PROYECTO DE LEY DE CIBERSEGURIDAD Y PROTECCIÓN DEL CIBERESPACIO PARAGUAYO

análisis legal y comentarios a la propuesta legislativa

TEDIC

PROYECTO DE LEY DE CIBERSEGURIDAD Y PROTECCIÓN DEL CIBERESPACIO PARAGUAYO

ANÁLISIS LEGAL Y COMENTARIOS A LA PROPUESTA LEGISLATIVA

TEDIC

JUNIO DE 2025

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.

La presente publicación ha sido financiada por la Unión Europea. Su contenido es responsabilidad exclusiva de TEDIC y no refleja necesariamente los puntos de vista de la Unión Europea.

Responsable del analisis legal y redacción
Maricarmen Sequera Buzarquis[1]

Junio, 2025

1 Abogada, Máster en Propiedad Intelectual por FLACSO Argentina. Especialista en Ciberseguridad por la Universidad de León y en Tecnopolítica por la Universidad de Barcelona. Fellow 2023 en el programa Global Competitiveness Leadership (GCL) Latin America and Caribbean Studies de la Universidad de Georgetown. Finalista de los Premios EQUALS in Tech 2021 y nombrada Heroína en los Premios RightsCon 2015 de Access Now. Miembro del Comité Regional de Subvenciones para América Latina y el Caribe de la Fundación Wikimedia – 2023-2025. Miembro de la red Global Future Councils del Foro Económico Mundial – 2025-2026.

TABLA DE CONTENIDOS

INTRODUCCIÓN

La creciente digitalización del país ha traído consigo nuevos desafíos de seguridad que requieren un marco normativo claro, proporcional y centrado en los derechos de las personas. En este contexto, saludamos la iniciativa legislativa que busca establecer una Ley de Ciberseguridad y Protección del Ciberespacio. No obstante, consideramos necesario que dicho marco esté sustentado en estándares internacionales, principios democráticos y una gobernanza abierta.

Este documento busca aportar una visión crítica y constructiva para fortalecer la propuesta desde una óptica técnica, jurídica y social.

El proyecto de Ley “De Ciberseguridad y Protección del Ciberespacio Paraguayo” fue presentado en la Cámara de Diputados en mayo de 2025. La iniciativa se compone de 29 artículos distribuidos en cinco títulos, que abordan aspectos como el objeto de la ley, las obligaciones institucionales, la prevención y detección de incidentes, así como la investigación y persecución de delitos relacionados, incluyendo disposiciones finales. Además esta propuesta nace a partir de las últimas filtraciones de las instituciones del Estado paraguayo. Actualmente existen 2 propuestas legislativas en el Congreso sobre este tema y un proyecto de ley.

Desde TEDIC reconocemos que este proyecto constituye un primer paso significativo para acelerar los procesos de consulta con múltiples actores y partes interesadas[2]. Su desarrollo deberá complementarse con una visión integral, que contemple tanto los derechos humanos como los aspectos técnicos y operativos del ecosistema digital.

Es importante subrayar que cualquier regulación en materia de ciberseguridad implica una alta complejidad, ya que debe integrarse armónicamente con el entramado legal existente. La nueva normativa deberá fortalecer y complementar las disposiciones vigentes relativas a la protección de los sistemas informáticos y la seguridad digital en general, asegurando coherencia jurídica y efectividad en su aplicación.

Por tanto, es fundamental que su enfoque sea compatible con parámetros internacionales sobre ciberseguridad y derechos humanos. Desde TEDIC[3] compartimos nuestros comentarios estructurales y sustantivos sobre el proyecto de ley de Ciberseguridad, así como de forma debido a la importancia del tema, gobernanza y ciberseguridad, se echa de menos un enfoque

2 Multiples parte/ multistakeholders – Metodología de la ONU: https://www.un.org/es/summit-of-the-future/stakeholders

3 Web oficial de TEDIC https://www.tedic.org/

actualizado, garantista y transparente.

Los principales inconvenientes encontrados por nuestra organización TEDIC, los cuales fueron explicado en los comentarios que enviamos al ministerio, son los siguientes:

1. LA NECESIDAD DE DISEÑAR UNA NORMATIVA O UNA POLÍTICA PÚBLICA SOBRE CIBERSEGURIDAD QUE CONTRIBUYAN A PARTIR DE PROCESOS INCLUYENTES Y TRANSPARENTES

Para diseñar una normativa de este nivel será importante crea una instancia de gobernanza sobre la ciberseguridad. Este proceso de participación de multiples partes interesadas (academia, sociedad civil, comunidad ténica, empresas y el Estado), así como la ciudadanía en general interesada en este tema puede sumarse a la formulación de una propuesta legislativa con los criterios de gobernanza en ciberseguridad. Asi mismo la ODCE (2015)[4] sugiere diseñar una gestión de riesgos de la ciberseguridad para la prosperidad económica y social. Además advierte que las políticas en este tema deberían “ser el resultado de un enfoque intergubernamental coordinado y de un proceso abierto y transparente en el que participen todas las partes interesadas.

Es indispensable que se abran espacios para que la ciudadanía participe del modelo de gobernanza de ciberseguridad y que el enfoque general de la norma prevea que la ciudadanía, y no el propio Estado, sea su principal beneficiario, pues, dada la acelerada transformación digital de nuestra sociedad, ya no hay duda de la importancia de la seguridad digital para todos los espacios de la vida social y económica de un país.

El informe de la OCDE, “Políticas de Banda Ancha para América Latina y el Caribe[5]”, en su capítulo 14 sobre gestión del riesgo digital, establece que el objetivo de una estrategia nacional o normativa sobre Ciberseguridad debe ser que todas las partes interesadas reconozcan que la gestión del riesgo digital es un desafío económico y social, no solo un asunto técnico o de seguridad nacional.

En los últimos años, la evolución de las políticas normativas nacionales, según los documentos de la OCDE, ha ampliado el enfoque, no solo protegiendo la infraestructura crítica, sino también abarcando la seguridad nacional en diversos sectores. La transformación digital ha intensificado la importancia de la seguridad digital, volviendo más complejo el panorama actual.

Así lo reconocen las recomendaciones de la OCDE más recientes (2021), que

4 OECD. Legal Instruments. Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity. Disponible en: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-041

5 OECD (2015) Políticas de banda ancha para América Latina y el Caribe https://www.oecd.org/es/publications/politicas-de-banda-ancha-para-america-latina-y-el-caribe_9789264259027-es.html

buscan “mejorar la seguridad digital de las actividades críticas”[6]. Este concepto de “actividades críticas” corresponde a los servicios esenciales mencionados en el documento, ubicándose en la intersección de varios ámbitos.

El manejo del riesgo digital debe entenderse como un desafío económico y social, no solo como un tema técnico o de seguridad nacional. En los últimos años, las políticas nacionales, como se observa en los documentos de la OCDE, han evolucionado, pasando de proteger solo las infraestructuras esenciales (críticas) a abarcar también la seguridad nacional en múltiples sectores como por ejemplo el impacto a la salud mental con el Ministerio de Salud Pública. La transformación digital ha ampliado el impacto de la seguridad digital, volviendo el panorama más complejo. La seguridad nacional es solo un aspecto de este enfoque más amplio.

