible en: https://read.oecd-ilibrary.org/science-and-technology/politicas-de-banda-ancha-para-america-latina-y-el-caribe/gestion-de-riesgos-de-seguridad-digital_9789264259027-17-es#page3. Accedido el 15 de julio de 2024.

La aplicación de alguno/s de los ejemplos mencionados anteriormente, compromete ciertos derechos que la propia Constitución Nacional del Paraguay menciona en su artículo 33, como el derecho a la intimidad, del derecho a la inviolabilidad de patrimonio documental y la comunicación, atentando contra la protección de datos personales. La vigilancia estatal forma parte de una de las preocupaciones y factores a atender al momento de hablar de ciberseguridad. En el entorno moderno se define que la vigilancia de las telecomunicaciones comprende monitorear, interceptar, recoger, analizar, usar, preservar, guardar, interferir u obtener información que incluya o refleje las comunicaciones pasadas, presentes o futuras de una persona, se derive o surja de ellas[2] (Sequera et al., 2016).

La vigilancia en las telecomunicaciones a partir del uso de tecnología biométrica es una de las maneras en que la policía nacional implementa el control y atenta contra la democracia al no garantizar el uso del anonimato de las personas para su participación en los debates o manifestaciones de interés público (Carrillo et al., 2018). Actualmente, en el Paraguay, al no disponer de una ley integral de datos personales, se agudiza la exposición y vulnerabilidad en términos de seguridad digital.

La autoría de las personas perpetradoras corresponde a diferentes tipologías, como, por ejemplo: ataques patrocinados por el Estado o por otros Estados, por el sector privado, por el terrorismo o grupos extremistas, crimen organizado, ataques de bajo perfil y ataques de personal con accesos privilegiados (Sequera et al., 2023). Cabe destacar que, la violencia de género en línea es uno de los ataques a la seguridad digital más frecuentes que se registra en el país (Carrillo et al., 2024). .

El impacto de estos ataques es clasificado en un rango bajo, medio o alto según la magnitud del hecho (Sancho, 2017). Por lo general, la bibliografía señala que los ataques facilitados por la tecnología tienen como objetivos a gobiernos y al sector privado, pero también se da con organizaciones activistas de causas sociales, defensores y defensoras de derechos humanos y las personas en general. Estos dos últimos grupos también son víctimas de los ataques, ya sea a través de espionaje, ataques a infraestructuras, robo y publicación de información sensible, ataques a redes sociales, entre otros. Es por ello, que esta investigación aborda el tema de ciberseguridad y defensores de derechos humanos para conocer el estadio en el cual se encuentra dicho sector en relación a su seguridad digital.

Es importante que se consideren aspectos fundamentales sobre ciberseguridad al momento de abordar el tema desde las políticas públicas de seguridad digital, así pues, considerar la transparencia y la inclusión de la sociedad civil, contar con un enfoque centrado en las personas, reconociendo sus deberes y protegiendo sus derechos, mantenerse actualizado constantemente por las características y dinámica del fenómeno, son aspectos claves para viabilizar el desarrollo social y económico, garantizando los derechos humanos[3].

2 Los autores Sequera, M. y Rolón Luna, j. (2016), utilizan esta definición a partir de lo señalado en Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones (2014). https://es.necessaryandproportionate.org/text. Accedido el el 05 de julio de 2024.

3 Estos puntos mencionados son resultado del análisis y debate que se dio en Colombia en torno a la ciberseguridad, a partir del borrador de un Decreto emitido por el MinTIC. Estos criterios en materia de seguridad digital también son los recomendados por la OCDE (2016). Fundación Karisma. (2024). Comentarios al borrador del decreto de ciberseguridad del MinTIC. https://web.karisma.org.co/comentarios-al-borrador-del-decreto-de-ciberseguridad-del-mintic/. Accedido el 25 de julio de 2024.

DEFENSORES DE LOS DERECHOS HUMANOS Y CIBERSEGURIDAD

En el año 1998 la Asamblea General de las Naciones Unidas[4] aprobó la Declaración sobre defensores de los derechos humanos, que trata lo relativo al derecho y el deber de las personas, los grupos y las instituciones para promover y proteger los derechos humanos y las libertades fundamentales universalmente conocidas. De manera específica, los defensores y defensoras referidos buscan la protección y promoción de los derechos humanos desde diferentes dimensiones como lo son: el desarrollo, la lucha contra la pobreza, las acciones humanitarias y de paz, los derechos civiles, políticos, económicos, sociales, culturales, ambientales, digitales, entre otros.

Es importante recordar que diversas instancias de la ONU han abordado este tema. En el 2022, por ejemplo, el Alto Comisionado de las Naciones Unidas para los Derechos Humanos presentó un informe al Consejo de Derechos Humanos, expresando serias preocupaciones sobre los ataques a la privacidad por parte de los estados. El Relator Especial sobre el derecho a la libertad de reunión pacífica y asociación, Clément Voule, enfatizó que estamos ante un preocupante aumento de legislación y políticas públicas dirigidas a combatir la ciberdelincuencia, que también abrió la puerta para sancionar y monitorear a activistas y manifestantes en muchos países del mundo[5].

En Paraguay, los defensores y defensoras de derechos humanos son sujetos medulares para garantizar la promoción y protección de los derechos fundamentales y, por ende, combatir situaciones de injusticias y arbitrariedades en los diferentes temas. Estas personas al cumplir roles clave para garantizar la calidad de la democracia y la salvaguarda de derechos, en general, se encuentran en una situación de riesgo y vulnerabilidad en cuanto a su seguridad y protección y, en particular, en lo que compete a la exposición en materia de ciberseguridad. Al respecto, resulta ilustrativo el proyecto de Ley presentado al Congreso paraguayo, donde se manifiesta la necesidad de la "Ley de Protección a periodistas, comunicadores y defensores de los Derechos Humanos"[6].

Como se mencionó anteriormente, en las últimas décadas el uso y dependencia tecnológica para el desarrollo de la vida ha demostrado un crecimiento exponencial. Los defensores y defensoras no están ajenos a este fenómeno y el ejercicio de la defensa de temas de DDHH conlleva la utilización asidua de plataformas y canales de comunicación digital ya sea para articular, organizar, difundir o intercambiar información. La vigilancia específica o masiva sobre las comunicaciones de las organizaciones y personas es una latencia perenne a la implicancia del ejercicio de protección de derechos.

Es por ello que analizar la ciberseguridad de defensores y defensoras de derechos humanos es clave para buscar estrategias y resguardar la protección física, jurídica, digital y psíquica, para así poder mitigar vulnerabilidades, amenazas e intimidaciones que puedan recibir. Lo mencionado colabora con el fortalecimiento y la calidad de la democracia y con el estado de derecho.

4 Resolución 53/144: Declaración de las Naciones Unidas sobre el derecho y el deber de los individuos, los grupos y las instituciones de promover y proteger los Derechos Humanos y las libertades fundamentales universalmente reconocidos. Aprobada en la Asamblea General del 9 de diciembre de 1998.

5 Oficina de los Derechos Humanos de las Naciones Unidas. (2019). Derechos a la libertad de reunión pacífica y de asociación. https://www.ohchr.org/. Accedido el 04 de junio de 2024.

6 Sistema de Información Legislativa del Paraguay. Proyecto de Ley. #Expediente: D-2164736. Proyecto de Ley de Protección a periodistas, comunicadores y defensores de derechos humanos. https://silpy.congreso.gov.py/web/expediente/124598. Accedido el 06 de julio de 2024.

También, por parte de los Estados es importante señalar que el tema de ciberseguridad empezó a ser considerado con mayor envergadura desde inicios del 2000, así pues, la OEA a través del Comité Interamericano Contra el Terrorismo (CICTE), aprobó[7] la "Adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y multidisciplinario para la creación de una cultura de seguridad cibernética", en la misma reconocen el desafío de construir capacidades de seguridad en el ciberespacio desde instancias nacionales y regionales, como así también tomando acciones de colaboración desde el sector público como privado.

En un análisis realizado por el TEDIC (2016) se indica que el desafío en materia de ciberseguridad no sólo tiene que ver con el terrorismo internacional, el espionaje o la ciberdelincuencia, sino que se debe dar capital atención a el código fuente del software y hardware que son utilizados, ya sea del sistema operativo o las diversas aplicaciones.

TIPOS DE ATAQUES DE CIBERSEGURIDAD

Los tipos de ataques de ciberseguridad son varios y la evolución con la que se ven nuevas variantes es constante. En Paraguay, el Centro de Respuestas ante Incidentes Cibernéticos (CERT-PY)[8] dependiente del Ministerio de Tecnologías, Información y Comunicación (MITIC) funciona desde el año 2012[9] y realiza registros y seguimiento a los principales tipos de ataques o incidentes cibernéticos registrados en el país[10]. A continuación, se da cuenta de algunos tipos de ataques que se dan en Paraguay y que el organismo refiere:

- **Compromiso de sistemas:** este tipo de hecho se da cuando los servidores están sujetos a la infestación o desconfiguración del sitio web, inyección de código o archivos maliciosos, entre otros.
- **Correo no deseado o malicioso (SPAM):** corresponden a correos electrónicos no solicitados o no deseados que son enviados con fines engañosos (estafa, extorsión, entre otros).
- ***Phishing:*** sucede cuando perpetradores de delitos informáticos quieren ganarse la confianza de las personas u organización utilizando mensajes y argumentos que generen credibilidad para que las víctimas ingresen sus datos en páginas web o formularios y resulten engañadas. Por lo general, los atacantes solicitan datos bancarios, contraseñas, información personal, entre otros.
- **Software malicioso (*Malware*):** se trata por lo general de software web que se ejecutan sin una indicación explicita del usuario y se instalan en el sistema. Por lo general son descargas maliciosas que pueden ser virus, troyano, gusano, *script*, *ransomware*, entre otros.
- **Acceso indebido a cuentas, sistemas o datos:** este tipo de ataque se da con el ingreso no autorizado del atacante a la cuenta personal o institucional utilizando algún método informático.
- **Escaneo / Fuerza bruta:** sucede cuando se da un acceso al sistema mediante el *cracking* de contraseñas (pruebas por aproximación hasta descifrar la contraseña), escaneo de puertos, entre otros.

---

7 Resolución AG/RES. 2004 (XXXIV-O/04)

8 CERT/ MITIC. (2023). Informe: Estado de la ciberseguridad en el Paraguay. Año 2022. https://www.cert.gov.py/wp-content/uploads/2024/01/Informe-Ciberseguridad-Paraguay-2022.pdf. Accedido el 10 de mayo de 2024.

9 Resolución SETICs № 18/12: Que crea el Equipo de Respuestas ante Emergencias Cibernéticas (CERT-PY), como una dependencia de la SETIC (Secretaría de Tecnologías de la Información y Comunicación) dependiente del Poder Ejecutivo y firmado el 30 de noviembre de 2012.

10 Es importante señalar que el CERT-PY considera no sólo los ataques realizados contra el espacio gubernamental, sino también, recibe información de ataques realizados contra el sector privado y la ciudadanía en general.

- **Problema de configuración / vulnerabilidad:** se define a este tipo de ataque como aquellas situaciones que relacionados con Internet y que constituye una amenaza latente de alto riesgo, como, por ejemplo, la exposición de contraseñas, entre otros.
- **Denegación de servicios (DoS/DDoS):** ocurre cuando se sobrecarga o ahoga una máquina o una web con peticiones en simultáneo, hasta lograr que el sistema colapse por incapacidad de respuesta. Con esto se logra que la web o la máquina deje de estar disponible.
- ***Ransomware:*** es un tipo de malware que a través de un código malicioso infecta equipos o sistemas informáticos dejándolos inutilizados. Los perpetradores por lo general se comunican con las víctimas y solicitan un pago para proceder con el rescate de la cuenta o la web.

Se suman a esta lista otros que son conocidos en el campo del ciberespacio, como lo son:

- **Inyección SQL:** Hallan vulnerabilidades en aplicaciones web al inyectar código SQL malicioso en formularios de entrada para acceder y manipular bases de datos.
- **Ingeniería social:** Se trata de manipulación psicológica de las personas para obtener información confidencial o sensible para acceder al sistema o dispositivo. Este tipo de ataque puede incluir a su vez al *phishing*, cebo, el *pretexting* y el *tailgating*. Este tipo de ataques también se nutre de información disponible públicamente, como, por ejemplo, aquellos que se encuentran en periódicos, revistas, sitios de redes sociales, entre otros.
- **Intermediario (MitM):** el ataque se da al interceptar comunicaciones entre partes sin que éstas lo perciban.
- **Suplantación de identidad (*Spoofing*):** el ataque sucede cuando se suplanta la identidad de la persona u organización para obtener acceso a la información o al sistema. Se suplantan IPs, correos electrónicos y/o DNS.
- ***Cross-Site Scripting* (XSS)*:*** se trata de la utilización de scripts maliciosos en sitios web para atacar a los usuarios que visitan dichos sitios, así pues, roban información y atacan en nombre del usuario.
- ***Rootkit:*** son herramientas que posibilitan que el atacante tenga acceso continuo y no detectado en algún sistema o dispositivo.
- ***Keylogger:*** A través de un software o hardware que identifica el uso de pulsaciones de teclas del usuario pueden robar información como contraseñas y datos personales.
- ***Botnets:*** Se trata de redes de dispositivos infectados y controlados y que pueden ser utilizados para realizar ataques tipo DDoS, *spam* y otros ataques maliciosos.

También, por otro lado, se dan ciertos tipos de ataques cibernéticos perpetrados con la intención de generar violencia digital contra personas u organizaciones y por ende causan daño emocional. Esto, a su vez, expande el temor de que las agresiones pasen del ámbito virtual a lo real. Es decir, en estos tipos de amenazas, la tecnología es utilizada como un medio (TEDIC, 2016). Es pertinente mencionar algunos de estos tipos de agresiones que se dan en el ciberespacio y que, sin dudas, afectan la ciberseguridad. Según Sequera y Acuña (2023), algunas de estas violencias de género facilitadas por la tecnología pueden ser[11]:

> Amenaza a la integridad física y a la vida. b) Discursos de odio y denigrantes. c) Extorsión. d) Difamación en línea. e) Vigilancia. f) *Doxxing*, g. Acoso en línea. h) Difusión de imagen intima no consentida. i) Recepción de materiales sexuales no solicitados. j) *Mobbing* laboral. k) *Cyberbullying*. l) Ataques coordinados.

