Comentarios al borrador 14 de noviembre de la Estrategia Nacional de Ciberseguridad paraguaya

El 14 de noviembre, MITIC publicó para comentarios públicos, el borrador de la última versión de la Estrategia Nacional de Ciberseguridad. Este documento busca desarrollar una estrategia sobre los siguientes ejes: Investigación, Desarrollo e Innovación, Protección de Infraestructuras Críticas, Capacidad de Respuesta ante Incidentes Cibernéticos, Capacidad de Investigación y Persecución de la Ciberdelincuencia, Administración Pública y Coordinación Nacional.

Por tanto, es fundamental que su enfoque sea compatible con parámetros internacionales sobre ciberseguridad y derechos humanos. Desde TEDIC[1] compartimos nuestros comentarios estructurales y sustantivos del documento, asi como de forma debido a la importancia del tema, gobernanza y ciberseguridad, se echa de menos un enfoque 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 que las políticas de ciberseguridad tengan una perspectiva de derechos humanos trasversal al documento

En el documento borrador en la parte inicial se incluyen todos los derechos fundamentales que se encuentran en la Constitucion nacional paraguaya, sin embargo solo se plantea al comienzo del mismo y no se realiza ninguna de las soluciones pensadas en la persona sino soluciones en la defensa de las infraestructuras.

La perspectiva de derechos humanos no solo abarca la protección de los activos informáticos, sino también el resguardo de la información personal[2] que circula dentro de estos sistemas. 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 reisgos tales como las pérdidas financieras, interrupciones en actividades, robo de propiedad intelectual, daños a la reputación, violaciones a la privacidad, disminución de la

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

2 La protección de la persona que está detrás de esta información o dato.

competitividad, amenanzas 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)[3], 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"[4] 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 libertad individual, incluso en contextos de corrupción económica y política.

El documento borrador, 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.

1.1 Grupos vulnerables

Aunque en los anexos se menciona una política de protección de la niñez en el entorno en línea, no se aborda adecuadamente la protección de otros grupos vulnerables, como defensores de derechos humanos[5], periodistas[6], activistas, opositores políticos y otras personas.

Uno de los grupos más expuestos a la violencia en línea son las mujeres, que representan la mitad de la población paraguaya, y que no están siendo suficientemente protegidas por este Plan.

3 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

4 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

5 TEDIC (2024) Ciberseguridad en defensoras y defensores de Derechos Humanos. https://www.tedic.org/wp-content/uploads/2024/10/Ciberseguridad-en-DDHH-en-Py-WEB.pdf

6 TEDIC (2023) La violenccia digital de género a periodistas en Paraguay. https://www.tedic.org/la-violencia-digital-de-genero-a-periodistas-en-paraguay/

Es importante recordar la resolución del Consejo de Derechos Humanos de la ONU, aprobada el 29 de junio de 2012, que establece que "los mismos derechos que tienen las personas fuera de línea deben ser protegidos en línea, especialmente la libertad de expresión, aplicable sin importar las fronteras y por cualquier medio elegido"[7].

En resumen, es necesario revisar la agenda de ciberseguridad a la luz de las normas de derechos humanos y sus valores fundamentales.

1.2 Políticas criptográficas

El desarrollo de este punto en el Plan debe incluir políticas de cifrado para proteger las comunicaciones y la navegación en Internet, asegurando el derecho a la privacidad e intimidad de los usuarios. 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".

1.3 Fomentar la anonimización de las personas usuaria 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[8], que ha demostrado ser más eficaz en la 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

---

7 Human Righs Council, ONU. (2012, junio 29). Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. http://ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc

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

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.

1.4 Fomento de la notificación a las personas usuarias

Es fundamental promover la notificación a los usuarios en caso de que sus datos personales hayan sido accedidos[9]. 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.

1.5 Se prioriza ratificar el segundo protocolo de Cibercrimen pero no se prioriza contar con una ley de protección integral de datos personales

El borrador de la estrategia 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 de protección integral de datos personales, un área fundamental en la era digital. La protección de datos personales no solo es un derecho fundamental de los ciudadanos, sino también un pilar clave para la confianza en la infraestructura digital y el ejercicio de la privacidad en línea.