El proyecto de Ciberseguridad debe definir si se trata de una política de seguridad digital centrada en la seguridad nacional o si tiene un alcance más amplio, estableciendo claramente sus límites. Aunque se destaca el papel más protagónico MITIC, la creación de un Vice Ministerio de Ciberseguridad, aún no alcanza el nivel necesario para constituirse como una política nacional de seguridad digital porque faltaría incluir más Ministerios como salud (salud mental en internet), de la mujer (violencia de género facilitada por la tecnología) del ambiente (impactos ambientales) al Tribunal Superior de Justicia Electoral (desinformación que afecta la confianza electoral[7] o ataques infraestructura crítica como maquinas de votación electrónica[8]) entre otros.

La OCDE destaca un importante desafío de coordinación entre diversas agendas políticas, como seguridad nacional, transformación digital y otros sectores clave, como salud, transporte y comunicaciones. Si bien la protección de infraestructuras críticas es clave para la seguridad nacional, no debe ser el único enfoque.

6 OECD. Bernat, L. (2021), "Enhancing the digital security of critical activities", Going Digital Toolkit Note, No. 17, https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf

7 TEDIC (2024) Reforma electoral en Paraguay https://www.tedic.org/reforma-electoral-en-paraguay/

8 La Nación (2023) Un incendio en la sede electoral de Paraguay destruyó 8500 máquinas de votación. https://www.lanacion.com.ar/el-mundo/un-incendio-en-la-sede-electoral-de-paraguay-destruyo-8500-maquinas-y-puso-en-duda-el-cronograma-de-nid29092022/

2.1) LA GOBERNANZA DE LA CIBERSEGURIDAD ESTÁ UNICAMENTE CENTRADA EN EL ESTADO A TRAVÉS DE SU CONSEJO NACIONAL DE CIBERSEGURIDAD

Si se trata de un Consejo Nacional de Ciberseguridad, la gobernanza debe priorizar la gestión del riesgo digital, definiendo claramente qué se protege, cómo se protege y cómo se coordina con los actores clave, tanto del sector privado como de la sociedad civil. Al menos, el mecanismo intergubernamental establecido en el borrador del proyecto, a todos los niveles (incluidos los operativos), debe incluir espacios de participación y colaboración con las diversas partes interesadas.

Las recomendaciones más recientes de la OCDE (2021) sobre cómo “Mejorar la seguridad digital de las actividades críticas”[9] destacan la importancia de una gobernanza eficaz, que debe garantizar la coherencia con los derechos humanos y los valores fundamentales. Según la OCDE, no existe un único enfoque para la coordinación gubernamental en los países miembros, y los marcos de gobernanza varían según las disposiciones constitucionales, el estilo de gobierno y la estructura administrativa de cada nación. Sin embargo, todos los marcos deben cumplir tres funciones clave: la definición del marco político global o estrategia, la aplicación del marco en cada sector y la capacidad operativa.

“La gobernanza puede ser centralizada en un único organismo, como la ANSSI en Francia, o distribuida entre varios actores, como en el caso del Reino Unido, donde la estrategia es desarrollada por un ministerio, pero la capacidad operativa está en manos de una agencia independiente, como el NCSC. Algunos países, como Dinamarca, requieren que cada ministerio responsable de un sector crítico desarrolle su propia subestrategia, lo que refleja un enfoque descentralizado. **Si bien los enfoques centralizados garantizan coherencia normativa, los descentralizados favorecen la aplicación específica en cada sector**, aunque requieren mayores esfuerzos para mantener la consistencia entre ellos.

Un desafío clave es garantizar que los organismos institucionales responsables cuenten con la capacidad necesaria para cumplir sus funciones, lo que incluye la financiación, recursos y experiencia en seguridad digital, un área escasa en muchos países y difícil de retener en el sector público. Por ello, puede ser más efectivo reunir experiencia en seguridad digital a través de un organismo central, dado que los retos técnicos son comunes a todos los sectores. Sin embargo, cada enfoque tiene sus pros y contras, y es fundamental encontrar un balance adecuado para lograr una gobernanza efectiva y adaptada a las realidades nacionales.”

9 OECD. Bernat, L. (2021), "Enhancing the digital security of critical activities", Going Digital Toolkit Note, No. 17, https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf

2.2 LA INCLUSIÓN DE MÁS INSTITUCIONES DEL CONCEJO DE CIBERSEGURIDAD

La gobernanza de la ciberseguridad no puede limitarse a actores técnicos o institucionales del sector digital como sugieren en el proyecto de ley en su artículo 7. Dado que los riesgos y efectos del entorno digital tienen implicaciones directas sobre la salud mental, la igualdad de género y el impacto ambiental, es fundamental incorporar de manera estructural al **Ministerio de Salud, al Ministerio de la Mujer y al Ministerio del Ambiente** en los espacios de toma de decisión y coordinación en materia de ciberseguridad.

El Ministerio de Salud debe participar activamente en el diseño e implementación de políticas públicas que aborden problemáticas como el acoso digital, la adicción tecnológica o el impacto psicológico del uso intensivo de plataformas digitales, especialmente en población joven. La salud mental vinculada al entorno digital es una dimensión crítica que exige respuestas institucionales intersectoriales.

Por su parte, el Ministerio de la Mujer tiene un rol clave en la prevención y atención de la violencia de género facilitada por tecnologías. El incremento de prácticas como el acoso en línea, la sextorsión, el doxxing o la difusión no consentida de contenido íntimo requiere una respuesta estatal coordinada, sensible al género y centrada en los derechos humanos. La ciberseguridad, en este sentido, debe ser una herramienta para la protección y el empoderamiento de mujeres, niñas y personas LGBTI+.

En cuanto al Ministerio del Ambiente, su integración es crucial para garantizar que el desarrollo de infraestructuras digitales, centros de datos, y procesos tecnológicos considere su huella ecológica y se alineen con principios de sostenibilidad. El consumo energético, la gestión de residuos electrónicos y la planificación de una transformación digital ambientalmente responsable deben formar parte de la agenda de ciberseguridad desde una mirada de justicia climática y responsabilidad intergeneracional.

En suma, una gobernanza de la ciberseguridad inclusiva y eficaz requiere una visión integral e interministerial que reconozca los vínculos entre el entorno digital y las políticas de salud pública, equidad de género y sostenibilidad ambiental. Incluir formalmente a estos ministerios en los órganos consultivos o decisorios fortalecerá la legitimidad, eficacia y pertinencia social de la estrategia nacional de ciberseguridad.

3) ENFOQUE MILITAR Y NO CIVIL

Dentro del conjunto de propuestas legislativas presentadas sobre ciberseguridad, el proyecto identificado con el expediente D-2584815, impulsado por el Diputado Luis Federico Franco Alfaro, se distingue por atribuir

la rectoría en materia de ciberseguridad al Ministerio de Defensa Nacional. Este enfoque contrasta con las otras dos iniciativas legislativas y con el anteproyecto promovido por la Universidad Metropolitana de Asunción, que plantean como ente rector al Ministerio de Tecnologías de la Información y Comunicación (MITIC).

La asignación de la ciberseguridad al ámbito de la defensa representa un cambio sustantivo en la naturaleza del enfoque institucional, desplazando la coordinación del ecosistema digital hacia una lógica de seguridad nacional y militarización. **Este modelo se aparta de las buenas prácticas internacionales promovidas por organismos multilaterales como la OCDE**, que recomiendan enfáticamente que la gobernanza de la ciberseguridad permanezca bajo conducción civil, garantizando la transparencia, la participación multisectorial y el respeto a los derechos humanos.