Estos ataques de violencia de género facilitada por la tecnología se desarrollan con una frecuencia puntual o coyuntural como así también, de manera constante y prolongada. La ocurrencia de los mismos coincide con la búsqueda de influenciar sobre opiniones en temas controversiales, como, por ejemplo: cambio climático, vacunación, salud sexual y reproductiva, entre otros.

Por lo general las amenazas a la ciberseguridad que se dan a través de las redes sociales, ya sean personales, profesionales u organizacionales. Comúnmente las personas subestiman las vulnerabilidades de estar en línea y existen diversos tipos de riesgo de exposición, así pues, se puede constatar que uno de los más comunes ocurre cuando se envía una solicitud de amistad e intenta hacer contacto con la posible víctima, la aceptación de vínculo podría ayudar a la persona atacante a recopilar gran cantidad de información, lugar de trabajo, donde reside, números telefónicos entre otros datos personales. En la segunda etapa, utilizan mensajería espontánea (vía WhatsApp o Facebook Messenger) para solicitar información directamente a la víctima (Martínez y Ávila: 217, 2021).

11 Para conocer en profundidad cada tipo de violencia se recomienda conocer el trabajo del TEDIC en materia de recolección y clasificación de casos de violencia digital (casos de violencia digital de género, hacia mujeres periodistas y hacia mujeres políticas). Disponible en www.tedic.org

LAS ORGANIZACIONES DE LA SOCIEDAD CIVIL Y SUS NIVELES DE CIBERSEGURIDAD

Es importante conocer los aportes de la literatura científica y en función a las evidencias halladas como respuestas que dan o pueden dar las organizaciones al tema de ciberseguridad. En este sentido, Sancho (2017) sistematiza documentos de organismos multilaterales y plantea los grados de madurez en materia de seguridad digital que pueden ser hallados en las instituciones y organizaciones (Sancho, 2017). A continuación, se da cuenta de lo que refiere la información:

FASE 1

Desconocimiento: la organización considera que el riesgo en materia de seguridad digital es muy poco relevante y no forma parte del proceso de gestión del riesgo institucional. La organización no conoce su nivel de interconexión.

FASE 2

Fragmentación: la organización reconoce la hiperconectividad como un foco potencial de riesgo y posee una percepción limitada de sus prácticas de gestión en el ciberespacio. La organización aplica un enfoque independiente en referencia al riesgo en Internet con una presentación de información fragmentada y casual.

FASE 3

Descendente: la máxima autoridad de la organización marca las pautas con respecto a la gestión del riesgo en Internet e inicia un abordaje de carácter descendiente de amenaza-riesgo-respuesta, sin embargo, no considera la gestión de riesgo cibernético como una ventaja medular para la organización.

FASE 4

Dominio: la máxima autoridad de la organización conoce plenamente la información con respecto a la gestión del riesgo en Internet, y plantea el desarrollo de políticas y acciones, así como define responsabilidades y mecanismos para la presentación de información. Comprende las vulnerabilidades de la organización, sus controles y sus interdependencias con terceras partes.

FASE 5

Interconexión: la organización está altamente conectada con sus pares y aliados, comparten información y mitigan conjuntamente riesgos en Internet como parte de sus operaciones rutinarias. Sus colaboradores demuestran una conciencia cibernética de uso y la organización está segura en materia de ciberseguridad.

Existen diferentes opciones para proteger la seguridad digital de las organizaciones. Es importante analizar como funciona la organización para escoger las mejores medidas o herramientas de seguridad, ya sea, construyendo una nueva herramienta o reutilizando alguna ya existente, o bien, construirla pensando en reutilizarla (Bewlay et al., 2021). La participación colectiva en procesos de construcción digital para organizaciones de la sociedad civil es clave para generar un nivel de protección fuerte y capaz de dar respuestas a eventuales ataques. El involucramiento de las personas es clave para garantizar un ecosistema de información sólido que se irá actualizando por el propio interés de los participantes de la comunidad (Paes, 2024).

PARAGUAY Y CIBERSEGURIDAD

La ciberseguridad en Paraguay es un tema que necesita ser socializado con actores del estado, el sector privado y la sociedad civil, de tal forma a transparentar procesos de regulación e implementación de la seguridad digital en el país. El estado debe propiciar una gobernanza participativa a fin de robustecer la democracia. Si bien, actualmente, se cuenta con centros de monitoreo que van registrando casos de vulnerabilidad y ataques, es preciso, reflexionar sobre el ecosistema que conforma la seguridad digital, como por ejemplo, la necesidad de una Ley de integral de protección de datos personales.

La visión del rol defensivo sobre la ciberseguridad en temas que atañen a asuntos militares o procesos bancarios, es una preponderante en el país. Sin embargo, es necesario tratar asuntos de ciberseguridad desde la mirada centrada en las personas, como principal objetivo, y así dar protección y garantía a deberes y derechos de las mismos. Pues, este es un tema no sólo técnico o de seguridad nacional. Es precioso, desde la mirada de los derechos humanos, actualizar el debate y plantear mecanismos efectivos y participativos para elevar la gestión del riesgo en asuntos digitales.

Normas vinculadas a ciberseguridad en Paraguay

Es preciso señalar que aún se necesita avanzar en materia de regulación normativa en lo que compete a ciberseguridad en el Paraguay. Sin dudas, una de las leyes más necesarias de crear es la Ley Integral de Protección de datos Personales (Sequera, 2019). No obstante, en los últimos años se han dado algunos pasos en cuanto a la aprobación de leyes, decretos presidenciales y resoluciones ministeriales. A continuación, se mencionan algunos hitos histórico-institucionales vinculantes al tema, pero que no agotan la necesidad de normativas más específicas:

- **Ley Nº 4989/2013**, "Que crea el marco de aplicación de las tecnologías de la información y comunicación en el sector público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs[12])"[13], y que luego con el **Decreto Nº 11.624/2013**, quedó reglamentada la institución y asentada la nueva estructura rectora en materia de políticas públicas para las TICs en el Paraguay.

  Así también, se destaca que con este decreto se creó la Dirección General de Políticas y Desarrollo de TICs y bajo la dependencia de ésta se constituyó la creación del Centro de Respuestas ante Incidentes Cibernéticos (CERT-PY), que es la instancia encargada de facilitar y fomentar la protección de los sistemas cibernéticos y de la información que respaldan la infraestructura nacional tanto gubernamental como del sector privado, así como para dar respuestas rápidas a los incidentes cibernéticos. Con intención de lograr mayor efectividad y aunar esfuerzos desde el legislativo en materia de TICs se aprobó el **Decreto Nº 5323/2016**, "Por el cual se reglamentan los Arts. 20 y 21 de

12 Se aclara que el actual órgano rector de las TICs en Paraguay es el Ministerio de Tecnologías de la Información y la Comunicación (MITIC), anteriormente la institución disponía de otro rango: Secretaría Nacional de Tecnologías de la Información y la Comunicación (SENATICs) y previamente, era conocida como Secretaría de Tecnologías de la Información y Comunicación (SETICs).

13 Con la aprobación de esta norma, fue derogada la Ley Nº 8.716/2012 "Por la cual se crea y reglamenta la Secretaría de Tecnologías de la Información y Comunicación (SETICs)".

la Ley Nº 4989/2013", básicamente, a través de dicha norma se disponía que los Organismos y Entidades del Estado debían integrar el Comité de Coordinación e Interoperabilidad y que el mismo tenía como responsabilidad desarrollar un plan anual de trabajo[14].

- **Ley Nº 6.207/2018**[15], "Que crea el Ministerio de Tecnologías, Información y Comunicación y establece su carta orgánica". A través de dicha reglamentación fue creada también y en dependencia al MITIC, la Dirección General de Ciberseguridad y Protección de la Información, dependiente a su vez del Viceministerio de Tecnologías de la información y Comunicación. Luego con el **Decreto Nº 2274/2019** se reglamenta la citada ley. Es importante destacar que, el MITIC reemplaza a la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs), cambiando de estatus institucional dentro de la jerarquización de la Poder Ejecutivo, así pues, pasó de Secretaría a Ministerio.

  Se destaca la **Resolución MITIC Nº 346/2020** a través de la cual se aprueba e implementa el reglamento de reporte obligatorios de incidentes cibernéticos de seguridad por parte los Organismos y Entidades del Estado (OEE) al Ministerio de Tecnologías de la Información y Comunicación (MITIC), a través del Centro de Respuestas a Incidentes Cibernéticos (CERT-PY), dependiente de la Dirección General de Ciberseguridad y Protección a la Información. A través de dicha resolución se indica que cualquier ciudadano, empresa, institución pública u organización extranjera puede reportar un incidente cibernético que afecte a un sistema de información del ecosistema digital nacional, propio o de terceros.

- **Decreto Nº 6234/2016**[16]. "Por el cual se declara de interés nacional la aplicación y el uso de las tecnologías de la información y comunicación (TIC), se define la estructura mínima con la que deberá contar y se establecen otras disposiciones para su efectivo funcionamiento", a través del cual el Poder Ejecutivo ordena a todas las instituciones del Ejecutivo a que cuenten con una única área especializada en Tecnología de la Información y de la Comunicación. Este decreto fue relevante por la institucionalizar y ordenar los asuntos vinculados a las TICs en general.

- **Decreto Nº 7052/2017**. "Por el cual se aprueba el Plan Nacional de Ciberseguridad y se integra la Comisión Nacional de Ciberseguridad". El Plan es el documento que plantea el fundamento para considerar y accionar en materia de ciberseguridad. El mismo señala que buscan integrar a los sectores involucrados con las TIC para alcanzar un mayor crecimiento económico y maximización de los beneficios, consiguiendo así un ciberespacio más estable, seguro, confiable y resiliente.

  En dicho decreto fueron trazados siente puntos de acción a ser desarrollados desde el liderazgo del Poder Ejecutivo: i) Sensibilización y Cultura; ii) Investigación, Desarrollo e Innovación; (iii) Protección de Infraestructuras Críticas; (iv) Capacidad de Respuesta antes Incidentes Cibernéticos; (v) Capacidad de Investigación y Persecución de la Ciberdelincuencia; (vi) Administración Pública; y (vii) Sistema Nacional de Ciberseguridad.

---

14 Se destaca que una de las áreas más atendidas por lo sensible de la temática es lo que compete al sector niñez y adolescencia. Así pues, se creó la Ley Nº 5653/2016, "De protección de niños, niñas y adolescentes contra contenidos nocivos de internet". Luego con el Decreto Nº 8098/2022 es reglamentada dicha ley y posterior a esto con la Resolución SENATICs Nº 143/2017 se aprueban las especificaciones técnicas mínimas del software mencionadas en la citada ley. Unos años más tarde, con la Resolución MITIC Nº 699/2019 fueron aprobados los "Criterios mínimos de seguridad para el desarrollo y adquisición de Software".

15 Ésta norma derogó a la Ley Nº 4989/13 y a su vez fue declarada la extinción de la SICOM y de la SENATICs respectivamente.

16 Este decreto a su vez derogó al Decreto Nº 1840/2014: "Se declara de interés nacional la aplicación y el uso de las Tecnologías de la Información y Comunicación (TICS) en la gestión pública y se ordena la implementación de las Unidades Especializadas TICS en las instituciones dependientes del Poder Ejecutivo".

También quedó establecida la Comisión Nacional de Ciberseguridad, que está integrada por las siguientes instituciones[17]:

a. Ministerio de Relaciones Exteriores
b. Ministerio de Defensa Nacional
c. Ministerio del Interior
d. Policía Nacional
e. Ministerio de Industria y Comercio
f. Ministerio de Educación y Ciencias
g. Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
h. Comisión Nacional de Telecomunicaciones (CONATEL)
i. Consejo Nacional de Ciencia y Tecnología (CONACYT)
j. Centro Nacional de Computación (CNC)
k. Instituto de Previsión Social (IPS)
l. Ministerio Público
m. Poder Judicial
n. Poder Legislativo

- **Ley Nº 6822/2021**, "De los servicios de confianza para las transacciones electrónicas, del documento electrónico, y de los documentos transmisibles electrónicos". El objeto estipulado por esta norma trata sobre el marco jurídico para la identificación electrónica, firma electrónica, el sello electrónico, el sello de tiempo electrónico, el documento electrónico, el expediente electrónico, el servicio de entrega electrónica certificada, el servicio de certificado para la autenticación de sitios web, el documento transmisible electrónico y en particular para las transacciones electrónicas. Luego con el **Decreto Nº 7576 /2022**, fue reglamentada la mencionada ley.

Ministerio Público - Unidad Especializada de Delitos Informáticos

En el año 2001 se crea el Convenio de Budapest sobre delitos informáticos y delitos en Internet, Paraguay lo ratificó en el año 2017 e inicia un proceso de armonización con las leyes y el sistema penal local (Sequera y Samaniego, 2018). En Paraguay, la instancia legal encargada para proceder y dar curso a investigaciones sobre casos de delitos informáticos en Paraguay es el Ministerio Público, a través de la Unidad Especializada en Delitos Informáticos, que fue creada en el año 2010 por Resolución de FGE Nº 3459/10 y ampliada por Resolución de FGE Nº 4408/2011. Accionan contra hechos punibles cometidos o facilitadas a través de la tecnología. Según las Resoluciones Nº 3459/10 y 4408/2011, los tipos penales de competencia exclusiva de la Unidad Especializada en Delitos Informáticos son los siguientes: Acceso indebido a datos, interceptación, preparación al acceso indebido a datos, alteración de datos, acceso indebido a sistemas informáticos, sabotaje a sistemas informáticos, alteración de datos relevantes, falsificación de tarjetas de crédito y débito y estafa mediante sistemas informáticos[18]. Así también, al consultar su sitio web se observa que la institución plantea dar respuestas de capacitaciones en materia de *cyberbullying*, *sexting*, pornografía infantil y *grooming*.

17 El decreto también indica que podrán integrar la Comisión Nacional y los Subcomités Especializados de trabajo, organizaciones de la sociedad civil, del sector privado y de la academia. El responsable de convocar y garantizar la participación de estas instancias es el Coordinador Nacional de Ciberseguridad y la Comisión Nacional de Ciberseguridad misma.