El hecho de que no se observe un compromiso explícito en el borrador respecto a la creación o priorización de una ley de protección de datos personales es preocupante. La falta de una normativa integral en este ámbito expone a los usuarios a riesgos como la recopilación, el uso indebido y la exposición de su información personal sin garantías claras de protección. En contraste, el esfuerzo por ratificar el segundo protocolo de Cibercrimen, aunque importante para la

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

cooperación internacional en la lucha contra el cibercrimen, no aborda directamente estos aspectos de protección individual que son esenciales para un entorno digital seguro y confiable.

Una ley de protección integral de datos personales debería ser prioritaria, ya que regula cómo las instituciones públicas y privadas manejan los datos de los ciudadanos, asegurando transparencia, derechos de acceso, rectificación, cancelación y oposición (derechos ARCO), y sancionando las infracciones.

El hecho de que la estrategia de ciberseguridad solo mencione acciones vinculadas a la ratificación del protocolo de Cibercrimen, sin un paralelo claro con la creación de una legislación de protección de datos, 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 los ciudadanos. Este desbalance puede tener implicaciones negativas para la confianza en el sistema digital del país, ya que los usuarios no solo necesitan protección contra delitos informáticos, sino también garantías de que sus datos personales serán manejados de manera responsable y segura.

Por lo tanto, es crucial que se reevalúe la estrategia de ciberseguridad, asegurando que se prioricen ambos aspectos de manera simultánea: la ratificación de instrumentos internacionales como el segundo protocolo de Cibercrimen y, al mismo tiempo, el desarrollo de una legislación nacional clara y efectiva para la protección de los datos personales, que forme parte integral de una política de ciberseguridad que considere tanto la defensa contra amenazas externas como la protección de los derechos individuales.

2) Cambiar de una narrativa de crisis hacia una narrativa positiva

La narrativa de crisis inminente, reforzada por los datos de incidentes presentados en el borrador, genera un lenguaje alarmista que oscurece la necesidad de abordar de manera objetiva los riesgos reales. Esta insistencia en un discurso de crisis ya se evidenció en el plan de ciberseguridad anterior. 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[10], daños ambientales, propiedad intelectual, daño a la reputación entre otros.

El borrador de la estrategia tampoco señala que la mayoría de los problemas de infraestructura tienen su origen 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.

3) Enfoque meramente de ataques (negativo)

A lo largo del documento se presentan diversos gráficos y datos sobre los ataques identificados en el país. Sin embargo, el borrador aborda la seguridad desde un enfoque predominantemente negativo, asociándola con la mera ausencia de daño. Este planteamiento limita la comprensión del concepto. En un sentido más amplio y sustantivo, la seguridad es un valor positivo: implica la

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

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, la política de seguridad en Internet 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 no solo fortalece la protección individual, sino que también contribuye a implementar "soluciones" que reduzcan las amenazas a los derechos humanos, pilar esencial de cualquier sistema democrático.

4) 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[11][12]. Esto se agrava con el almacenamiento de datos ciudadanos mediante tecnologías cada vez más accesibles, no solo para el gobierno, sino también para empresas privadas y grupos delictivos[13]. Existen antecedentes de la compra de software de vigilancia por parte del Estado paraguayo[14][15]

La estrategia 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.

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.

---

11 Wikipedia. PEGASUS https://en.wikipedia.org/wiki/Pegasus_Project_(investigation)

12 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/

13 TEDIC (2022) Vigilancia policial en manifestaciones en Paraguay https://www.tedic.org/manifestaciones-libres-guia-sobre-la-vigilancia-policial-en-manifestaciones-en-paraguay/

14 TEDIC (2016) Espionaje a periodistas por parte del Estado paraguayo. https://www.tedic.org/espionaje-a-periodista-confirma-que-el-estado-intercepta-comunicaciones-ilegalmente/

15 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/

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"[16]

4) Protección a los divulgadores de seguridad digital

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[17]. 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 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

16 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

17 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/

existen para asegurar que no sea perseguida por hacerlo? Sin estas protecciones, se desincentiva una contribución esencial para la seguridad digital.