Organizaciones como Fundación Karisma, desde la sociedad civil latinoamericana, también han advertido sobre los riesgos de un abordaje militar de la ciberseguridad. Este tipo de enfoque tiende a priorizar la lógica del control, la vigilancia y la defensa del Estado, por encima de la protección de derechos individuales y la promoción de una internet libre, abierta e inclusiva. Además, refuerza estructuras cerradas, poco participativas y menos sujetas a mecanismos de rendición de cuentas.

La militarización de la ciberseguridad **puede limitar el involucramiento de actores clave como la academia, el sector privado, la sociedad civil y organismos especializados en derechos humanos y tecnología**s. También desalinea la legislación nacional de los principios de gobernanza democrática de internet, que exigen la inclusión de múltiples partes interesadas y la construcción de políticas públicas desde la transparencia, la deliberación pública y el enfoque de derechos.

La rectoría civil no solo es una cuestión administrativa: es un principio estructural que define el carácter democrático de la política pública de ciberseguridad. Sustituir ese enfoque por uno militar compromete no solo la legitimidad institucional del marco normativo, sino también su capacidad de generar confianza, articular sectores y construir respuestas eficaces, sostenibles y respetuosas de las libertades fundamentales.

4) LA NECESIDAD DE QUE LA LEY DE CIBERSEGURIDAD CUENTE CON PRINCIPIOS RECTORES Y SANCIONES CLARAS

En el proyecto de ley en su artículo 1 al 3 habla sobre el objeto de ley y el ámbito de aplicación y un glosario sin embargo en toda la ley no existe ningún principio general.

Para que una ley tenga coherencia legislativa es importante desarrollar un apartado exclusivo de principios. Por ejemplo en el caso de la ley de Ciberseguridad de Chile[10] (Ley 21663) se encuentran algunos principios relevantes que pueden servir de inspiración:

Control de daños: frente a un ciberataque o a un incidente de ciberseguridad se deberá actuar coordinada y diligentemente, y adoptar las medidas para evitar su escalada y su posible propagación a otros sistemas.

Cooperación con la autoridad: para resolver los incidentes de ciberseguridadse deberá prestar cooperación con la autoridad competente y, si es necesario, cooperar entre diversos sectores, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios.

Coordinación: la ANCI y las autoridades sectoriales deberán cumplir sus cometidos coordinadamente, propender a la unidad de acción y evitar la duplicación o interferencia de funciones.

Seguridad en el ciberespacio: es deber del Estado resguardar la seguridad en el ciberespacio y velar que las personas puedan participar de un ciberespacio seguro, por lo que otorgará especial protección a las redes y sistemas que contengan información de aquellos grupos de personas que suelen ser en mayor medida objeto de ciberataques.

Respuesta responsable: la aplicación de medidas para responder a incidentes de ciberseguridad o ciberataques en ningún caso podrá significar la realización o el apoyo a operaciones ofensivas.

Seguridad informática: toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias.

Racionalidad: las medidas para la gestión de incidentes, las obligaciones de ciberseguridad y el ejercicio de las facultades de la ANCI deberán ser necesarias y proporcionales al grado de exposición a los riesgos, y al eventual impacto social y económico.

Seguridad y privacidad por defecto y desde el diseño: los sistemas informáticos, aplicaciones y tecnologías de la información deben diseñarse, implementarse y gestionarse teniendo en cuenta la seguridad y la privacidad de los datos personales que procesan.

4.1) LAS INFRACCIONES DEBEN SER DEFINIDAS CON CLARIDAD, CLASIFICADAS Y DEBEN SER PROPORCIONALES Y PREVIAMENTE DETERMINADAS POR LEY

Por otro lado, si bien el artículo 25, del proyecto menciona que las infracciones serán sancionadas a través de procedimientos administrativos sumarios —

10 Ley 21663 – Ciberseguridad. Chile (2025). Disponible en: https://www.leychile.cl/leychile/navegar?idNorma=1202434&idParte=10496230&idVersion=2222-02-02

incluyendo medidas como apercibimientos, multas e inhabilitaciones—, **no se especifican las conductas que serán consideradas leves, graves o gravísimas.**

Esta omisión resulta preocupante desde el punto de vista jurídico, ya que entra en tensión con el principio de legalidad, consagrado tanto en el derecho penal como en el derecho administrativo sancionador. Conforme a este principio —expresado en la máxima *"nullum crimen, nulla poena sine lege"*— ninguna persona puede ser sancionada por una conducta que no haya sido previamente definida y clasificada por una norma clara y precisa.

En el ámbito administrativo, la **potestad sancionadora del Estado debe ejercerse con base en normas que establezcan con antelación y exactitud** qué conductas constituyen infracción, su gravedad y la sanción correspondiente. La falta de una tipificación adecuada podría dar lugar a interpretaciones discrecionales, comprometiendo los principios de seguridad jurídica, legalidad y debido proceso.

Por ello, es imprescindible que el proyecto incluya una tipificación detallada de las infracciones y su correspondiente graduación, garantizando así el respeto al marco jurídico vigente y la legitimidad de las sanciones impuestas.

Se sugiere observar cómo, por ejemplo, la ley chilena abordó las sanciones.

Cuadro de Infracciones Graves – Ley de Ciberseguridad en Chile

Conducta	Obligado	Sanción
No haber implementado los protocolos y estándares establecidos por la Agencia para prevenir, reportar y resolver incidentes de ciberseguridad.	Todos	Multa de hasta 10.000 UTM, o hasta 20.000 UTM si se trata de un operador de importancia vital (OIV).
No haber implementado los estándares particulares de ciberseguridad.	Todos	Multa de hasta 20.000 UTM
Entregar fuera de plazo la información requerida para la gestión de un incidente de ciberseguridad.	Todos	Multa de hasta 20.000 UTM
Entregar a la ANCI información manifiestamente falsa o errónea.	Todos	Multa de hasta 20.000 UTM
Incumplir la obligación de reportar establecida en el artículo 9.	Todos	Multa de hasta 20.000 UTM
Negarse injustificadamente a cumplir una instrucción de la ANCI o entorpecer deliberadamente su actuación durante la gestión de un incidente, siempre que no tenga sanción especial.	Todos	Multa de hasta 20.000 UTM
Reincidir en una misma infracción leve dentro del plazo de un año.	Todos	Multa de hasta 20.000 UTM

Conducta	Obligado	Sanción
No haber implementado el sistema de gestión de seguridad de la información continuo (art. 8, letra a).	OIV	Multa de hasta 20.000 UTM
No haber elaborado o implementado los planes de continuidad operacional y ciberseguridad (art. 8, letra c).	OIV	Multa de hasta 20.000 UTM
No informar a los potenciales afectados sobre incidentes o ciberataques que puedan comprometer gravemente su información o sistemas (art. 8, letra g).	OIV	Multa de hasta 20.000 UTM
No adoptar medidas oportunas para mitigar la propagación o impacto de un incidente o ciberataque (art. 8, letra e).	OIV	Multa de hasta 20.000 UTM

5) CENTRAR LA NORMATIVA EN LA PROTECCIÓN DE LAS PERSONAS Y NO EN LA INFRAESTRUCTURA

Desde una perspectiva de derechos humanos, la Cibersguridad no solo abarca la protección de los activos informáticos, sino también el resguardo de la información personal[11] que circula dentro de estos sistemas.