18 Ministerio Público. (2024). Unidad Especializada de Delitos Informáticos. https://ministeriopublico.gov.py/unidad-especializada-de-delitos-informaticos-. Accedido el 06 de mayo de 2024.

Gobierno Nacional y sus políticas públicas sobre ciberseguridad

El MITIC inició un proceso para actualizar la Estrategia Nacional de Ciberseguridad de Paraguay 2024-2028 (ENC PY)[19]. La intención actual del gobierno es convertir en un *hub* tecnológico regional al país, esto responde a la necesidad de mostrar seguridad digital para que inversores decidan asentarse en el Paraguay. Las preocupaciones de actualización tecnológica apuntan a la criptomoneda, la nube, y la inteligencia artificial. Mientras que las preocupaciones sobre las amenazas refieren a que tratan sobre posibles pérdidas financieras, robo de datos personales e interrupciones en el servicio, entre otros.

En el 2023, el Gobierno Nacional firmó un convenio en materia de ciberseguridad con los Estados Unidos de Norteamérica, las instituciones encargadas de encaminar y presentar el convenio fueron la Dirección General de Ciberseguridad y Protección a la Información (DGCPI), del MITIC, y la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA)[20]. En este sentido, el acuerdo firmado entre Paraguay y los Estados Unidos de América, marca el camino que se transitará[21] en materia de tecnología digital, tanto en infraestructura como en la promoción de internet. Se destaca que la defensa digital es uno de los puntos medulares que plantean trabajar con el convenio.

Reporte de incidentes cibernéticos

Según la última publicación del CIRT-PY (2022), las estadísticas de los últimos incidentes cibernéticos en el país y que fueron reportados por instituciones del Estado, CSIRTs extranjeros, empresas del sector privado y ciudadanos, dan cuenta de que fueron recibidos 3.668 reportes de incidentes y la institución logró atender a 2.083 de estos casos. El informe indica que la mayor cantidad de estos sucesos tienen que ver con los sistemas o dispositivos comprometidos (*defacement*), servidores con códigos maliciosos y *phishing* principalmente. Mientras que, los de menor perpetración, pero que ocurren, tienen que ver con casos de *ransomware*.

Las vulnerabilidades identificadas se relacionan con contraseñas débiles, desactualizaciones y también con *malwares* siendo partes de *Botnets* (*Emotet, Avalanche, botnet Hajime*). El documento también señala que no tuvieron registros de ataques de DoS/DDoS, pero indican que, por lo general, cuando se da este tipo de casos, las víctimas prefieren reportar directamente a los proveedores del servicio de internet. Lo mismo ocurre con accesos indebidos a cuentas o datos, que las víctimas prefieren contactar directamente con las plataformas del servicio, sea Google, Facebook o X, entre otros. Esta situación demuestra que falta ampliar y unificar el sistema de registro de incidentes cibernéticos en el país.

19 Ministerio de Tecnologías, Información y Comunicación. (06 de junio de 2024). Por qué es importante para el Paraguay actualizar su Estrategia Nacional de Ciberseguridad. https://mitic.gov.py/por-que-es-importante-para-el-paraguay-actualizar-su-estrategia-nacional-de-ciberseguridad/. Accedido el 12 de junio de 2024.

20 Diario La Nación. (2023). Destacan hito en ciberseguridad paraguaya tras acuerdo de cooperación con EE. UU. www.lanacion.com.py/politica/2023/07/06/destacan-hito-en-ciberseguridad-paraguaya-tras-acuerdo-de-cooperacion-con-ee-uu/. Accedido el 13 de junio de 2024.

21 Diario ABC Color. (2023). Paraguay firma con EEUU acuerdo de ciberseguridad. www.abc.com.py/politica/2023/11/11/paraguay-firma-con-eeuu-acuerdo-de-ciberseguridad/. Accedido el 26 de mayo de 2024.

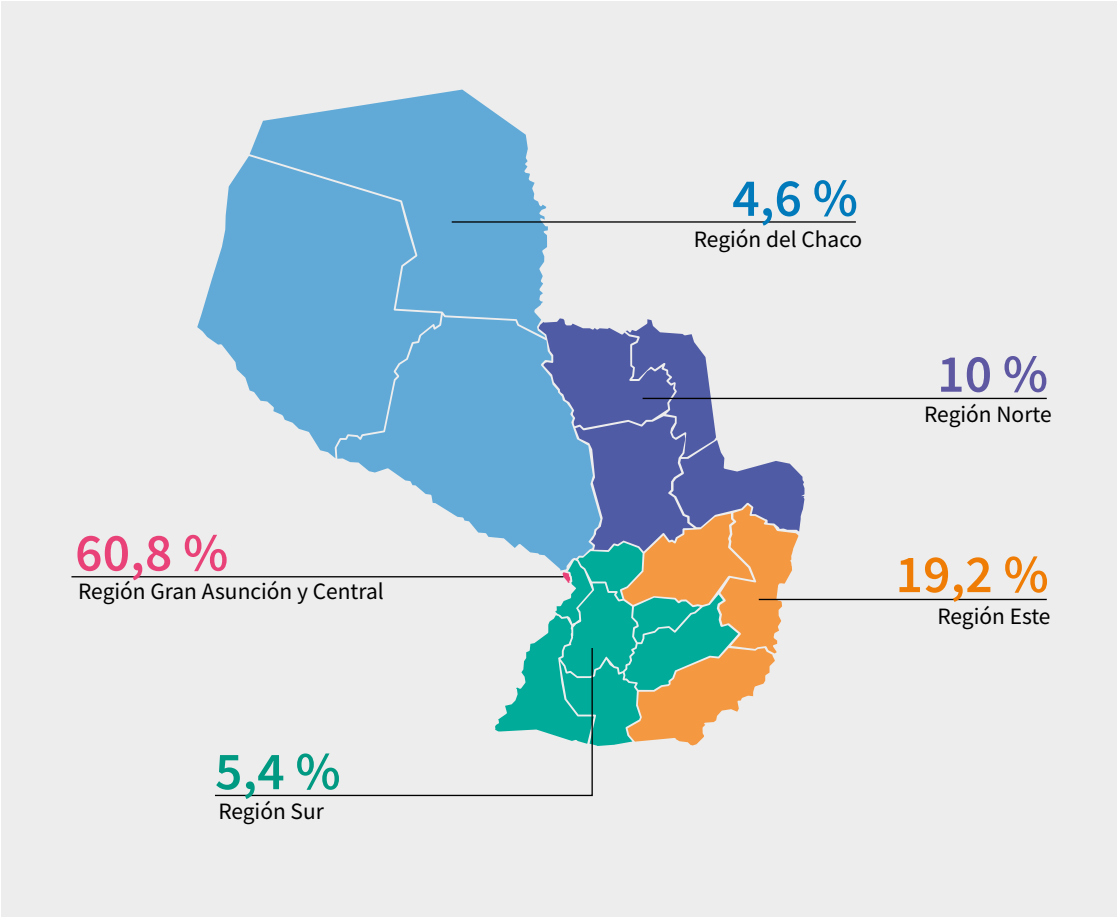
HALLAZGOS CUANTITATIVOS

La encuesta recogió información de ciento treinta (130) defensores y defensoras de derechos humanos del Paraguay. Los bloques de la encuesta se centraron en información de las personas relacionadas a: a. datos demográficos, b. ubicación y desplazamiento, c. infraestructura y herramientas digitales, d. seguridad, e. riesgos y amenazas, y f. violencia basada en género. La adscripción organizacional de defensores y defensoras fue variada, así manifestaron pertenecer a organizaciones campesinas, indígenas, urbanas, ambientales, de salud, de niños, niñas y adolescentes, de libertad de expresión, feministas, LGTBIQ+, juveniles, estudiantiles, entre otros.

A. DATOS SOCIODEMOGRÁFICOS

El rango de edad de participantes correspondió a 31,5 % de 18 a 28 años; 36,9 % de 29 a 45 años; 25,4 % de 46 a 60 años y de 60 años en adelante 6,2 % respectivamente. Las personas encuestadas mayormente residen en la Región Gran Asunción y Central con el 60,8 %; en la Región Este (Caaguazú, Itapúa y Alto Paraná) residen el 19,2 %; en la Región Norte (Amambay, Concepción, Canindeyú y San Pedro) el 10 %; en la Región Sur (Cordillera, Guairá, Caazapá, Misiones, Paraguarí, Central y Ñeembucú) el 5,4 %; en la Región del Chaco (Alto Paraguay, Boquerón y Presidente Hayes) el 4,6 % respectivamente.

GRÁFICO 1. Área de residencia de las personas defensoras encuestadas*.



*Observación: Sobre una base de ciento treinta (130) encuestados.

En cuanto al grado de escolaridad, la muestra señala que la composición de personas encuestadas ha sido de 0,8 % no tiene escolaridad; 4,6 % desarrolló la primaria; 16,9 % alcanzó la secundaria; 10,8 % completó alguna tecnicatura universitaria; 57,4 % es profesional de grado y 23,1 % es profesional con posgrado.

Los porcentajes sobre las preferencias de recibir o seguir instrucciones o sugerencias de aprendizaje resultaron muy próximas, mostrando pequeñas variaciones. La mayoría de las personas participantes indicaron que al momento de recibir instrucciones o sugerencias de aprendizaje se sienten más cómodas siguiendo instrucciones con un esquema de imágenes paso a paso (37,7 %); en segundo lugar, les gusta seguir instrucciones desde un documento escrito (36,9 %); y, por último, indicaron que les parece mejor seguir instrucciones desde un video (25,4 %).

Las personas encuestadas se identificaron mayormente como latinos, alcanzando el 42,3 %; luego como mestizos, alcanzando el 34,6 %; posteriormente como blancos con el 7,7 %; como indígenas se identificaron el 6,9 %; y, con 0,8 % como afrodescendientes. Resulta significativo que el 7,7 % refirió que no se siente identificado con ninguna de las anteriores.

Al consultar sobre si las personas encuestadas contaban con algún tipo de discapacidad, el 95,4 % refirió que no y el 4,6 % manifestó que sí. De este último grupo, las discapacidades más frecuentes son las de tipo visual (50 %), y luego con el 16,7 % cada una, las de tipo auditiva, física y psicosocial.

El 61,5 % de las personas encuestadas se identificó como mujer; el 35,4 % como hombre; 2,3 % como persona no binaria; 0,8 % como hombre trans. Mientras que la pregunta sobre orientación sexual mostró el siguiente resultado: 62,3 % dijo ser persona heterosexual; 20 % como persona bisexual; 6,9 % como persona homosexual; 1,6 % como asexual (hetero afectiva y demisexual); 1,5 como persona pansexual; y el 7,7 % no quiso compartir esta información.

B. UBICACIÓN Y DESPLAZAMIENTO

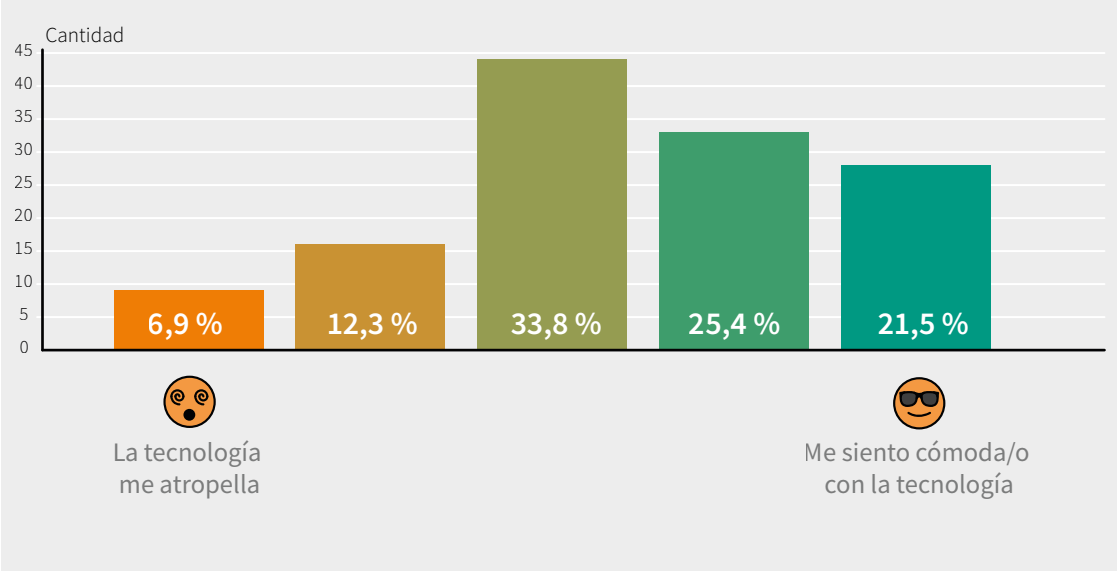
Sobre la consulta referida a la zona en la que vive, el 53,8 % de las personas señaló que vive en alguna capital departamental, el 23,1 % en alguna cabecera municipal y también con el 23,1 % en áreas rurales. Por su parte, en relación a la pregunta en qué tipo de zona desempeña su trabajo, el 60,8 % mencionó que lo hace en cabeceras departamentales; el 26,2 % en áreas rurales y el 13,1 % en cabeceras municipales.

Las personas encuestadas indicaron que se desplazan fuera de sus ciudades y/o barrios en el que viven con las siguientes frecuencias porcentuales: 34,6 % lo hace semanalmente; 33,8 % de manera diaria; 26,9 % mensualmente; 2,3 % anualmente y 2,3 % no viaja.

C. INFRAESTRUCTURA Y HERRAMIENTAS DIGITALES

Al preguntar a las personas ¿Cómo se siente en relación con el uso de tecnologías digitales? Las personas respondieron, valorando en una escala de 1 a 5, donde 1 representó "La tecnología me atropella" y 5 "Me siento cómoda/o con la tecnología (instalo y pruebo herramientas y tengo medidas de seguridad en mis cuentas), la mayoría de las personas coincidió que se encuentra en un grado intermedio, es decir en el rango 3 con el 33,8 % y luego se observa una escala descendente del rango 4 (25,4 %) y rango 5 (21,5 %). Para el caso del rango 1, donde la persona principalmente se siente atropellada por la tecnología se registró a un grupo de 6,9 %, mientras que el rango 2 alcanzó el 12,3 %.

GRÁFICO 2. Identificación con relación al uso de la tecnología*.