5) Comentarios sobre la metodología del diseño de la estrategia

La metodología utilizada para la elaboración de la estrategia requiere una revisión. Aunque el documento menciona la realización de consultas y mesas de trabajo, los temas y ejes centrales no fueron definidos de manera conjunta. No se logró un consenso sobre cuáles acciones deben ser prioritarias, deseables o urgentes.

Además, las reuniones se llevaron a cabo de forma aislada, sin permitir la interacción entre los distintos actores involucrados, como el gobierno, empresas y sociedad civil. En nuestro caso, nos agruparon exclusivamente con la academia en todas las consultas, lo que limitó la diversidad de perspectivas y el intercambio de ideas. Esto no cumplió con los estándares necesarios para un proceso verdaderamente inclusivo y participativo.

Es fundamental adoptar una metodología de consulta abierta y basada en un enfoque “multitakeholder” que fomente el diálogo directo entre todas las partes interesadas, asegurando que sus voces sean escuchadas e integradas de manera equitativa en la toma de decisiones.

6) Limitaciones del enfoque sobre aspectos laborales y sus demandas

La formación y el reclutamiento en el área de ciberseguridad deben ir más allá de perfiles técnicos provenientes de carreras informáticas. Es fundamental incorporar aspectos de diversas disciplinas, como la salud mental, el impacto ambiental y la violencia de género facilitada por la tecnología. Estos problemas, que afectan directamente al entorno digital, requieren una visión integral que aborde tanto la protección de datos como el bienestar social de los usuarios. La capacitación en psicología y salud mental es esencial para gestionar problemas como el acoso en línea y los trastornos derivados del uso excesivo de las tecnologías.

Además, la sostenibilidad ambiental es un tema clave que debe ser considerado dentro de la ciberseguridad. Las infraestructuras tecnológicas tienen una huella ecológica considerable, y los profesionales de la ciberseguridad deben ser conscientes del impacto ambiental de las tecnologías. Integrar conocimientos de ciencias ambientales en la formación permitirá desarrollar prácticas responsables y sostenibles en el manejo de la infraestructura digital, reduciendo su impacto negativo en el medio ambiente.

Otro aspecto importante es la violencia de género en línea, que se ha incrementado con la expansión de las tecnologías digitales. El acoso sexual, la difusión de imágenes sin consentimiento y la explotación de mujeres y niñas en el entorno digital requieren una formación específica en estudios de género y derechos humanos. Los profesionales de ciberseguridad deben estar

preparados para crear un entorno digital más inclusivo, seguro y equitativo, protegiendo a las víctimas y promoviendo políticas preventivas.

Finalmente, la regulación legal es fundamental para gestionar la privacidad, el cibercrimen y los derechos digitales de los ciudadanos. La formación de expertos en ciberseguridad debe incluir conocimientos jurídicos, permitiendo la creación de marcos normativos adaptados a los nuevos retos digitales. Este enfoque interdisciplinario hará que la ciberseguridad no solo proteja redes y datos, sino también que sea capaz de enfrentar los desafíos sociales, económicos y éticos que surgen con el avance de las tecnologías.

7) Limitaciones de enfoque sobre las inversiones en investigaciones sobre ciberseguridad

El enfoque de fomentar la investigación y el desarrollo en ciberseguridad, tal como se presenta en la estrategia actual, presenta una limitación importante al no incluir un análisis profundo de los perpetradores de ciberataques, sus impactos sobre la población y las necesidades específicas de las víctimas. La ciberseguridad no debe verse únicamente desde la perspectiva técnica, sino también desde el impacto social y humano que estos ataques generan. Es fundamental que la investigación en este campo no solo se concentre en proteger infraestructuras, sino también en comprender el contexto de los atacantes, sus motivaciones y los efectos que sus acciones tienen sobre las personas, especialmente los grupos vulnerables.