Actualmente no solo se trata de proteger al Estado de un ataque que comprometa el control sobre la infraestructura eléctrica de un centro poblado, **sino que se debe proteger, por dar ejemplos, los datos de las personas que pueden sufrir cuando se dan fugas masivas de información en sectores esenciales como la salud, de evitar los impactos en una economía** cuando se secuestra el sistema de suministro de gasolina en una región determinada, o de prevenir afectaciones a los derechos de la población si sucede un ciberataque que compromete las elecciones en un país democrático. Gestionar el riesgo nacional digital tiene como propósito proteger la seguridad nacional, pero va mucho más allá y su finalidad principal **es la de apoyar la prosperidad económica y social**, es pensar en la seguridad ciudadana y no solo de los Estados.

También es necesario reflexionar cómo los más recientes escándalos mundiales sobre Ciberseguridad dan cuenta de la vulnerabilidad de determinados grupos poblacionales —especialmente defensores de derechos humanos[12], periodistas[13], activistas medioambientales[14], etcétera— a ataques que provienen del crimen organizado, pero también que son protagonizados por su propio Estado.

11 La protección de la persona que está detrás de esta información o dato.
12 TEDIC (2024) Ciberseguridad en defensores y defensoras de derechos humanos en Paraguay: https://www.tedic.org/ciber_defensores/
13 TEDIC (2023) Violencia digital a mujeres periodistas. Disponible en: https://www.tedic.org/la-violencia-digital-de-genero-a-periodistas-en-paraguay/
14 TEDIC (2025) Defensa de los derechos humanos en la transción climática: aporte de TEDIC al informe del ACNUDH. Disponible en: https://www.tedic.org/defensa-de-los-derechos-humanos-en-la-transicion-climatica-el-aporte-de-tedic-al-informe-del-acnudh/

En este contexto, es importante **diferenciar los conceptos de vulnerabilidad y riesgo**. Por un lado, la vulnerabilidad se define como una debilidad en los sistemas de protección, especialmente en los dispositivos e información de personas defensoras de derechos humanos. Por su parte, el riesgo se entiende como la probabilidad de que una vulnerabilidad sea explotada, lo que implica considerar tanto la posibilidad de que ocurra un evento como las consecuencias que este podría tener. Finalmente, un incidente se produce cuando un riesgo se materializa en un contexto donde existe una vulnerabilidad.

Aunque el enfoque predominante ha sido la defensa del Estado a través de organismos como el CERT, también se reconoce la necesidad de ampliar la seguridad digital a la ciudadanía y que **incluya todos los tipos de riesgos tales como las pérdidas financieras, interrupciones en actividades, robo de propiedad intelectual, daños a la reputación, violaciones a la privacidad, disminución de la competitividad, amenazas a la libertad de expresión, daños físicos y medio ambientales**. Además, esto es particularmente crucial para garantizar un entorno seguro para quienes defienden los derechos humanos, dado su papel fundamental en la protección de los valores democráticos.

El Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión (2015)[15], **David Kaye, destaca la relevancia del cifrado y el anonimato** en las comunicaciones digitales. Estas herramientas son esenciales no solo para industrias clave, como los medios de comunicación, sino también para la democracia en general.

La OCDE, en sus publicaciones sobre seguridad digital, subraya la importancia de poner a las personas en el centro de las políticas. Sus “Recomendaciones sobre la gestión del riesgo digital”[16] destacan cuatro principios clave:

1. Mejorar la concienciación, competencias y capacitación de la población.
2. Fomentar la co-responsabilidad, un principio ya presente pero poco desarrollado en el Conpes de seguridad digital.
3. Priorizar los derechos humanos como objetivo central.
4. Promover la cooperación entre múltiples actores, incluyendo gobiernos, sector privado, academia y sociedad civil.

Además, la OCDE no solo menciona genéricamente los derechos humanos, sino que resalta su impacto en áreas como la privacidad y la protección de denunciantes, especialmente en la lucha contra la corrupción. Estos lineamientos subrayan la responsabilidad de los gobiernos de garantizar la

15 ONU (2015) Report on encryption, anonymity, and the human rights framework https://www.ohchr.org/en/calls-for-input/report-encryption-anonymity-and-human-rights-framework

16 OECD (2015) Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0415

libertad individual, incluso en contextos de corrupción económica y política.

El proyecto, sin embargo, ignora documentos recientes de la OCDE que enfatizan la gestión de vulnerabilidades y el papel crucial de los investigadores de seguridad en la protección digital. Adoptar estas recomendaciones debería conducir a una política nacional que reconozca y proteja esta labor esencial.

La promoción y protección de los derechos humanos como elemento central de cualquier política nacional de seguridad digital es central para que ésta aporte a la prosperidad económica y social y hay que hacer el esfuerzo por integrarlos, en esta propuesta no se observa la centralidad ni profundidad que tiene que tener una normativa de la seguridad de las personas en el ciberespacio.

5.1) POLÍTICAS CRIPTOGRÁFICAS

El proyecto debe incluir **principios de cifrado para proteger las comunicaciones y la navegación en Internet, asegurando el derecho a la privacidad e intimidad de las personas usuarias**. Esto podría lograrse a través de talleres prácticos, por ejemplo, enseñando a los usuarios a cifrar dispositivos como discos duros externos.

Es fundamental destacar que la criptografía es un componente esencial de muchos sistemas, como el bancario o el comercio electrónico. Por lo tanto, no debe limitarse a ciertos grupos, sino ser accesible a toda la población. Una comunicación o navegación sin cifrado no solo es “menos segura”, sino que queda expuesta a vulnerabilidades y accesos no autorizados a través de "puertas traseras".

5.2) FOMENTAR LA ANONIMIZACIÓN DE LAS PERSONAS USUARIAS EN INTERNET Y SALVAGUARDAS NACIONALES

El anonimato en Internet es clave para la libertad de expresión. David Kaye, ex relator especial de ONU citado más arriba, resalta en su informe que “la encriptación y el anonimato proporcionan la privacidad y seguridad necesarias para el ejercicio de la libertad de opinión y expresión en la era digital”. En línea con esta premisa, Kaye recomienda que las legislaciones nacionales reconozcan el derecho de los individuos a **proteger la privacidad de sus comunicaciones mediante tecnologías de cifrado y anonimato, y promuevan el acceso a estas herramientas.** Subraya que el debate sobre su uso debe centrarse en los beneficios que ofrecen, especialmente para grupos en riesgo de interferencia ilegal.

Es esencial que el borrador de la estrategia adopte estas recomendaciones con un enfoque de derechos. También se debe respaldar la política de MITIC sobre software libre y código abierto[17], que ha demostrado ser más eficaz en la

17 Challet, D., & Du, Y. L. (2005). MICROSCOPIC MODEL OF SOFTWARE BUG DYNAMICS: CLOSED SOURCE VERSUS OPEN SOURCE. http://arxiv.org/pdf/condmat/0306511.pdf

solución rápida de fallos de seguridad.