Observación: Los rangos próximos al 1 representó "La tecnología me atropella" y los cercanos al 5 "Me siento cómoda/o con la tecnología (instalo y pruebo herramientas y tengo medidas de seguridad en mis cuentas).

Sobre el uso de tecnologías digitales, 63,1 % mencionó que utiliza la tecnología de manera autónoma; 23,1 % señaló que consulta con alguien en el trabajo o red de apoyo; y 13,8 % manifestó que siempre consulta con un familiar o amigo cercano.

Las actividades que realizan a través de las tecnologías digitales, mayormente lo hacen con fines de Educación y trabajo (Participa de reuniones virtuales para su trabajo o procesos de formación) al 85,4 %; con fines de Entretenimiento y comunicaciones (Accede a redes sociales y mensajería espontánea), coincidieron al 70 %; y con fines de Incidencia digital (desarrolla una agenda política o social a través de medios digitales), lo hacen al 27,7 %.

Al momento de seleccionar los dispositivos que utilizan para sus actividades cotidianas, defensores y defensoras señalaron al 99,2 % de coincidencia que el celular es el principal dispositivo utilizado; en segundo lugar, computadoras portátiles (76,9 %); en tercer lugar, y de manera compartida con el 18,5 % computadoras de escritorio y memoria USB; en el cuarto lugar, disco duro externo (16,2 %), en quinto lugar, tabletas (13,8 %); en sexto lugar, relojes inteligentes o similares (7,7 %); y por último, asistente de voz (6,9 %).

Las personas distinguieron las opciones sobre cómo se conectan a internet, señalaron al 76,9 % que la manera más común es a través de datos personales; el 71,5 % indicó que lo hace a través de internet del hogar; 53,1 % a través de internet en el trabajo; 20 % a través de punto wifi de un privado; 13,8 % a través de plan de datos provistos por el trabajo; 2,3 % a través de plan de datos provistos por alguna cooperación internacional; 11,5 % a través de internet público (en plazas o bibliotecas, etc.); 8,5 % en algún café Internet; 6,3 % a través de sistema prepago.

De manera mayoritaria, al 98,5 % las personas defensoras refirieron que cuentan con señal de telefonía celular donde realizan sus actividades de forma cotidiana, en contraposición al 1,5 % que no dispone del mismo.

Las personas defensoras indicaron que para las actividades del trabajo utilizan los siguientes tipos de herramientas: 116 personas usan cuentas de correo personal; 104 defensores se comunican a través de apps de mensajería instantánea (WhatsApp, etc.); 97 personas también coinciden en utilizar herramientas de almacenamiento en la nube; 90 personas se valen de cuentas de redes sociales; 70 defensores prefieren cuentas de correo exclusivo para el trabajo; 21 cuenta con software de seguridad (antivirus, herramientas de elusión, etc.); 19 utiliza transmisión en vivo; 2 usan software de apoyo para capacidades diversas; y 4 personas manifestaron otro tipo de actividades.

En la sección relacionada a redes sociales, las personas escogieron bajo criterios de selección múltiple cuáles son las redes sociales que utilizan, sus respuestas mostraron que utilizan Facebook al 86,2 %; Instagram al 76,9 %; Twitter al 62,3 %; TikTok al 38,5 %; Snapchat al 6,2 %; y, por último, un acumulado del 6,4 % indicó otro tipo de redes (LinkedIn, Pinterest, etc.).

Las personas encuestadas marcaron que se sirven como principal tipo de mensajería instantánea de WhatsApp (100 %), luego Facebook Messenger (41,5 %), posteriormente Telegram (41,6 %); le sigue Signal (12,3 %), y, por último, el (1.6 %) mencionó otro tipo de mensajería (Outlook chat e Instagram chat). En un siguiente campo de consulta sobre otro tipo de red social que utilizan, las personas indicaron Instagram, LinkedIn, Tinder, Slack, Reddit, Tumblr e iMessage.

En cuanto a la realización de transmisiones en vivo, las personas que manifestaron valerse de este recurso, dijeron que utilizan Facebook Live (42,4 %), Instagram Live (42,4 %), Twitter Spaces (5,4 %), Twtich (4.3 %), y Youtube en vivo (17,4 %).

De las personas encuestadas, el 54,6 % indicó que administra redes sociales, sitios web o cualquier otro servicio digital para la organización en la que trabaja, en contraposición, el 45,4 % no lo hace. Las personas que pertenecen al primer grupo, mencionaron que manejan redes sociales (Instagram, X, Facebook, TikTok), páginas webs y Apps Web, así como el WhatsApp de la organización.

Sobre la sección que indagó sobre el sistema operativo con el que cuentan en sus computadoras, el 44,6 % mencionó que utiliza Windows legalmente adquirido; 18,5 % Windows pirata o sin licencia; el 29,2 % señaló que usa Windows, pero no sabe si es legal o sin licencia; 5,4 % utiliza Mac iOS X (Apple); 4,6 % GNU/Linux (Software libre); y el 11,7 % no sabe la denominación del sistema operativo que utiliza.

La mayoría de las personas defensoras, al 97,1 % utiliza como dispositivo de comunicación el teléfono inteligente Smart; el 11,5 % también usa teléfono de línea baja; el 3,8 % dijo usar teléfono satelital; y con el 0,8 % mencionó a la Tablet.

Al ser abordados con la pregunta referida al programa con el que funcionan sus teléfonos móviles, las personas dijeron Sistema Android (80 %); iPhone iOS (17,7 %); Windows Phone 0,8 % y otros al 2,4 %.

Los medios de comunicación que más utilizan para el trabajo son: WhatsApp (96,9 %); Correo electrónico (75,4 %); Llamadas telefónicas desde el celular (60,8 %); Google Meet (41,5 %); Conversaciones en persona (34,6 %); Zoom (16,9 %); Facebook o Messenger (13,1 %); Teams (7,7 %); Llamadas desde línea baja (4,6 %); Twitter (4,6 %); SMS (2,3 %); Skype (1,5 %) y otros (2,4 %).

D. SEGURIDAD

El porcentaje alto de respuestas, al 76,2 % de las personas encuestadas, indican que no han recibido algún tipo de capacitación en materia de seguridad digital, en contraposición al 23,8 % que sí recibió alguna capacitación. Las personas que manifestaron haber recibido alguna capacitación, agregaron que lo hicieron antes o durante la pandemia, otro grupo menor lo hizo de manera reciente en un plazo cercano a 1 año.

Sobre la sección que abordó la consulta referida a conocer si la persona ha realizado algún análisis de riesgo en seguridad digital, el 91,5 % señaló que no lo ha hecho, en contraposición al 8,5 % que manifestó que sí lo hizo. De este último grupo, los periodos que referenciaron como tiempo en el que realizaron el último análisis, algunos dijeron año 2021, y luego el año 2023, también, se destaca un comentario que mencionó “realizo todo el tiempo, pero debo tomar acciones de seguridad”.

El porcentaje de personas que utiliza la misma contraseña para más de una cuenta es de 56,2 % en contraposición al 43,8 % que utiliza contraseñas diferentes para sus cuentas. Al consultarles si al ingresar al navegador sus cuentas se abren automáticamente sin pedir contraseñas, el 70 % señaló que sí.

Al ser abordados sobre si comparte sus dispositivos digitales, el 84,6 % manifestó que no lo hace y el 15,4 % mencionó que sí lo comparte. Y, por el contrario, al ser consultados si las personas prestan dispositivos de otras personas, las respuestas fueron al 79,2 % que no y al 20,8 % que sí. Las personas que comparten dispositivos en ambos grupos, señalaron que comparten computadoras de escritorio del hogar, del trabajo, notebooks, tabletas y celulares.

El 52,3 % indicó que cuentan con copia de respaldo (backup) de la información almacenada en sus dispositivos; el 21,5 % referenció que no dispone del mismo y el 26,2 % dijo que no sabe.

Sobre las medidas de seguridad que las personas defensoras adoptan, el 88,5 % señaló que tiene clave de acceso en el teléfono (ej. contraseña, pin, patrón o huella); 65,4 % corresponde a que tiene clave de acceso en mis otros dispositivos como computadores o tabletas (ej. contraseña, pin, patrón o huella); 37,7 % usa antivirus en la computadora o tableta; 16,2 % usa antivirus en el celular; 0,8 % VPN o authenticador; el 3,8 % ninguna; y otros 1,6 %.

También, las personas defensoras de DDHH, dijeron que siempre cierran sus sesiones cuando terminan de utilizarlas en un dispositivo que no les pertenece (74,6 %); usan contraseñas diferentes para todas sus cuentas (34,6 %); usan autenticación de dos pasos (40,8 %); almacenan sus contraseñas en un lugar seguro o en un programa de gestión de contraseñas (ej. KeePass, 1Password, BitWarden, etc.) (11,5 %); cifran el contenido de sus dispositivos (9,2 %); borran regularmente

datos sensibles (ej. mensajes, fotos, etc.) de sus dispositivos móviles (ej. teléfono, portátil, tableta) (40,8 %); revisan regularmente las configuraciones de seguridad y privacidad de sus cuentas y dispositivos (16,2 %); hacen copias de respaldo en soportes externos como discos duros externos, memorias USB (15,4 %); hacen copias de respaldo en la nube (ej. iCloud, Google Drive, Microsoft OneDrive) (35,4 %); ninguna (7,7 %); mientras que 3,2 % mencionaron otro tipo de prácticas, como por ejemplo borrar datos sensibles pero no regularmente; la realización de trabajos en la nube (Google drive) y usar diferentes cuentas de trabajo; tener cuentas diferentes para actividades diferentes; navegar de incógnito y también que utilizan de forma aleatoria y no sistemática los diferentes tipos de seguridad.

Al ser consultadas las personas sobre las medidas de seguridad que utilizan las personas para proteger su red Wifi, el 70,8 % manifestó que usa contraseñas fuertes para la red Wifi; 10,8 % cambia la contraseña de la red Wifi periódicamente; 3,1 % señaló que crean una red de invitados diferente a la de uso propio y 20,5 % señaló que no utiliza ninguna medida de seguridad.

E. RIESGOS Y AMENAZAS

El 94,6 % de las personas encuestadas señaló que la organización a la cual pertenece no cuenta con algún protocolo de seguridad para atender situaciones de riesgo o amenazas digitales, solo el 5,4 % manifestó que sí cuentan con protocolos y detallaron que entre las acciones que consideran los protocolos se destacan los siguientes puntos: comunicar el incidente al punto focal de tecnología informática; no abrir enlaces sospechosos; activar VPN cuando ingresamos a una App de la organización; criterios de uso de contraseña (extensión y caracteres, así como cambio periódico); entre otros. Los valores porcentuales de registro de incidentes de seguridad indican que el 94,6 % dijo que no cuentan con registro de incidentes de seguridad digital.

GRÁFICO 3. Disponibilidad de protocolos de seguridad digital en las organizaciones.

Es importante señalar que las personas indicaron que tanto el protocolo como el registro en materia de incidentes de seguridad digital en la organización, por lo general recae en el equipo de informática y/o el de comunicación, mientras que los demás miembros no conocen sobre los procedimientos.

Sobre la identificación de posibles amenazas digitales más inmediatas y graves que las personas defensoras identifican como potenciales y que pueden estar enfrentando de manera personal u organizacional, seleccionaron las siguientes opciones:

Ingreso no autorizado (*hackeo*) al correo o cuentas en redes sociales.	**63,1 %**
Recepción de *phishing*: enlaces a sitios falsos a través de mensajes de texto, mensajería instantánea o correo electrónico, con el fin de robar información personal e información de acceso, o instalar, programas maliciosos.	**43,1 %**
Pérdida de información.	**32,3 %**
Acoso sexual a través de redes sociales, correo electrónico, llamadas o mensajes de texto.	**24,6 %**
Robo de dispositivos (celulares, computadores, tabletas, discos duros, USB).	**30 %**
Acoso a través de redes sociales, correo electrónico, llamadas o mensajes de texto.	**18,5 %**
Borrado de información en el sitio web de la organización o plataformas de terceros donde se almacena información.	**16,2 %**
Secuestro de información de la organización con fines extorsivos (*Ransomware*).	**12,3 %**
Confiscación de dispositivos por autoridades (ej. Policía, Ejército, Fiscalía).	**14,6 %**
Ingreso no autorizado (*hackeo*) a la página web de la organización.	**13,1 %**
Matoneo o acoso a través de redes sociales, correo electrónico, llamadas o mensajes de texto.	**9,2 %**
No creo estar enfrentando ninguna amenaza.	**9,2 %**
Alteración de la información en el sitio web de la organización o plataformas de terceros donde se almacena información.	**8,5 %**
Retención de dispositivos por grupos ilegales (ej. bandas criminales, narcos).	**7,7 %**
Otras situaciones. Las personas indicaron que les preocupa la recepción de llamadas sin saber cómo obtuvieron sus números telefónicos, mencionaron que reciben constantemente solicitud de amistad de perfiles extraños, generalmente uniformados militares con apariencia extranjera, entre otros.	**2,4 %**

Ante la pregunta: En el último año, ¿Usted, alguna persona de su organización o su organización ha sufrido algún incidente de seguridad digital?[22] El 58,5 % indicó que no ha sufrido algún incidente digital, mientras que el 41,5 % señaló que sí. De este último grupo, las personas seleccionaron los siguientes tipos de ataques recibidos:

Ingreso no autorizado (hackeo) al correo o cuentas en redes sociales	**38,9 %**
Recepción de phishing: enlaces a sitios falsos a través de mensajes de texto, mensajería instantánea o correo electrónico, con el fin de robar información personal e información de acceso, o instalar, programas maliciosos.	**24,1 %**
Llamadas o mensajes de suplantación a través de redes sociales, mensajes de texto y telefonía celular, con el fin de estafa, robo de información personal e información de acceso.	**22,2 %**
Pinchazos (interceptación de comunicaciones, llamadas de voz y mensajes).	**20,4 %**
Robo de dispositivos (celulares, computadores, tabletas, discos duros, USB).	**18,5 %**
Pérdida de información.	**16,7 %**
Acoso a través de redes sociales, correo electrónico, llamadas o mensajes de texto.	**14,8 %**
Acoso sexual a través de redes sociales, correo electrónico, llamadas o mensajes de texto.	**13 %**
Ingreso no autorizado (hackeo) a la página web de la organización	**9.3 %**
Borrado de información en el sitio web de la organización o plataformas de terceros donde se almacena información.	**7,4 %**
Matoneo o acoso a través de redes sociales, correo electrónico, llamadas o mensajes de texto	**5,6 %**
Secuestro de información de la organización con fines extorsivos (Ransomware).	**1,9 %**
Alteración de la información en el sitio web de la organización o plataformas de terceros donde se almacena información.	**1,9 %**
Confiscación de dispositivos por autoridades (ej. Policía, Ejército, Fiscalía).	**1,9 %**
Retención de dispositivos por grupos ilegales (ej. bandas criminales, narcos).	**1,9 %**
Otros tipos de incidentes. En esta categoría, las personas citaron casos que ocurrieron, como lo fueron el encendido de cámara y grabación sin manipulación de la misma y la constante de creación de perfiles falsos.	**3,8 %**

22 Esta pregunta se enriqueció aclarando que un incidente sucede cuando la seguridad de sus servicios, infraestructura o información han sido comprometidos o vulnerados.

Al consultar a las personas defensoras si realizó alguna denuncia con respecto al incidente ocurrido, el 77,8 % dijo que no realizó denuncia en contraposición al 22,2 % que sí realizó denuncia. Las personas que manifestaron realizar la denuncia, mayormente lo hizo ante las plataformas de redes sociales (Google, Facebook, WhatsApp) (70,8 %), en segundo lugar, ante la policía (29,2 %) y, por último, ante instituciones internacionales (4,2 %). Describieron que el tipo de respuestas que recibieron por parte de las instituciones, en general estuvieron marcadas por la ausencia de resultados y por mucha burocracia. Algunas personas dijeron que la experiencia que tuvieron se limitó a que la institución recibiera la denuncia. A continuación, algunas frases ilustrativas:

- *Me contacté con META y seguí los pasos que me indicó un asistente de Facebook, pero no logramos concretar la recuperación de nuestra página de Facebook ya que el proceso se volvió muy burocrático y llevó mucho tiempo.*

- *Además del largo periodo de duración en su respuesta, fue la derivación a un grupo técnico especializado para luego más procesos burocráticos, por lo cual dejamos el report.*

- *No hice denuncia solo realicé un comunicado diciendo que mi WhatsApp ha sido hackeado y que estoy cambiando de número.*

- *Recibí el apoyo de mis amistades y algunas personas que trabajan en Radios comunitarias.*

- *No fue mi caso, fue el de colegas de otras oficinas de la red. El equipo global de informática tomó cartas en el asunto y se comunicó sobre el caso a todo el staff de Latinoamérica y el Caribe, dando recomendaciones de seguridad.*

Las personas refirieron que sus trabajos no se vieron afectados por los incidentes al 68,5 % en contraposición al 31,5 % que dijo que manifestó haber sido afectado.

También, las personas señalaron que en caso de sufrir un incidente de seguridad digital acudirían de manera inmediata a: otras organizaciones (47,7 %); a familiares (35,4 %); a instituciones (Defensoría del Pueblo, entidades de cooperación) (30 %); de manera específica a instituciones policiales (26,9 %); a la comunidad (24,6 %); no acudiría a nadie (11,5 %); a instituciones internacionales (6,9 %); y a la iglesia (1,5 %).

Se les consultó a las personas si en el último año, alguna persona de su organización o su organización ha experimentado alguna amenaza a través del correo, mensajes en redes sociales, WhatsApp, mensajes de texto y/o llamadas telefónicas por razón de sus actividades[23], al respecto el 73,1 % indicó que no y el 26,9 % manifestó que sí. Así también, se les preguntó si han estado expuestas a amenazas directas accediendo a información personal y sensible sobre ellas[24] y el 73.8 % manifestó que no y el 26.2 % señaló que sí. En referencia a este último grupo, al ser consultados si se ha visto afectado su trabajo por estas situaciones, el 80,5 % dijo que no y el 19,5 % dijo que sí.

23 Este ítem aclaró que las amenazas comprenden amenazas de índole sexual, de muerte u otros daños físicos, amenazas o intimidación a familiares cercanos, etc.

24 Este ítem aclaró que información personal y sensible incluye datos de contacto, ubicación, información sobre amenazas o procesos legales en curso, información de intereses políticos, etc.

Las personas dieron referencias sobre cómo se podría mejorar la seguridad y también la observación sobre prácticas peligrosas que podrían poner en riesgo la seguridad de la organización. Dijeron que acostumbran activar el "Modo Avión" cuando inician alguna reunión para tratar información sensible mientras que, mayormente indicaron que necesitan capacitaciones sobre el tema de seguridad digital, porque por desconocimiento a veces ignoran la identificación de un hecho peligroso porque no saben reconocer la amenaza o riesgo. Mencionaron que existe una necesidad de generar protocolos de seguridad digital, así como campañas para que la comunicación sea libre y no vigilada.

Las personas consultadas identificaron riesgos para los defensores, defensoras y las organizaciones, mencionaron que uno de los mayores riesgos que tienen es la pérdida de información, la falta de backup, como evitar ataques tipo phishing, conocer cómo lidiar con perfiles falsos, y cuidar a defensores y defensoras en atención a su nivel de exposición.

Algunas personas explicitaron ciertas situaciones:

- *Una persona de la organización que maneja las redes sociales de la organización, viajó a Europa para una actividad y no contaba con información de seguridad digital, lo que hizo que no identifique situaciones de riesgos en la utilización de cualquier wifi público y la conexión a cargas USB de aeropuertos, lo que derivó en el hackeo de nuestras redes a través de un virus.*

- *He notado al momento de las movilizaciones por el Arancel 0 y ley HC que compañeros y compañeras, y familiares recibieron amenazas desde la institución pública (universidad) de la cual soy estudiante.*

- *Mi error es utilizar wifis libres en situaciones donde no tengo la posibilidad de tener datos.*

- *Es importante que nuestra red de DDHH organice una serie de talleres para analizar y establecer estrategias, acciones y mecanismos de seguridad digital para las y los defensores, y sus organizaciones.*

Al consultar a las personas, si quieren saber más sobre temas de seguridad de la información y la infraestructura tecnológica para poder desempeñar mejor su labor sin miedo a cometer algún error, las personas dijeron que necesitan desarrollar talleres o cursos para mejorar la seguridad personal, profesional y organizacional. Dijeron que es prioritario iniciar estas capacitaciones para prevenir situaciones antes que lamentar hechos consumados. Algunas personas describieron la necesidad señalando lo siguiente:

- *Desde la organización estudiantil sería ideal conocer a profundidad sobre las herramientas confiables para proteger nuestros datos o nuestros archivos. Así también sobre la probabilidad que hay del "hackeo" o de "pinchar" los dispositivos móviles cuando nos encontramos en contextos de lucha o de acciones de fuerza, como tomas, marchas, manifestaciones, escraches, etc.*

- *Necesitamos saber hacer más segura las cuentas y las páginas web de organizaciones.*

- *Queremos guardar de mejor manera la información personal dentro de las nubes y dispositivos, saber si hay leyes de respaldo respecto a la información que se filtra o amenazas que se reciben desde las autoridades.*

- *Que nos ayuden a entender más sobre la tecnología.*

- *Cómo podemos hacer para detectar pinchazos y protección de páginas.*

- *Capacitación para saber usar el teléfono en sí.*

- *Tips para elaborar el protocolo.*

- *Muchas veces no abrimos correos cuando se ven sospechosos o también pasó que detectamos que se intentó acceder al Gmail de la organización. Necesitamos más acompañamiento en seguridad digital".*

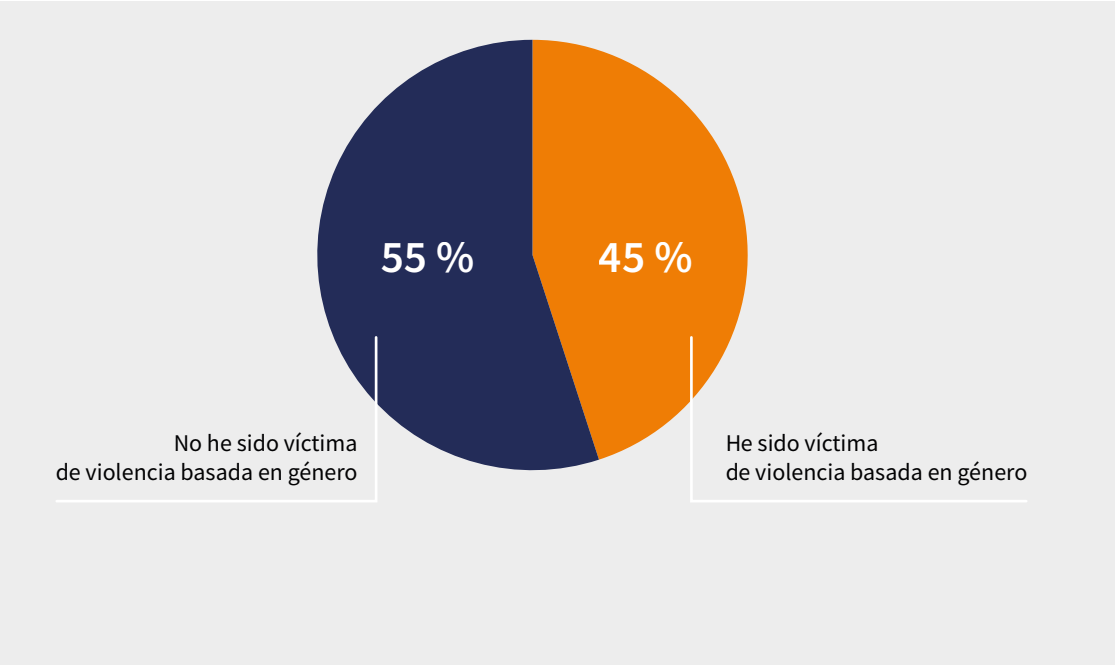
- *Queremos recibir capacitaciones especialmente en temas de seguridad digital para activistas NNA's de derechos humanos.*

- *Necesitamos comprender mejor el cifrado y entender cómo se da el monitoreo de los dispositivos.*

F. VIOLENCIA DE GÉNERO

El 45.4 % de las personas encuestadas manifestó que sí ha sido víctima de alguna forma de violencia de género y el 54,6 % dijo que no. De manera específica, 40 % dijo que ha sido víctima de alguna forma de violencia de género a través de medios digitales, mientras que 60 % indicó que no.

GRÁFICO 4. Casos de violencia basada en género contra defensoras de DDHH en Paraguay.



Al ser consultadas las personas sobre la forma de violencia de género facilitada por la tecnología de la que ha sido víctima, las mismas refirieron las siguientes opciones:

Ciberacoso.	21,6 %
Discriminación (Trato desfavorable o perjudicial dado a una persona, por motivos arbitrarios en razón de su género, sexo u orientación sexual).	21,6 %
Acoso sexual a través de redes sociales, correo electrónico, llamadas o mensajes de texto por motivos arbitrarios en razón de su género, sexo u orientación sexual).	15,7 %
Ofensa sexual (expresiones verbales, no verbales y escritas).	13,7 %
Divulgación de información personal como: dirección, número de teléfono, redes sociales, dirección de trabajo, entre otras (doxxing) por motivos arbitrarios en razón de su género u orientación sexual.	9,8 %
Matoneo o acoso a través de redes sociales, correo electrónico, llamadas o mensajes de texto por motivos arbitrarios en razón de su género, sexo u orientación sexual).	5,9 %
Suplantación de identidad en línea.	3,9 %
Divulgación no consentida de imágenes íntimas.	3,9 %
Sextorsión (Chantaje o extorsión con una imagen o video de la persona desnuda o realizando actos sexuales).	2 %
Otra forma de violencia digital de género.	2 %

De manera específica, al ser consultadas las personas sobre otras formas de violencia de género facilitada por la tecnología que ha recibido, las mismas dijeron haber recibido: amenazas de muerte; un trato de inferioridad por ser mujer y ofensas en redes. Según refirieron, los ataques por la orientación sexual y la divulgación de información sensible son situaciones comunes.

Al consultar a las personas defensoras sobre las acciones necesarias para disminuir las violencias de género dentro de los espacios virtuales, las mismas dijeron que: se necesita reglamentar el tema de seguridad digital con un enfoque que luche contra la discriminación y el racismo, contar con un Estado presente, generar políticas públicas de protección de datos, promover espacios de formación y capacitación sobre temas digitales para conocer y practicar mecanismos de cuidado personal y organizacional; exigir a las plataformas de redes sociales que fortalezcan sus mecanismos de seguridad para su usufructo. Plantean pensar qué se puede hacer con el tema de perfiles falsos, pues es una preocupación, ya que el mayor grado de acoso proviene de este tipo de cuentas. Consideran que se necesita realizar una sensibilización con la policía y el poder judicial para que entiendan la exposición en la que se encuentran defensores y defensoras de derechos humanos ante tanto discurso de odio y situaciones de acoso, entre otros tipos de violencia. A continuación, se detallan alguno de los aportes que defensores y defensoras señalaron:

- *Se necesita educación en seguridad digital y no publicar información que pueda utilizarse y volverse nuestro contrario. Creo que los niveles de exposición a los que estamos llegando es alto y estamos regalando nuestra información es excesivo y deberíamos poner límites nosotrxs mismxs.*

- *La verdad que debería ser sancionada la violencia, creo que la impunidad fomentada por las falsas identidades son caldo de cultivo para los violentos. Por otro lado, estructuralmente es necesario educar.*

- *Se necesita sacar a la luz hechos de violencia y sancionar en lo formal e informal, sobre la igualdad de derechos y de género.*

HALLAZGOS CUALITATIVOS

CONSIDERACIONES SOBRE EL ABORDAJE CUALITATIVO

El enfoque cualitativo se basó principalmente en el empleo de las técnicas de grupos focales y entrevistas individuales semiestructuradas a partir de guía de pautas y cuestionarios[25].

Se realizaron dos (2) grupos focales con la participación de 8 personas por cada grupo. Se contó con la participación de defensores y defensoras de organizaciones que trabajan diferentes temáticas de derechos humanos (derecho a la ciudad, campesinado, LGTBIQ+, Educación, ambiente, entre otros). Así también se realizaron tres (3) entrevistas en profundidad con informantes clave por su trayectoria en los ámbitos de actuación de ciberseguridad y/o derechos humanos.