Además, se debe fomentar la notificación a los usuarios si sus datos personales son accesados, proporcionando tiempo y suficiente información para impugnar decisiones o buscar soluciones alternativas. La obligación de notificar recae en el Estado, pero los proveedores de servicios de comunicaciones deben poder notificar a las personas directamente. El retraso en la notificación solo debe justificarse en casos excepcionales, como cuando exista un riesgo grave para la seguridad o la vida humana, y siempre bajo la autorización de la autoridad judicial competente.

5.3) FOMENTO DE LA NOTIFICACIÓN A LAS PERSONAS USUARIAS

El proyecto aborda la notificación de incidentes en su artículo 15; sin embargo, el enfoque se limita exclusivamente a la obligación de informar a las autoridades competentes dentro de un plazo de 24 horas. Esta disposición omite un componente clave presente en los estándares internacionales y buenas prácticas: la notificación oportuna a las personas usuarias potencialmente afectadas. Incluir esta obligación es fundamental para garantizar la transparencia, mitigar daños y proteger adecuadamente los derechos de quienes podrían ver comprometida su información o sus sistemas. La exclusión de esta dimensión debilita el enfoque centrado en la ciudadanía y reduce la efectividad del marco de respuesta ante incidentes.

Es fundamental **promover la notificación a las personas usuarias en caso de que sus datos personales hayan sido accedidos**[18]. Esta notificación debe incluir información suficiente para que los usuarios puedan impugnar la decisión o explorar otras soluciones. Además, deben tener acceso a los materiales que respalden la solicitud de autorización. Aunque la obligación primaria de notificar recae en el Estado, los proveedores de servicios de comunicación deben tener la libertad de informar a los usuarios directamente.

El retraso en la notificación solo se justifica en las siguientes circunstancias:

1. Si la notificación podría poner en grave peligro el objetivo de la vigilancia autorizada o si existe un riesgo inmediato para la vida humana.
2. Si la autorización para el retraso de la notificación es concedida por la autoridad judicial competente en el momento de la autorización de la vigilancia.
3. Si el usuario afectado es notificado tan pronto como el riesgo desaparece, según lo determine la autoridad judicial competente.

18 EFF (2013) Notificación del usuario. Necesarios y proporcionados. https://necessaryandproportionate.org/es/necesarios-proporcionados

6) SE SUGIERE INCLUIR EN OBLIGACIONES A LAS ENTIDADES EN LA LEY DE CIBERSEGURIDAD

Para una norma de alto nivel en materia de ciberseguridad, es esencial establecer de forma clara y precisa los deberes generales que deben cumplir las entidades sujetas a su aplicación. Los artículos 8 y 9 referidos a las obligaciones son insuficientes, estos **deberes generales** incluyen:

- La obligación de adoptar de forma permanente medidas tecnológicas, organizacionales, físicas y/o informativas orientadas a prevenir, detectar, reportar y gestionar incidentes de ciberseguridad.
- Asimismo, las entidades deberán implementar los protocolos y estándares que establezca el Viceministerio de Ciberseguridad, así como aquellos estándares particulares que correspondan conforme a la regulación sectorial aplicable.
- Dichos protocolos y estándares deben estar diseñados con el propósito de prevenir y gestionar los riesgos vinculados a la ciberseguridad, mitigar el impacto de los incidentes, preservar la continuidad operacional de los servicios, y salvaguardar la confidencialidad e integridad de la información, redes y sistemas informáticos.

Además de los deberes generales, la norma debe incluir un conjunto de **deberes específicos** para asegurar una gestión más técnica, constante y profunda de la ciberseguridad dentro de cada entidad obligada.

- Entre ellos se encuentra la implementación de un sistema de gestión de seguridad de la información de carácter continuo, así como la obligación de mantener un registro actualizado de las acciones ejecutadas como parte de dicho sistema.
- Las entidades también deberán elaborar e implementar planes de continuidad operacional y de ciberseguridad que estén debidamente certificados y sujetos a revisiones periódicas. Adicionalmente, será necesario llevar a cabo operaciones constantes de monitoreo, simulacros y análisis de sistemas para identificar amenazas o programas maliciosos, y reportarlos oportunamente al CSIRT Nacional.
- Por otro lado, las entidades deberán adoptar sin demora las medidas necesarias para contener y minimizar los efectos de los incidentes de ciberseguridad. También deberán contar con las certificaciones establecidas por la legislación vigente y, cuando corresponda, notificar a los potenciales afectados sobre la ocurrencia de incidentes, especialmente cuando se trate de compromisos graves de datos personales o sistemas críticos. Esta notificación deberá realizarse en los casos requeridos por la autoridad competente o cuando sea

indispensable para prevenir futuros incidentes.

- Finalmente, la norma deberá exigir la existencia de programas permanentes de capacitación, formación y sensibilización del personal, incluyendo campañas de ciberhigiene, así como la designación obligatoria de un delegado de ciberseguridad, quien actuará como enlace con el MITIC y deberá reportar a las máximas autoridades de la entidad.

7) LA NECESIDAD DE COMPLEMENTAR CON URGENCIA NORMATIVAS COMO LA LEY DE INFRAESTRUCTURA ESENCIALES

El proyecto de ciberseguridad muestra una clara priorización de la ratificación del segundo protocolo de Cibercrimen, lo que refleja un enfoque en el fortalecimiento de las medidas legales contra el cibercrimen a nivel internacional. Sin embargo, este enfoque parece desatender la necesidad urgente de desarrollar una legislación nacional robusta y complementarias a esta norma:

7.1) INFRAESTRUCTURAS ESENCIALES

El proyecto solo incluye una definición general de “infraestructura crítica” en el artículo 3 y menciones mínimas a sus obligaciones, sin desarrollar un marco normativo sólido y autónomo. Esta limitación es especialmente problemática dado que muchas de las funciones vitales del Estado y la sociedad —como la generación eléctrica, las telecomunicaciones o incluso el sistema de votación— dependen de sistemas físicos y digitales que deberían recibir protección prioritaria. Por ejemplo, ¿las máquinas de votación deberían considerarse infraestructura crítica por su rol en la legitimidad democrática? ¿O las redes eléctricas por su impacto sistémico en la economía y la seguridad?

La experiencia comparada muestra que países como Chile (2023) y Brasil (2020) han optado por normativas específicas para proteger estas infraestructuras esenciales. Además, la Guía "Going Digital" de la OCDE[19] ofrece aportes clave al debate, destacando que el concepto de infraestructura crítica evolucionó en los años 90 para abarcar sectores como energía, finanzas, salud y telecomunicaciones. Posteriormente, se introdujo la noción de infraestructuras críticas de información (ICI) al reconocer la importancia de los sistemas digitales que respaldan dichos sectores. Sin embargo, la dificultad de delimitar las ICI ha dificultado su integración efectiva en los marcos políticos nacionales.

La OCDE propone ir más allá del enfoque centrado en activos físicos o sistemas específicos, y **sugiere adoptar el concepto de "actividades críticas", centrado en los riesgos que afecten la continuidad de servicios**

19 OECD. Bernat, L. (2021), "Enhancing the digital security of critical activities", Going Digital Toolkit Note, No. 17, https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf

esenciales. Según este enfoque, lo relevante no son solo los activos subyacentes, sino las funciones cuya interrupción tendría consecuencias graves para la salud, seguridad, protección ciudadana o el bienestar económico y social. Bajo esta lógica, sectores como la minería o la industria automotriz podrían ser considerados críticos en determinados contextos nacionales, no por su infraestructura en sí, sino por su impacto sistémico.