La dinámica del enfoque cualitativo posibilitó que los participantes elaboren libremente relatos a partir de preguntas y situaciones propuestas por la entrevistadora, produciendo un marco de referencia que permitió indagar sobre los consensos y disrupciones durante las conversaciones.

Los resultados se presentan a partir de temáticas con hallazgos generales y particulares teniendo en cuenta los grupos de edad, actores y zonas territoriales de actuación. Las frases y verbalizaciones que ilustran los hallazgos de los grupos y entrevistas se ajustan al principio de anonimidad.

Perfiles de casos entrevistados

	Código	Perfil	Características
GRUPOS FOCALES	G1DJ	Defensores de DDHH Jóvenes De 18 -30	8 participantes: 4 mujeres 4 hombres Defensores de organizaciones de mujeres, jóvenes,LGTBIQ+, ambiente.
	G2DA	Defensores de DDHH Adultos De 34 -55 años	8 participantes: 4 mujeres 4 hombres Defensores de organizaciones de campesinado, educación, cultura, ambiente
ENTREVISTAS	E1	Defensor de DDHH	Defensor que trabaja temáticas de derechos NNA Más de 5 años de experiencia en el ámbito de DDHH
	E2	Defensora DDHH	Defensora de derechos del campesinado Más de 5 años de experiencia en el ámbito de DDHH
	E3	Defensor de DDHH	Director de organización de DDHH. Más de 5 años de experiencia en el ámbito de DDHH

25 Las guías fueron elaboradas por la Fundación Karisma y en Paraguay fueron adaptadas y ajustadas para su aplicación.

PRINCIPALES HALLAZGOS

1. Campos de actuación de los defensores de Derechos Humanos

Los defensores y las defensoras de Derechos Humanos distinguen sus espacios de actuación como institucional y desde la ciudadanía y a escala nacional y local. A nivel institucional participan en discusiones sobre marcos regulatorios, mesas de trabajo con el poder ejecutivo, audiencias públicas y lobby con el legislativo y acompañando la defensa de casos en los estrados judiciales. Por otro lado, en los espacios de redes de ciudadanía, desarrollan proyectos, talleres, agendas de participación ciudadana y promoción de los DDHH. Cabe mencionar, que la mayoría de las personas entrevistadas coinciden en que, en los últimos años, en ambos espacios hubo retrocesos, ya que se observa un ascenso de grupos que atacan los derechos humanos fundamentales, sobre todo los derechos de grupos como las mujeres, y las personas LGTBIQ+.

Estos grupos anti-derechos cuentan con gran capacidad de difusión y recursos para desinformar y ser visibles a través de redes y plataformas digitales.

- *M: Llevo trabajando hace más de dos décadas, en reuniones técnicas con representantes del Ministerio de Salud y Educación, y es impresionante como las propias directoras tienen miedo, para hablar de derechos de mujeres o LGTBIQ+, y la palabra género, ya está proscripta.*

- *H: Es así como ella dice, esto se debe a que los grupos anti-derechos, lograron entrar, desinformar, manipular, inventar historias, que dan miedo y siembra el odio en las propias comunidades". (G2DA Defensores de DDHH Adultos, 30 a 55 años).*

- *H: Muchos para no mencionar la homosexualidad en reuniones formales dicen tendencia de género a veces se dan silencios por el temor… cuando hay personas con ciertos cargos y que ejercen poder… mucha gente no quiere hablar u opinar por eso (E1- Defensor Derechos de NNA).*

2. Dinámicas de utilización de herramientas digitales e internet.

El uso de herramientas digitales es una práctica cotidiana dada para las y los defensores de derechos humanos. Consideran que dicho uso se potenció y normalizó durante la pandemia. La incorporación de dichas herramientas en las dinámicas de las organizaciones y colectivos sociales fue muy repentina, sin posibilidad de reflexionar sobre sus alcances o riesgos.

- *M: Fue como una vorágine, no dio tiempo de pensar, qué usamos, cuáles son los riesgos, era tener que usar para el trabajo, para realizar las reuniones, el meet, zoom, grupos de WhatsApp, es como algo que vino a quedarse, y aprendimos su uso básico, pero no tenemos un conocimiento real de lo que implica, es aprender cómo usar y hasta ahí"(G2DA Defensores de DDHH Adultos, 30 a 55 años).*

La mayoría de las personas consultadas valora la importancia de las herramientas digitales, para acceder a información, mantener vínculos, apertura de nuevas posibilidades de formación, y sobre todo el intercambio de experiencias con grupos y colectivos diversos. En ese sentido, jóvenes defensores expresaron que su interés por el activismo en DDHH, se originó a partir de espacios virtuales y grupos en línea.

- *H: primero seguí como un programa de la organización (XXX), que tenía un influencer, y comencé a interesarme por el tema de la deforestación, y luego hicieron como un conversatorio virtual, y posteriormente pasé a un grupo de Telegram… Después se hizo un campamento y ahora, mira soy ya voluntario del proyecto (XXX). Pienso, que para los jóvenes es una manera buena de llegar, a través de las redes sociales, sobre todo para crear interés, difícil que vaya a una reunión de una… Es como que vas conociendo de a poco la temática, la organización (G1DJ Defensores de DDHH, Jóvenes, de 18 -30).*

- *M: En mi caso también yo vi una publicación de Instagram, sobre una actividad de la comunidad de LGTBIQ+, escribí y comencé a seguir… Concuerdo con lo que él dice, no es todo para levante (risas)… Te podés informar, ver que hay personas que tienen los mismos intereses, la importancia de los derechos, y sobre todo de discutir y participar, más aún cuando los haters están full (G1DJ Defensores de DDHH, Jóvenes, de 18 -30).*

- *Algunas organizaciones campesinas que cuentan con acceso a internet y herramientas digitales lograron readaptar estrategias para la comercialización de sus productos, o bien realizaron articulaciones con otras organizaciones para crear nuevos circuitos de ventas en línea.*

- *H: A partir de un proyecto, logramos ofertar en una página y en grupos de WhatsApp los productos, y creo que eso fue muy importante para tener otra posibilidad de comercializar los productos G2DA Defensores de DDHH Adultos, 30 a 55 años).*

3. Ciberseguridad

La mayoría de las personas entrevistadas coinciden en que la ciberseguridad es un tema aún desconocido y lejano, en el sentido de incorporarla dentro de la cultura organizacional. Es decir, no está incorporado de manera consciente como parte de las prácticas de cuidado, protección y seguridad de las organizaciones. Al respecto consideran, que la necesidad de dicho abordaje emerge ante determinadas coyunturas políticas o ante eventos dándose respuestas reactivas. Un mayor cuidado o percepción de los riesgos de la violencia digital es más sentida en términos personales. En ese sentido coinciden en dimensionar la exposición y vulneración actual de defensores y la tensión que genera sostener públicamente posicionamientos, declaraciones o actos.

- *H: Yo creo que no somos conscientes de todo lo que significa el mundo digital… sobre todo para los que no somos nativos digitales… No somos conscientes de la serie de "aceptos" que damos para usar aplicaciones o lo que sea… (E1- Defensor Derechos de NNA).*

- *M: Por ejemplo, cuando se discutía la famosa donación de la comunidad europea y transformación educativa nos dimos cuenta lo vulnerables que éramos en términos de comunicación, protección de nuestras cuentas, y datos. La campaña en contra fue feroz… lleno de ataques de discursos de odio, y viralización de fake, con nuestros logos con información falsa (E2- Defensor Derechos de NNA).*

- *H: Famoso antes de la marcha, ya sabemos que tenemos que super cuidar nuestros celulares y más los de la organización, y también de los principales voceros (G1DJ Defensores de DDHH, Jóvenes, de 18 -30).*

- *M: La campaña anti-derechos fue muy sucia… hacían flayers y nos trataban de dibujar con burla a todas nuestras identidades… para nosotros no es una ofensa lo que decían, pero era una burla a tu identidad ideológica, de género, a todas tus identidades. Esto vivimos cuando se trataron temas como Transformación Educativa, UNA No Te Calles, Plan de Niñez… (E1- Defensor Derechos de NNA).*

- *M: Cuando hicimos un seminario por la plataforma zoom, con enlaces abiertos sin previa inscripciones entraron a hackear las charlas, pasando videos porno o dibujando en la pantalla… A partir de lo ocurrido tomamos medidas de protección y hacíamos inscripciones previas (G2DA Defensores de DDHH Adultos, 30 a 55 años).*

- *H: Lo complicado es cuando se realizan colectas solidarias, y entran estafadores utilizando o clonando las redes, a partir de eso buscamos mecanismos para garantizar la información y transparencia (G2DA Defensores de DDHH Adultos, 30 a 55 años).*

Una de las debilidades señaladas por defensores es la delegación de los cuidados y protección en términos de ciberseguridad de las organizaciones a los encargados de comunicación, como un tema aislado, casi como una cuestión técnica a ser abordada de manera específica. También, la multi-asignación de tareas, hace que sea descuidada la ciberseguridad de las organizaciones.

- *M: En la mayoría de las organizaciones, nosotras mismas somos todo… CM, vocera, logística, encargada de tecnología… hacemos todo (G1DJ Defensores de DDHH, Jóvenes, de 18 -30).*

- *H: La verdad que de todo el tema de redes sociales y nuestra página web, el encargado es el de comunicación… los demás no sabemos mucho del tema de cuidados digitales G2DA Defensores de DDHH Adultos, 30 a 55 años).*

4. Repertorios de Violencia

Participantes de grupos y de entrevistas coinciden en caracterizar a la violencia digital en las redes sociales como la más frecuente, en ascenso y es la que afecta psicológicamente a referentes y activistas de DDHH. Expresan preocupación ante el hecho de que dicha situación en la actualidad está normalizada. Consideran que existe una percepción tácita, de que “uno debe estar preparado a soportar o adaptarse dicha violencia”.

- *M: La violencia es las redes sociales, es día a día y más cuando se instalan agendas, que a veces son más cortinas de humo del gobierno… Pero genera conversación, es impresionante el odio, la agresión, pero lo más terrible es que como ya se está normalizando, y te dicen y bueno estás en temas de derechos, tenemos que saber que es así, tipo hay que aguantar y eso no me parece. Algo hay que hacer al respecto (G2DA Defensores de DDHH Adultos, 30 a 55 años).*

- *M: En cuanto a los ataques difamatorios, han sido ataques más amplios… eso les ha pasado a todos los directores de la organización (XXX), ataques que se daban desde periodistas incluso… estos ataques la reciben todas las organizaciones. La identificación de situaciones de ataques se da sobre todo cuando los debates están más candentes… tipo lo de transformación educativa (E3 director de organización de DDHH).*

- *H: Yo me siento seguro cuando no me atacan… cuando no te discriminan cuando te hacen comentarios, porque quieras o no te va trabajando y afectando la autoestima (G1DJ Defensores de DDHH, Jóvenes, de 18 -30).*

- *M: Antes me importaba los comentarios agresivos y negativos… tipo decía porque la gente es mala conmigo si yo soy buena… pero ahora ya no me importa… siempre hay hate en las redes… y siempre se repiten los argumentos… (G1DJ Defensores de DDHH, Jóvenes, de 18 -30).*

- *M: La violencia es directa en comentarios… cada vez que sale una noticia sobre mi salen los transfóbicos… salen y dicen que me tengo que ir al urólogo y esas cosas… para mi es agresivo… Antes respondía los comentarios… pero después deje de responder… entra gente y te desea la muerte y ni siquiera sabe que hago, a qué me dedico (G1DJ Defensores de DDHH, Jóvenes, de 18 -30).*

Los defensores perciben un aumento de la violencia en los grupos de WhatsApp abiertos y específicos, debido a la facilidad con la que circulan contenidos con informaciones falsas. Esto genera la toma de posiciones exaltadas que pueden derivar en violencia offline, especialmente cuando son grupos con participantes conocidos o cercanos en términos territoriales.

- *H: Los grupos de familia, o vecinos son los más densos, de verdad yo temo más que de ahí surja o se agite una situación y que luego quieran agredirme ya físicamente (G1DJ Defensores de DDHH, Jóvenes, de 18 -30).*

- *H: En grupos grandes de WhatsApp hay gente infiltrada… que está en los grupos por las causas en términos amplios…. Pero hay de todo ahí… esa gente se burla de los argumentos de defensores… esa gente trae información falsa al grupo (E1- Defensor Derechos de NNA).*

- *M: Son argumentos manipuladores… cada día te tirotean más… y la gente en los grupos ve y cree cualquier cosa, cuando te das cuenta de que es un video mentiroso, pero cuando querés responder, ya están todos ahí ofendidos, y después "Ekyhyje chugui kuera eikoro pe callere… porque ha´ekuera oimoa nde ha´eha abortera, pe´a que amoa"[26] (G1DJ Defensores de DDHH, Jóvenes, de 18 -30).*

- *H: Una situación que me sorprendió es que estábamos organizando un encuentro super importante por un caso que estábamos manejando… y quedamos en vernos en un lugar… y de repente aparecen muchos policías casualmente en el lugar donde nos teníamos que reunir con las personas afectadas por el avasallamiento de sus derechos (E1- Defensor Derechos de NNA).*

5. Amenazas: Percepción de Riesgos

El principal riesgo percibido hace referencia a las cuentas de redes sociales públicas y a las plataformas de articulación en línea de las organizaciones. Estas pueden ser objeto de ataques, uso indebido de la identidad colectiva, objeto de comentarios agresivos masivos e incluso hackeadas para darlas de baja en momentos de debate público.

- *H: Es como que ahora todos somos sospechosos por pertenecer a la sociedad civil, por hablar de derechos de la niñez, derechos de las personas con discapacidad… se valen con atacar a dos tipos de perfiles: -el de la organización en sí y -el de les defensores (E1- Defensor Derechos de NNA).*

26 Traducción del guaraní al español: tenes miedo de ellos cuando andas por las calles porque ellos creen que sos abortera, esto que lo otro.

- *M: Recibir amenazas… de donde sacaron eso solemos preguntarnos… quien le dijo… te amenazan cuando exponen tu identidad… el rostro del defensor, utilizan el logo de la organización, el nombre… todo… los ataques mayormente se dan desde lugares anónimos… (G1DJ Defensores de DDHH, Jóvenes, de 18 -30).*

- *H: Como organización nosotros recibimos varios ataques a nuestros servidores… llegó el momento y tuvimos que cambiar el servidor que habíamos contratado por otro más seguro… y en los últimos tres meses, recibimos un ataque de un programa maligno y un ataque para tratar de entrar en nuestros correos… Eso nos pasa a nosotros y también a otras organizaciones. E3 director de organización de DDHH).*

Resulta significativo, que las organizaciones que se encuentran el interior del país, en zonas rurales utilicen la ampliación WhatsApp, como principal vía de comunicación y de tramitación de documentaciones. Según lo expresado por un referente de DDHH, esto genera mayor riesgo y vulneración para las organizaciones.

- *H: El abordaje de esto en el campo y en la ciudad es diferente. En el campo no es tan extendido el uso de la herramienta de internet en general. Te doy un ejemplo, se tiene una computadora de escritorio y la información se guarda ahí… no utilizan nube o ese tipo de herramientas. En los teléfonos celulares sólo se usa WhatsApp en lugar del mail, toda la información se pasa por ahí… en cuanto a redes mayormente se usa solo Facebook y no otra red… (E3 director de organización de DDHH).*

Se observa un mayor cuidado o protección de las cuentas públicas y privadas personales de las personas referentes de DDHH. Lo significativo es que dicho cuidado implica un retiro momentáneo y cese de las publicaciones en las redes sociales o en algunos casos la moderación en la posición política.

- *H: Asumí que mis redes sociales se fueron volviendo menos político… yo siento que existe un ataque fuerte cuando tenemos que suavizar nuestros perfiles para poder tener paz… tiene que ver con la salud mental… como yo quiero tener paz tengo que suavizar mi perfil (E1- Defensor Derechos de NNA).*

Otro riesgo percibido se relaciona con la vulneración de la identidad digital y la falta de ley de protección de dato en el país.

- *H: Ahora para pedir información pública te piden introducir tu identidad digital y ahí hacen el une con flecha… te expones totalmente… este tema afecta a seguridad y protección laboral (E1- Defensor Derechos de NNA).*

Un hecho considerado grave y que ilustra la situación en la que se encuentran las organizaciones de la sociedad civil, fue la utilización sin consentimiento de la grabación de una reunión vía plataforma zoom de representantes de las OSC como “prueba/acusación” por parte de un senador de la República, para sostener su posición en el marco del tratamiento de la Ley “Que establece el control, la transparencia y la rendición de cuentas de las organizaciones sin fines de lucro”.

- *H: No tenemos casos específicos de espionaje… pero tenemos sospechas… por ejemplo esto de la filtración de la reunión cerrada que tuvimos sobre la Ley de la ONG y que se mostró en plena sesión del Senado, es algo muy llamativo… no sé cómo llamarlo… filtración, espionaje… pero es muy grave (E3 director de la Coordinadora de Derechos Humanos del Paraguay).*

6. Estrategia de Seguridad

En cuanto a las estrategias de seguridad, la mayoría de las personas entrevistadas aluden a medidas o estrategias que emplean en el uso particular de herramientas digitales: como son la de verificación de pasos y seguridad de contraseñas de las cuentas, cambio en el tono de las publicaciones y bloqueo de cuentas de agresores.

- *H: El anonimato vuelve a ser una herramienta porque hay una persecución y un cercenamiento fuerte… pongo mis redes en perfil privado… trato de que se vea como más joda mi perfil… que no se vea tan político… hay que hacer los dobles factores de autenticación, todo eso (E1- Defensor Derechos de NNA).*

- *M: Yo agarro y bloqueó directamente a las personas hater… Twitter es lo más agresivo… es como la cloaca de todo lo que pasa… Utilizo huella, contraseña… todo… no sé si uso WhatsApp con dos pasos (G1DJ Defensores de DDHH, Jóvenes, de 18 -30).*

Entre las medidas en términos organizacionales señalan, el llamado, a modo de campaña para bloquear cuentas y no dar visibilidad a quienes promueven el odio e iniciar la utilización de software libre.

- *M: Entonces ahí empezamos a pedir que las personas denuncien y se le pueda dar de baja a esos perfiles… Algunas cosas buenas de las plataformas es que vos podés bloquear ciertas palabras… eso creo que suma a parte de los bloqueos para identificar el hate desde el lenguaje (G1DJ Defensores de DDHH, Jóvenes, de 18 -30).*

- *H: Nosotros empezamos a adoptar algunas medidas, por ejemplo, ahora ya estamos empezando a usar LINUX, mensajerías usando otras que no son las convencionales… información que tenemos en la nube estamos buscando otras maneras de protegerlas mejor (director de organización de DDHH).*

7. Recomendaciones de las personas defensoras de DDHH.

En cuanto a ciberseguridad y organizaciones de los DDHH, las personas defensoras recomiendan:

1. Contar con un protocolo para atender y saber que hacer frente ante casos de ataques cibernéticos.
2. Buscar formatos creativos, sencillos y accesibles para difundir derechos digitales (podcast, utilizar imágenes sencillas, campañas, entre otros).
3. Establecer un programa o agenda con las redes de organizaciones para visibilizar la violencia digital.
4. Articular entre las organizaciones un sistema de cuidado y protección en materia de ciberseguridad.

CONCLUSIÓN

La investigación realizada sobre ciberseguridad en defensores y defensoras de derechos humanos en Paraguay es una contribución importante para conocer las prácticas, el uso tecnológico, los riesgos y amenazas relacionadas al campo de la seguridad digital. Uno de los aportes del estudio es el mapeo actualizado de organizaciones y de personas defensoras para trazar la línea de base en materia de seguridad digital y esto a su vez posibilitará el seguimiento y la realización de nuevas mediciones en el transcurso del tiempo sobre el tema.

A partir del análisis de los hallazgos cuantitativos como cualitativos, se puede dar cuenta que el nivel de ciberseguridad de las organizaciones y de las personas defensoras se caracteriza por el desconocimiento y fragmentación sobre el tema de seguridad digital. Mayormente se observa poco conocimiento sobre los riesgos o amenazas digitales, lo que les resulta difícil de dimensionar y dificulta la toma de acciones. Esta falta de formación, combinada con una dependencia creciente de las tecnologías digitales, refuerza la percepción de que la ciberseguridad es algo inalcanzable para muchas personas sin conocimientos técnicos.

Es relevante destacar que la noción de bienestar en temas de seguridad digital y autocuidado digital está profundamente influenciada por conceptos colonizados que imponen una carga individual sobre cada persona para protegerse. En contextos de desigualdad, como el que enfrentan los defensores y defensoras en Paraguay, esta visión individualizada no es adecuada. Como resultado, la seguridad digital es vista como un privilegio, lo que genera frustración y culpa en aquellas personas que no logran cumplir con las expectativas impuestas de autocuidado.

El CIRT-PY registra las estadísticas de los últimos incidentes cibernéticos reportados en el país, especialmente, los que ocurrieron en las dependencias estatales, pero también informa sobre denuncias recibidas por parte del sector privado y por la ciudadanía. Las vulnerabilidades identificadas coinciden con lo señalado por defensores de DDHH, estos son contraseñas débiles, desactualizaciones y *malwares*.

La mayoría de las personas defensoras participantes de la investigación residen y se movilizan en áreas urbanas y valoran positivamente el acceso y uso de la tecnología (sienten que la misma no las atropella). Sin embargo, este acceso no siempre va acompañado del conocimiento necesario para mantener una seguridad efectiva. En cuanto al uso de tecnologías digitales, la mayoría (63 %) lo hace de manera autónoma, pero hay un número importante que recurre a familiares y amigos para poder utilizarla. Éste hecho, encuentra su correlato con los aportes cualitativos, que refieren que con la pandemia tuvieron que aprender “sobre la marcha” y, por lo tanto, no pudieron conocer a profundidad los riesgos implicados ni tomar decisiones informadas sobre su seguridad digital.

La principal mensajería instantánea que se utiliza es WhatsApp (100 %), seguida por Facebook Messenger (41 %), y posteriormente Telegram (42 %). A pesar del uso extendido de estas herramientas, los resultados muestran un elevado porcentaje de personas que nunca recibieron capacitación en seguridad digital, alcanzando el 76 %. Esto refleja que la mayoría de los defensores de DDHH no cuentan con la formación adecuada para identificar riesgos, amenazas o dar un uso seguro a la tecnología. Las personas defensoras indicaron que, por lo general, no realizan análisis de riesgos en seguridad digital (91 %) y utilizan la misma contraseña para todas sus cuentas (56 %). Además, el 94 % de las personas indicó que su organización no cuenta con protocolos en esta área, lo que agrava la situación de vulnerabilidad.

Se pudo observar en los hallazgos cualitativos como cuantitativos que las cuestiones que atañen a lo digital recaen principalmente en el equipo de comunicación o de informática. Mientras que en organizaciones pequeñas se da una multi-asignación de tareas o roles en las mismas personas.

En este contexto, se vuelve crucial entender que las respuestas a la seguridad de las personas que defienden los derechos humanos en Paraguay deben tener una mirada colectiva. Solo se podrá alcanzar un bienestar integral (incluyendo el digital) si se logra cambiar la estructura para que todas las personas puedan disfrutar de condiciones equitativas. La transformación cultural y relacional es fundamental para construir un entorno en el que la seguridad digital sea accesible para todas las personas. Si bien esto no implica que la solución sea únicamente colectiva, tampoco debe olvidarse que el autocuidado sigue siendo esencial.

Los tipos de amenazas digitales más comunes por lo general tienen que ver, en su mayoría, con 1. Ingreso no autorizado (hackeo) al correo o cuentas en redes sociales; 2. Recepción de *phishing*: enlaces a sitios falsos a través de mensajes de texto, mensajería instantánea o correo electrónico, con el fin de robar información personal e información de acceso, o instalar, programas maliciosos; 3. Pérdida de información; 4. Acoso sexual a través de redes sociales, correo electrónico, llamadas o mensajes de texto; 5. Robo de dispositivos (celulares, computadores, tabletas, discos duros, USB). En los últimos años ocurrieron mayormente las dos primeras categorías.

El 45% de las personas encuestadas manifestó que sí ha sido víctima de alguna forma de violencia de género facilitada por la tecnología y de ese número de manera específica, 40 % dijo que ha sido víctima a través de medios digitales. Las personas mencionaron que los tipos de violencia más comunes de las que han sido víctimas fueron ciberacoso, discriminación y acoso sexual en redes sociales, por correos electrónicos, llamadas, mensajes de textos por motivos arbitrarios en razón de su género, sexo u orientación sexual. Algunas personas incluso mencionaron amenazas de muerte y ofensas por el hecho de ser mujeres, lo que subraya la gravedad de los riesgos a los que se enfrentan.

Además, las personas defensoras perciben hechos que atentan contra su privacidad y derechos, y muchas se sienten vigiladas o monitoreadas. Algunas personas relataron que son escuchadas a través de sus teléfonos, y sospechan que son hechos de espionaje y robo de información. Este contexto refuerza la importancia de no sobrecargar a los individuos con la responsabilidad de su propia seguridad, sino de avanzar hacia soluciones colectivas y estructurales.

Según la encuesta, el 78 % de las personas que recibieron ataques o amenazas no realizaron denuncias y las que lo hicieron mencionaron haberlo hecho ante las plataformas, la policía o la defensoría del pueblo. En todos los casos, mencionaron que realizar las denuncias resulta muy burocrático y por lo general se reduce a dejar constancia de los hechos.

Finalmente, los mecanismos de seguridad que adoptan las personas, frecuentemente son instintivos, pues, la mayoría refirió no haber recibido capacitación alguna, y para cuidarse, optan por colocar el dispositivo en “modo avión”, “apagar el teléfono” durante las reuniones y “suavizar su perfil en redes sociales”

En conclusión, la investigación revela que la noción de bienestar en seguridad digital, tal como la conocemos, está profundamente colonizada, colocando la responsabilidad de protección sobre las personas en lugar de abordar las desigualdades estructurales que perpetúan las vulnerabilidades. En este contexto, la seguridad digital de las personas defensoras de derechos humanos es percibida como un privilegio, lo que genera frustración y sentimientos de culpa al no poder cumplir con expectativas inalcanzables. Es fundamental comprender que las respuestas a la seguridad, en particular para quienes defienden derechos humanos en Paraguay, deben adoptar una mirada colectiva. Solo un cambio estructural profundo permitirá alcanzar un bienestar integral, incluido el digital, que sea accesible para todas las personas. Este proceso requiere una transformación cultural y relacional que posibilite la construcción de un entorno más equitativo. Si bien el autocuidado sigue siendo importante, esta investigación subraya que la solución no es meramente individual, sino que debe ser parte de una estrategia colaborativa y compartida que permita a todas las personas protegerse y prosperar en un entorno digital más justo.para evitar ser blanco de ataques.

RECOMENDACIONES

A partir de los datos hallados en el campo cualitativo, cuantitativo y el cruzamiento con las fuentes secundarias, se recomiendan los siguientes puntos:

- Trabajar de manera prioritaria en la sensibilización y capacitación sobre temas digitales con las personas y organizaciones de DDHH. Esto implica dimensionar el alcance del uso tecnológico y los cuidados que deben de adoptar para contar con seguridad y poder desarrollar las actividades de defensa de derechos.
- Elaborar herramientas sencillas para difundir los lineamientos básicos de cuidado en materia de seguridad digital.
- Articular una plataforma con las organizaciones que se ocupan de temas de DDHH para elaborar protocolos en materia de seguridad digital y dar respuestas a los distintos tipos de ataques cibernéticos.
- Establecer una agenda de ciberseguridad con las organizaciones para prever y visibilizar los casos de violencia digital contra defensores y organizaciones de DDHH.
- Generar mecanismos para proteger a las personas defensoras y organizaciones de DDHH de situaciones de vigilancia masiva y específica provenientes de todo tipo de sector (estatal o de grupos delictivos o criminales).
- Involucrar a organizaciones y defensores de DDHH en el proceso de construcción y aprobación de una ley de protección integral de datos personales.
- Elaborar una caja de herramientas con los lineamientos básicos y rutinarios de cuidados digitales a seguir: utilizar contraseñas seguras, cambiarlas durante cierto periodo, mantener los dispositivos actualizados, utilizar software libre, implementar doble factor de autenticación para fortalecer la seguridad de las contraseñas, cuidar la cadena de suministro, revisando los términos de uso, cuidar la información almacenada, e idealmente utilizar tecnologías de cifrado.
- Exigir a las plataformas de redes sociales que fortalezcan sus mecanismos de seguridad para su usufructo.
- Promover que las organizaciones de DDHH generen e implementen protocolos de seguridad digital.
- Generar una práctica de monitoreo a través del registro de los hechos de vulneración y violencia digital hacia defensores y organizaciones de DDHH.