Por tanto, resulta fundamental que Paraguay desarrolle una ley específica sobre infraestructura crítica —o, idealmente, sobre actividades críticas— que defina con claridad sus alcances, obligaciones y mecanismos de protección, articulada con la normativa de ciberseguridad pero no subsumida dentro de ella.

7.2 AUSENCIA DE ARTICULACIÓN CON OTRAS POLÍTICAS Y MARCOS NORMATIVOS

Finalmente, el proyecto no establece vínculos con instrumentos existentes o en desarrollo, como el Plan Estratégico de Ciberseguridad 2025–2028 (Decreto 3900/25), el proyecto de ley sobre Inteligencia Artificial (D-2584139), el proyecto de ley Integral de protección de datos personales (D-2162170) o futuras normativas sobre gobernanza de datos. Esta falta de integración refuerza una visión fragmentada, centrada casi exclusivamente en el aspecto técnico-punitivo de la ciberseguridad, sin incorporar una mirada holística que articule derechos fundamentales, políticas públicas y estrategias tecnológicas.

Una ley moderna de ciberseguridad debería actuar como marco integrador, que dé coherencia y sentido a todas las iniciativas relacionadas con el entorno digital, y que sirva como punto de partida para la formulación de políticas intersectoriales. Su función debe ir más allá de la protección contra delitos informáticos; debe fomentar un ecosistema digital resiliente, inclusivo y centrado en la persona.

El hecho de que el proyecto de ciberseguridad solo mencione acciones vinculadas a la ratificación del protocolo de Cibercrimen (mirada punitivista), sin un paralelo claro con la creación de una lista de normativas complementarias tales como se citan más arriba puede reflejar una visión más orientada a los aspectos técnicos de la seguridad informática y la cibercriminalidad, en lugar de una visión integral de la ciberseguridad que también abarque la protección de la privacidad y los derechos fundamentales de las personas. Este desbalance puede tener implicaciones negativas para la confianza en el sistema digital del país, ya que las personas usuarias no solo necesitan protección contra delitos informáticos, sino también garantías de que sus datos personales serán manejados de manera responsable y segura.

8) SEGURIDAD POR DISEÑO

El proyecto debe priorizar y conceptualizar la seguridad desde el diseño,

garantizando que los estándares de certificación sean establecidos en colaboración con el Estado, expertos de la sociedad civil y la academia, y no exclusivamente a través de empresas con certificaciones ISO. La ciberseguridad no solo enfrenta amenazas como el terrorismo internacional, el espionaje estatal o el cibercrimen, sino también riesgos inherentes al código fuente de software y hardware, como sistemas operativos y aplicaciones. Por lo tanto, el proyecto debe incluir mecanismos para garantizar la seguridad de la información que vayan más allá de soluciones básicas como los antivirus.

Es esencial definir medidas de seguridad rigurosas y auditar los sectores críticos, asegurando la protección de la infraestructura a través de la Comisión Nacional, con la participación de expertos de la sociedad civil para garantizar la supervisión pública. Además, se podría incentivar a las empresas locales que cumplan con los estándares de seguridad y la protección de los derechos humanos, promoviendo este enfoque en centros educativos y universidades.

El proyecto debe incluir medidas para desincentivar a los fabricantes que comprometan la seguridad de las personas usuarias, como aquellos que instalan puertas traseras o mecanismos de vigilancia. Esta práctica es particularmente delicada, ya que algunos gobiernos conocen estas vulnerabilidades y eligen no denunciarlas por beneficio propio. Asimismo, es importante incentivar a las empresas y organizaciones a adoptar mejores prácticas de seguridad, como el uso de conexiones cifradas (HTTPS), autenticación de doble factor y otras tecnologías de comunicación segura, especialmente en iniciativas de ciudades inteligentes y otros sistemas críticos.

9) CAMBIAR DE UNA NARRATIVA DE CRISIS HACIA UNA NARRATIVA POSITIVA

A lo largo del proyecto se presentan terminologías sobre los tipos ataques que existen en el ciberespacio, se aborda la seguridad desde un enfoque predominantemente negativo, asociándola con la mera ausencia de daño. Este planteamiento limita la comprensión del concepto de Ciberseguridad. En un sentido más amplio y sustantivo, la (ciber)seguridad es un valor positivo: implica la capacidad de una persona para acceder a recursos fundamentales y utilizarlos según sus necesidades y preferencias.

Desde la perspectiva de los Derechos Humanos, la seguridad se enfoca en garantizar que las personas puedan actuar libremente y de manera responsable. Por ello, el proyecto de ley de ciberseguridad no debería limitarse a un rol puramente defensivo, sino asumir un papel facilitador, con el objetivo de promover el bienestar de las personas como eje central.

Este enfoque además de fortalecer la protección individual, contribuye a implementar “soluciones” que reduzcan las amenazas a los derechos humanos, pilar esencial de cualquier sistema democrático.

La narrativa de crisis inminente en la introducción y motivación, reforzada por los datos de incidentes presentados en el proyecto, genera un lenguaje alarmista que oscurece la necesidad de abordar de manera objetiva los riesgos reales. Esta insistencia en un discurso de crisis en la motivación del proyecto y en el plan de estrategia de ciberseguridad ya fueron evidenciados. A nivel global, muchos gobiernos están siendo cuestionados por emplear estas "amenazas", tanto internas como externas, como justificación para incrementar significativamente la inversión en ciberseguridad, con un enfoque en sistemas de vigilancia masiva que terminan por ampliar el control sobre Internet y sobre la ciudadanía.

1. Este enfoque también distorsiona el debate al mezclar desafíos de distinta naturaleza:
   Por un lado, se mencionan amenazas donde la tecnología es intrínseca al riesgo, como ataques a infraestructuras críticas, ataques DDoS, espionaje o accesos no autorizados a datos, dispositivos o redes.
2. Por otro, se incluyen amenazas en las que la tecnología actúa solo como medio. Ejemplos de esto son la pornografía infantil, el envío masivo de correos no deseados o la planificación de robos. En estos casos, el riesgo no reside en la infraestructura tecnológica, sino en la comunicación y el contenido en sí. Aunque la tecnología puede amplificar la magnitud o el alcance de estos delitos, no constituye un elemento central en la definición de ciberseguridad.

Consideramos fundamental replantear esta narrativa hacia un enfoque positivo y centrado en las personas ("human-centered approach"). Esto implica que el Estado paraguayo desarrolle políticas de protección tanto en línea como fuera de ella, priorizando el bienestar de los individuos.

Finalmente, es crucial destacar los riesgos generados por las políticas y prácticas tanto del Estado como del sector privado. Estas incluyen desde el uso de puertas traseras y accesos directos hasta el manejo deficiente de sistemas, como la falta de HTTPS o la existencia de vulnerabilidades críticas.

Tampoco se abordan los problemas que afectan directamente a la población, como los diseños digitales intencionalmente adictivos, que pueden tener graves consecuencias para la salud mental. Estos incluyen estrés, ansiedad y la sensación de hiperconexión constante, que impactan negativamente en el bienestar individual y colectivo[20], daños ambientales, propiedad intelectual, daño a la reputación entre otros.