BIBLIOGRAFÍA

1. Acuña, J. (10 de Octubre de 2017). Hacia una visión de seguridad digital para todos y todas. https://www.tedic.org/hacia-una-vision-de-seguridad-digital-para-todos-y-todas/. Accedido el 09 de mayo de 2024.

2. Aguilar, J. M. (Abril de 2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Instituto de Estudios Internacionales–Universidad de Chile. Vol.53 № .198 , págs. 169-197. Obtenido de Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-37692021000100169. Accedido el 13 de mayo de 2024.

3. Bewlay, L., Kilbey, H. y Paes, B. (28 de octubre de 2021). Construcción de herramientas digitales en organizaciones de justicia social: Qué considerar antes de empezar. https://www.theengineroom.org/library/building-digital-tools-in-social-justice-organisations-what-to-consider-before-getting-started/. Accedido el 18 de julio de 2024.

4. Carrillo, E., Sequera, M. Fulchi, L. (2018). La enajenación contínua de nuestros derechos. Sistemas de identidad: biometría y cámaras de vigilancia no regulada. https://www.tedic.org/wp-content/uploads/2018/07/La-enajenaci %C3 %B3n-continua-de-nuestros-derechos_TEDIC_2018.pdf. Accedido el 18 de junio de 2024.

5. Carrillo, E., Bogado, A. y Kostic, B. (2024). Perpetradores de violencia de género en línea. Hoja de ruta para investigaciones. https://www.tedic.org/wp-content/uploads/2024/07/Perpetradores-de-violencia-de-genero-online-1.pdf. Accedido el 10 de julio de 2024.

6. Centro de respuestas ante incidentes cibernéticos. (2024). Ministerio de Tecnologías de la Información y Comunicación: https://www.cert.gov.py. Accedido el 02 de mayo de 2024.

7. CERT-PY. (2020). Estado de la ciberseguridad en Paraguay. Año 2020. Asunción: Ministerio de Tecnologías de la Información y Comunicación. https://www.cert.gov.py/wp-content/uploads/2022/02/Informe_Ciberseguridad_Paraguay_2020_-_final-2.pdf

8. Informe: Estado de la ciberseguridad en el Paraguay. Año 2022. Asunción: CERT-PY/MITIC. https://www.cert.gov.py/wp-content/uploads/2024/01/Informe-Ciberseguridad-Paraguay-2022.pdf. Accedido el 10 de mayo de 2024.

9. Diario ABC Color. (11 de noviembre de 2023). Paraguay firma con EEUU acuerdo de ciberseguridad. www.abc.com.py/politica/2023/11/11/paraguay-firma-con-eeuu-acuerdo-de-ciberseguridad/. Accedido el 26 de mayo de 2024.

10. Diario La Nación. (06 de julio de 2023). Destacan hito en ciberseguridad paraguaya tras acuerdo de cooperación con EE. UU. www.lanacion.com.py/politica/2023/07/06/destacan-hito-en-ciberseguridad-paraguaya-tras-acuerdo-de-cooperacion-con-ee-uu/. Accedido el 13 de junio de 2024.

11. Diario Última Hora. (6 de Enero de 2024). Obtenido de MITIC no desconoce incidente de ciberseguridad de telefonía: www.ultimahora.com/mitic-no-desconoce-incidente-de-ciberseguridad-de-telefonia. Accedido el 09 de mayo de 2024.

12. Fundación Karisma. (2024). Consideraciones para un plan de respuestas a incidentes de ciberseguridad. Obtenido de Bogotá: https://web.karisma.org.co/consideraciones-parael-diseno-de-un-plan-derespuesta-a-incidentesde-ciberseguridad/. Accedido el 23 de julio de 2023.

13. Fundación Karisma. (2024). Comentarios al borrador del decreto de ciberseguridad del MinTIC. https://web.karisma.org.co/comentarios-al-borrador-del-decreto-de-ciberseguridad-del-mintic/. Accedido el 25 de julio de 2024.

14. Machín, N. y. (Octubre de 2016). Ciberseguridad como factor crítico en la seguridad de la Unión Europea. Madrid: Universidad Compluetense. Revista UNISCI. № 42. pp. 47-68: https://www.redalyc.org/pdf/767/76747805002.pdf. Accedido el 15 de mayo de 2024.

15. Martínez, E. y. (Abril de 2021). Revista digital de Ciencia, Tecnología e Innovación. ISSN 1390-9150. Vol. 8. № 2. pp. 221-234. Obtenido de Ciberseguridad en las redes sociales: una revisión teórica.

16. Ministerio Público. (2024). Unidad Especializada de Delitos Informáticos. https://ministeriopublico.gov.py/unidad-especializada-de-delitos-informaticos-. Accedido el 06 de mayo de 2024.

17. Ministerio de Tecnologías, Información y Comunicación. (06 de junio de 2024). Por qué es importante para el Paraguay actualizar su Estrategia Nacional de Ciberseguridad. https://mitic.gov.py/por-que-es-importante-para-el-paraguay-actualizar-su-estrategia-nacional-de-ciberseguridad/. Accedido el 12 de junio de 2024.

18. Naciones Unidas. (1998). La Declaración de los defensores de los derechos humanos. Resolución A/RES/53/144. Obtenido de Oficina del Alto Comisionado de los Derechos Humanos. https://www.ohchr.org/es/special-procedures/sr-human-rights-defenders/declaration-human-rights-defenders. Accedido el 08 de junio de 2024.

19. Naciones Unidas. (2011). Oficinas del Alto Comisionado de Derechos Humanos: Colombia, Guatemala y México. Comentarios sobre la declaración de defensores y defensoras de derechos humanos. https://www.corteidh.or.cr/tablas/28995.pdf. Accedido el 16 de mayo de 2024.

20. Naciones Unidas. (2024). Acerca de los defensores de los derechos humanos. Relator Especial sobre los defensores de los derechos humanos. Obtenido de Oficina del Alto Comisionado de los Derechos Humanos. https://www.ohchr.org/es/special-procedures/sr-human-rights-defenders/about-human-rights-defenders#:~:text=Los %20defensores %20act %C3 %BAan %20en %20favor,circulaci %C3 %B3n %20y %20la %20no %20discriminaci %C3 %B3n. Accedido el 13 de mayo de 2024.

21. OECD. 2016. Políticas de banda ancha para América Latina y el Caribe: Un manual para la economía digital. Gestión de riesgos de seguridad. Obtenido de: digitalhttps://read.oecd-ilibrary.org/science-and-technology/politicas-de-banda-ancha-para-america-latina-y-el-caribe/gestion-de-riesgos-de-seguridad-digital_9789264259027-17-es#page3. Accedido el 20 de junio de 2024.

22. Organización de los Estados Americanos. (8 de Junio de 2004). Resolución AG/RES. 2004 (XXXIV-O/04) “Adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y multidisciplinario para la creación de una cultura de seguridad cibernética”. Obtenido de https://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp. Accedido el 18 de mayo de 2024.

23. Oficina de los Derechos Humanos de las Naciones Unidas. (2019). Derechos a la libertad de reunión pacífica y de asociación. https://www.ohchr.org/. Accedido el 04 de junio de 2024.

24. Paes, B. (28 de junio de 2024). Un ejercicio de imaginación: el trabajo de fortalecer los ecosistemas de información. https://www.theengineroom.org/library/an-exercise-in-imagination-the-work-of-strengthening-information-ecosystems/. Accedido el 15 de julio de 2024.

25. Ramírez, A. (23 de Diciembre de 2023). Ciberdefensa como estrategia para seguridad y soberanía digital en Paraguay. Obtenido de Revista Jurídica: Investigación en Ciencias Jurídicas y Sociales. № 14.1. Págs 16-41: https://ojs.ministeriopublico.gov.py/index.php/rjmp/article/view/327. Accedido el 19 de mayo de 2024.

26. Revista Foco. (30 de Noviembre de 2018). 4 Pautas para proteger la seguridad digital de tu emprendimiento. Obtenido de https://foco.lanacion.com.py/2018/11/30/4-pautas-para-proteger-la-seguridad-digital-de-tu-emprendimiento/. Accedido el 26 de mayo de 2024.

27. Sancho Hirare, C. (2017). Ciberseguridad. Presentación del dossier. Obtenido de URVIO, Revista Latinoamericana de Estudios de Seguridad, Núm. 20, pp. 8-15: https://www.redalyc.org/journal/5526/552656641001/html/. Accedido el 17 de mayo de 2024.

28. Sequera, M. (2022). Manifestaciones libres. Guía sobre la vigilancia policial en manifestaciones en Paraguay. https://www.tedic.org/wp-content/uploads/2022/03/Guia-Manifestaciones-libres-WEB.pdf. Accedido el 12 de junio de 2024.

29. Sequera, M. y Acuña, J. (2023). La violencia digital de género a periodistas en Paraguay. https://www.tedic.org/wp-content/uploads/2023/10/Violencia-Genero-Periodistas-TEDIC-2023-web-2.pdf. Accedido el 18 de mayo de 2024.

30. Sequera, M. y Samaniego, M. (2018). Cibercrimen: desafíos de la armonización del Convenio de Budapest en el sistema penal paraguayo. https://www.tedic.org/wp-content/uploads/2018/10/minuta_TEDIC.pdf. Accedido el 03 de junio de 2024.

31. Sequera, M., Toledo, A. y Ucciferri, L. (2018). Derechos Humanos y Seguridad Digital: una pareja perfecta. Aportes de la sociedad civil hacia políticas nacionales de seguridad digital que respeten y protejan los derechos humanos. https://www.tedic.org/wp-content/uploads/2018/12/InformeCiberseguridadParte1.pdf. Accedido el 8 de julio de 2024.

32. Sequera, M. y Rolón Luna, J. (2016). Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Paraguay. TEDIC y Electronic Frontier Foundation. https://www.tedic.org/wp-content/uploads/2018/12/Vigilancia-estatal-de-las-comunicaciones-y-derechos-fundamentales-en-Paraguay.pdf. Accedido el 05 de julio de 2024.

33. Sequera, M. (2019). El billetaje electrónico. Nuestros derechos están en juego. Obtenido de www.tedic.org/el-billetaje-electronico-nuestros-derechos-estan-en-juego

34. Sistema de Información Legislativa del Paraguay. Proyecto de Ley. #Expediente: D-2164736. https://silpy.congreso.gov.py/web/expediente/124598. Accedido el 06 de julio de 2024.

35. TEDIC. (Junio de 2016). Comentarios al Borrador del Plan Nacional de Ciberseguridad. Obtenido de https://www.tedic.org/wp-content/uploads/2016/06/observaciones-sobre-el-plan-de-ciberseguridad_v14jun-.pdf. Accedido el 01 de junio de 2024.

36. TEDIC. (8 de Marzo de 2018). Obtenido de Derechos humanos y seguridad digital: una pareja perfecta. https://www.tedic.org/derechos-humanos-y-seguridad-digital-una-pareja-perfecta/. Accedido el 13 de mayo de 2024.

37. TEDIC. (2 de Octubre de 2018). Hacia una justicia penal que hable el lenguaje de Internet. Obtenido de https://www.tedic.org/hacia-una-justicia-penal-que-hable-el-lenguaje-de-internet/. Accedido el 23 de mayo de 2024.

38. Leyes, decretos y reglamentos consultados

39. Decreto Nº 11.624/2013, “Por el cual se reglamenta la ley Nº 4989 del 9 de agosto de 2013, y crea el marco de aplicación de las Tecnologías de la Información y Comunicación en el sector público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs) y establece la estructura orgánica y funcional de la citada Secretaría Nacional”.

40. Decreto Nº 5323/2016, “Por el cual se reglamentan los Arts. 20 y 21 de la Ley Nº 4989/2013”: “Que crea el marco de aplicación de las TICs en el sector público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)”.

41. Decreto Nº 8098/2022, reglamentación de la ley 5653/2016: “De protección de niños, niñas y adolescentes contra contenidos nocivos de internet”.

42. Decreto Nº 2274/2019, reglamentación de la Ley Nº 6.207/2018: “Que crea el Ministerio de Tecnologías de la Información y Comunicación y establece su carta orgánica”.

43. Decreto Nº 6234/2016, “Por el cual se declara de interés nacional la aplicación y el uso de las tecnologías de la información y comunicación (TIC), se define la estructura mínima con la que deberá contar y se establecen otras disposiciones para su efectivo funcionamiento”.

44. Decreto Nº 7052/2017, “Por el cual se aprueba el Plan Nacional de Ciberseguridad y se integra la Comisión Nacional de Ciberseguridad”.

45. Decreto Nº 7576 /2022, reglamentación de la Ley Nº 6822/2021: “De los servicios de confianza para las transacciones electrónicas, de los documentos transmisibles electrónicos”.

46. Ley Nº 4989/2013, “Que crea el marco de aplicación de las tecnologías de la información y comunicación en el sector público y crea la Secretaría Nacional de Tecnologías, Información y Comunicación (SENATICs)”.

47. Ley № 6822/2021, “De los servicios de confianza para las transacciones electrónicas, del documento electrónico, y de los documentos transmisibles electrónicos”.

48. Ley № 5653/2016, “De protección de niños, niñas y adolescentes contra contenidos nocivos de internet”.

49. Ley № 6.207/2018, “Que crea el Ministerio de Tecnologías, Información y Comunicación y establece su carta orgánica”.

50. Resolución MITIC № 699/2019, Aprobación de los “Criterios mínimos de seguridad para el desarrollo y adquisición de Software”.

51. Resolución MITIC № 346/2020, “A través de la cual se aprueba e implementa el reglamento de reporte obligatorios de incidentes cibernéticos de seguridad por parte los Organismos y Entidades del Estado (OEE) al Ministerio de Tecnologías de la Información y Comunicación (MITIC), a través del Centro de Respuestas a Incidentes Cibernéticos (CERT-PY)”.


Tecnología
& Derechos
Humanos