En la parte de la motivación del proyecto como en el borrador de ley tampoco se señala que la mayoría de los problemas de infraestructura tienen su origen

20 TEDIC (2021) Salud mental en Internet y el uso de las tecnologías. https://www.menteenlinea.org/white_paper/Salud-Mental-en-Internet.pdf

en el sector privado, debido al desarrollo de sistemas débiles, la falta de mantenimiento del hardware y software, y otras vulnerabilidades. Es fundamental que el plan incluya mecanismos que fomenten un mayor intercambio entre empresas privadas y organismos públicos, con el objetivo de mejorar la respuesta a las amenazas de seguridad en Internet desde un enfoque de derechos humanos.

Ambos sectores desempeñan roles cruciales en la detección y control de amenazas. Sin embargo, cualquier mecanismo de cooperación debe estar claramente definido, sujeto a escrutinio público y contar con salvaguardas adecuadas. Por ejemplo, se deben prever sanciones en casos de fuga de información personal, mecanismos de reparación en situaciones de abuso y garantías para proteger los derechos de las personas afectadas.

Es necesario identificar los factores económicos, sociales y políticos que exponen a las personas a estos riesgos. Más allá de entender cómo se vulneró la seguridad, resulta esencial prevenir dichas situaciones y ofrecer apoyo integral a las víctimas.

10) NO SE INCLUYE LA VIGILANCIA DE LAS COMUNICACIONES POR PARTE DEL ESTADO ENTRE LOS ANTECEDENTES

Dentro de las problemáticas de seguridad, no se mencionan los riesgos asociados con la adquisición de herramientas de vigilancia masiva[21][22]. Esto se agrava con el almacenamiento de datos de la ciudadanía mediante tecnologías cada vez más accesibles, no solo para el gobierno, sino también para empresas privadas y grupos delictivos[23]. Existen antecedentes de la compra de software de vigilancia por parte del Estado paraguayo[24][25]

El proyecto de ciberseguridad debe abordar este tema desde un análisis bidireccional. Por un lado, las agencias y dependencias gubernamentales deben contar con herramientas para la persecución de delitos, siempre que su uso esté estrictamente regulado por un marco legal que respete los derechos humanos. Por otro lado, el plan debería incluir un estudio de mejores prácticas internacionales en torno a:

- La protección de la privacidad y los datos personales.
- Los derechos humanos, el derecho internacional humanitario y los valores fundamentales.

21 Wikipedia. PEGASUS https://en.wikipedia.org/wiki/Pegasus_Project_(investigation)
22 TEDIC (2018) La enajenación continua de nuestros derechos – Reconocimiento facial en Paraguay – vigilancia masiva. https://www.tedic.org/la-enajenacion-continua-de-nuestros-derechos-sistemas-de-identidad-biometria-y-camaras-de-vigilancia-no-reguladas-en-paraguay/
23 TEDIC (2022) Vigilancia policial en manifestaciones en Paraguay https://www.tedic.org/manifestaciones-libres-guia-sobre-la-vigilancia-policial-en-manifestaciones-en-paraguay/
24 TEDIC (2016) Espionaje a periodistas por parte del Estado paraguayo. https://www.tedic.org/espionaje-a-periodista-confirma-que-el-estado-intercepta-comunicaciones-ilegalmente/
25 TEDIC (2016) Más preguntas y dudas sobre el software malicioso adquirido por la SENAD. https://www.tedic.org/mas-preguntas-y-dudas-sobre-software-malicioso-adquirido-por-senad/

Asimismo, es crucial incorporar mecanismos de notificación a las partes afectadas cuando su información se vea comprometida, permitiéndoles verificar los hechos y presentar denuncias en casos de abuso, ya sea por parte de instituciones estatales o empresas privadas.

Finalmente, la Relatoría Especial de Libertad de Expresión e Internet de la ONU señala: *"Las respuestas de los Estados en materia de seguridad en el ciberespacio deben ser limitadas y proporcionales, buscando cumplir con fines legales precisos que no comprometan las virtudes democráticas que caracterizan a la red"*[26]

11) PROTECCIÓN A LOS DIVULGADORES DE SEGURIDAD DIGITAL (WHISTLEBLOWERS[27])

Las políticas de ciberseguridad deben desalentar y condenar que los propietarios de sistemas, incluidos actores estatales, utilicen herramientas legales para amenazar con acciones judiciales a quienes reportan vulnerabilidades, en lugar de acoger sus informes de buena fe[28]. La OCDE ha identificado que los principales riesgos legales para los investigadores de seguridad se encuentran en áreas como el derecho penal, la propiedad intelectual, la protección de datos y el derecho contractual. Sin embargo, el borrador de la estrategia actual ignora por completo la necesidad de estrategias que reconozcan el papel crucial de estos investigadores y que les ofrezcan canales confiables para reportar vulnerabilidades.

El trabajo más reciente del grupo de seguridad digital de la OCDE se ha centrado en la gestión de vulnerabilidades, abordando la protección de los investigadores de seguridad digital y la creación de una respuesta coordinada a sus informes sobre vulnerabilidades. En 2021, la OCDE publicó varios documentos diseñados para apoyar a los estados en el desarrollo de sus políticas nacionales de seguridad digital.

La seguridad digital está claramente vinculada a derechos como la libertad de expresión y la privacidad, pero también impacta áreas como la salud y el medio ambiente. Los documentos de la OCDE destacan que su protección debe ser una prioridad en los planes nacionales. Hoy en día, la ciberseguridad no solo busca proteger al Estado de ataques que comprometan infraestructuras críticas, sino también salvaguardar datos personales en sectores esenciales como la salud, prevenir impactos económicos como el secuestro de sistemas de suministro de combustible, y proteger la integridad de procesos

26 ONU (2015) Report of the Special Rapporteur to the Human Rights Council on the use of encryption and anonymity to exercise the rights to freedom of opinion and expression in the digital age. http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

27 Whistleblowers. https://es.wikipedia.org/wiki/Alertador

28 Una vulnerabilidad digital es un error de diseño o de implementación, o una debilidad que tiene un equipo, programa, servicio o tecnología que puede ser explotada para comprometer la información o la seguridad de un sistema. https://web.karisma.org.co/comunicado-de-prensa-nuevo-reporte-de-la-ocde-reconoce-el-trabajo-de-karisma-en-la-construccion-de-una-ruta-para-la-divulgacion-de-vulnerabilidades-en-colombia/

democráticos como las elecciones.

La gestión del riesgo digital nacional debe ir más allá de la seguridad estatal y enfocarse en la protección de la ciudadanía, promoviendo la prosperidad económica y social.

El documento actual omite abordar este tema crucial. Curiosamente, menciona hackatones organizados por el Estado para identificar vulnerabilidades y riesgos, pero no ofrece garantías ni protecciones para quienes detectan estos problemas fuera de esos espacios controlados. ¿Qué sucede si una persona encuentra una vulnerabilidad de manera independiente? ¿Qué mecanismos existen para asegurar que no sea perseguida por hacerlo? Sin estas protecciones, se desincentiva una contribución esencial para la seguridad digital.

12) DEFINICIONES ERRÓNEAS CONCEPTUALES, VAGAS Y AMPLIAS

En el proyecto de ley de ciberseguridad se observa una falta de coherencia terminológica en relación con los conceptos utilizados para referirse a las conductas ilícitas en el entorno digital. Aunque coloquialmente se emplean expresiones como “ciberamenazas” o “ciberdelitos”, estos términos no tienen un reconocimiento normativo claro ni en el Código Penal paraguayo ni en los tratados internacionales como el Convenio de Budapest sobre Ciberdelincuencia.

En este contexto, sería recomendable que la ley proponga una unificación conceptual que armonice el lenguaje jurídico con el marco penal vigente. Por ejemplo, en lugar de “ciberdelitos” o “delitos cibernéticos” —términos que no están definidos ni tipificados actualmente—, se debería emplear “delitos informáticos”, que es la categoría más reconocida tanto en la doctrina penal como en los instrumentos internacionales.

Asimismo, es fundamental unificar y clarificar el uso de términos como “ciberataques” (artículo 1, 3 y 13) y “ataques cibernéticos” dentro del proyecto. Mientras que el artículo 3 ofrece una definición básica de “ciberataques”, el artículo 14 menciona “ataques cibernéticos” sin una referencia clara a su significado, lo que genera ambigüedad. Para evitar interpretaciones inconsistentes, estos conceptos deben alinearse con figuras penales ya existentes, como el sabotaje informático, el acceso indebido a sistemas, o el daño a datos o infraestructuras digitales. En caso de que se propongan nuevas tipificaciones delictivas, resulta imprescindible establecer su relación con el marco penal vigente, asegurando así tanto su aplicabilidad efectiva como su compatibilidad jurídica con el ordenamiento nacional.

En suma, para garantizar una aplicación efectiva, precisa y jurídicamente

sólida de la ley, es fundamental que se revise y unifique el uso de terminología penal y técnica, asegurando su coherencia con el ordenamiento jurídico nacional e internacional.

ULTIMA HORA | ASUNCIÓN DOMINGO 11, DICIEMBRE 2022 — Política 5

Advierten que políticos usan datos de redes para influir en los votantes

Las campañas electorales se sirven de datos recopilados de las personas en redes sociales para afectar sus decisiones. Tedic comparte por este motivo una guía para contrarrestar sus efectos.

Ante la cercanía de las elecciones internas, previstas para el 18 de diciembre, la organización Tedic pone sobre la mesa y visibiliza la manera en que las campañas políticas son diseñadas a partir de datos que los usuarios generan en las redes sociales, como sus características personales, preferencias o prácticas de consumo, y a partir de esa información influir en sus decisiones.

Para reducir sus efectos y tener control sobre este hecho, Tedic expuso una guía para el votante, con siete consejos para depurar los datos ante el uso abusivo en época de elecciones.

"El mundo de las campañas políticas se ha vuelto cada vez más complejo y cada vez más impulsado por los datos generados por las personas usuarias de redes sociales y tecnología. Estos datos se extienden mucho más allá de los padrones electorales: todo, desde el contenido de nuestro carrito de compra web, la interacción en publicaciones de Facebook, hasta el cine que elegimos visitar un viernes por la noche, puede ser utilizado por partidos y políticos para armar un perfil de persona votante y así influir en nuestras decisiones", señala la organización de derechos digitales.

El objetivo es que las personas puedan emitir su voto "sabiendo cómo y cuándo se utilizan estas técnicas digitales y qué pueden hacer para contrarrestarlas".

En el material, al que se puede acceder en la página web de Tedic, se explica qué tipo de datos se recopilan y cómo son utilizados para persuadir a los votantes. Entre las técnicas de campaña que se citan se encuentran la escucha digital, la microsegmentación y las pruebas A/B.

"Cuanto más sepan las campañas políticas sobre vos, más pueden influirte ya sea reclutándote como voluntario, animándote a donar, influenciando tu voto, o incluso hacer que vayas al colegio electoral en el día de las elecciones", explica el material.

CONSEJOS. De los siete consejos que se apuntan, el primero es "cambiar la rutina", se refiere a suscripciones o pagos online. Se recomienda cambiar ocasionalmente estas prácticas, como por ejemplo, hacer un pago en efectivo.

El segundo, "personalizar preferencias en redes sociales", que se refiere a medidas a partir de la configuración del perfil, donde se pueden cambiar preferencias de anuncios y márketing, o borrar el historial de actividades.

Tercero, "bloquear navegadores del teléfono y computadora", para adelantarse a algunos rastreadores en línea utilizados por partidos políticos. Se puede habilitar la opción de "no rastrear".

Cuarto, "informarse" sobre el panorama de anuncios políticos, que se pueden ver en la Biblioteca de Anuncios de Facebook, el informe de Transparencia de Google, entre otros.

Cinco, "limitar quiénes saben dónde estás". Se recomienda borrar la huella de ubicación del dispositivo móvil.

Seis, "hablar" con representantes de partidos políticos para solicitar información de cómo usan los datos personales en su campaña.

Por último, el consejo siete, "compartir con la comunidad", amigos y familia, la información de cómo se usan los datos personales en las campañas políticas.

"Los partidos políticos tienen que pedirte permiso antes de recopilar tus datos personales. Pero cuando hacés clic en 'Acepto' en un sitio web, aplicación o boletín informativo, puede que no quede claro qué datos personales estás accediendo a compartir", explica la guía.

En el material se hace énfasis en que las plataformas de las redes sociales tienen acceso a todo tipo de datos que pueden ser útiles sobre las personas votantes, como hábitos de gasto, estilo de vida, actividad en línea, otros. "Esto los convierte en sitios ideales para que las campañas políticas hagan publicidad. Las campañas políticas pueden usar Facebook (propietario de Instagram y WhatsApp), Google (propietario de Youtube y Búsqueda de Google) y Snapchat, para dirigirte anuncios específicos, basados en cosas como tu edad, ubicación y género. Pero también pueden usar información muy concreta, como con qué tipo de contenido interactuás en sus plataformas, incluyendo a lo que le das 'Me gusta' o comentás", detalla.

El ámbito es todavía poco claro, según se apunta en la guía.

Esta falta de claridad o desconocimiento por parte de las personas es calificado como poco democrático, por lo que desde Tedic se recomienda conocer cómo se utilizan los datos para persuadir en una elección, de modo que se puedan tomar decisiones políticas más informadas.

ARCHIVO

Perfiles. Con información del votante, los partidos pueden influir en sus decisiones y persuadirlos con mensajes adaptados.

CÓMO DEPURAR DATOS

- ✔ **Cambiá tus rutinas.** Como pagar en efectivo ocasionalmente.
- ✔ **Personalizá tus preferencias.** En anuncios o borrar tu historial.
- ✔ **Bloqueá los navegadores.** Habilitá "no rastrear".
- ✔ **Informate.** Sobre los anuncios políticos.
- ✔ **Limitá quién sabe dónde estás.** Borrá huellas de ubicación.
- ✔ **Hablá.** Preguntá cómo usan tus datos.
- ✔ **Hablá con tu comunidad.** Familia y amigos.

Tu actividad y la información que proporcionas

Meta. Facebook e Instagram recopilan tus actividades.

Datos de tu Cuenta de Google

Estos datos se usan para personalizar los anuncios y se basan en la información que tú compartes o que puede suponerse sobre ti. Administra los datos en tu Cuenta de Google

Género: Mujer — Edad: Entre 35 y 44 ... — Idioma: 5 idiomas

Categorías usadas para mostrarte anuncios

Es posible que veas anuncios dirigidos a personas de estas categorías, que se basan en tu actividad en Google. Puedes agregar anuncios de otras categorías o desactivar las que no quieres ver.

Google. El gigante muestra cómo usa datos para anuncios.