Este año, en TEDIC, publicamos una investigación sobre cómo los ataques que utilizan tecnología impactan a los defensores y defensoras de derechos humanos, quienes son objetivos frecuentes de amenazas digitales, acosos y campañas de desinformación[18]. Estos ataques no solo afectan la seguridad de los datos, sino que también ponen en peligro la libertad de expresión, el acceso a la información y la defensa de los derechos humanos. Esta investigación subraya la necesidad urgente de que el Estado, junto con las políticas de ciberseguridad, aborden la problemática desde un enfoque de derechos humanos, garantizando la protección de los activistas, periodistas y defensores que trabajan en entornos de alta vulnerabilidad.

La falta de un enfoque que contemple el impacto de estos delitos sobre las personas y su entorno social impide que se desarrollen soluciones eficaces basadas en evidencia. Es necesario que la estrategia de ciberseguridad del país reconozca la complejidad del panorama y trabaje en la creación de marcos de investigación que no solo busquen fortalecer la infraestructura, sino también proteger los derechos fundamentales de los individuos y colectivos en riesgo. Esto debe incluir una cooperación más estrecha entre entidades de derechos humanos, gobiernos y organizaciones de la sociedad civil, para generar políticas de ciberseguridad que estén alineadas con principios de justicia y equidad.

18 TEDIC (2024) Ciberseguridad en defensoras y defensores de Derechos Humanos. https://www.tedic.org/wp-content/uploads/2024/10/Ciberseguridad-en-DDHH-en-Py-WEB.pdf

8) Modelo desactualizado de gobernanza

Actualmente, desde la OCDE, se propone un modelo de gobernanza que incluya a todos los interesados e involucrados y que les dé herramientas a estos para gestionar y prevenir sus propios riesgos, y donde el Gobierno tenga una labor de coordinar y proponer modelos de análisis de riesgo. Es decir, una visión dinámica con múltiples actores, en contraposición a una visión estática con un solo y poderoso protagonista. Lamentablemente, la propuesta de mintic, se limita ha hacer un inventario de infraestructura.

El informe de la OCDE, “Políticas de Banda Ancha para América Latina y el Caribe[19]”, en su capítulo 14 sobre gestión del riesgo digital, establece que el objetivo de una estrategia nacional 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 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 buscan “mejorar la seguridad digital de las actividades críticas”[20]. 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 la infraestructura crítica a abarcar también la seguridad nacional en múltiples sectores. 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 borrador de la estrategia 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 y CERT, 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[21] o ataques infraestructura crítica[22]) entre otros.

---

19 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

20 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

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

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. Además, la extrapolación de metodologías de seguridad digital a otros ámbitos de la gobernanza digital, como lo hace el borrador de la estrategia, es contraproducente.

En las políticas de seguridad digital, la seguridad nacional juega un papel central, pero requiere controles y mecanismos de rendición de cuentas para evitar abusos. El borrador de la estrategia no es claro al definir si es una política de seguridad digital nacional ni establece mecanismos de control y seguimiento adecuados.

8.1 La gobernanza de la ciberseguridad está unicamente centrada en el Estado y sus comités

Si se trata de una política nacional de seguridad digital, 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 de la estrategia, a todos los niveles (incluidos los operativos), debe incluir espacios de participación y colaboración con las diversas partes interesadas.

En línea con los comentarios generales, las políticas nacionales de seguridad digital deben abordar la complejidad de coordinar diversos sectores con intereses y regulaciones muy variados. Las recomendaciones más recientes de la OCDE (2021) sobre cómo “Mejorar la seguridad digital de las actividades críticas”[23] 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

22 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/

23 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

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 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."

¿Cuál es el modelo paraguayo? ¿Cuáles son sus pros y contras? ¿Cómo los potencian y mitigan? nada de eso se explica en el documento justificativo del borrador de la estratégia de Ciberseguridad.

9) Definiciones erroneas conceptuales, vagas y amplias

9.1 Falta de unificación de conceptos: ciberdelitos, delitos cibernéticos, delitos informáticos

Se han identificado errores que podrían generar confusión tanto en la lectura como en la implementación del documento, especialmente debido a la ambigüedad en el uso de términos como "delitos informáticos", "ciberdelitos" y "delitos cibernéticos". Sería recomendable clarificar y unificar estos términos para evitar interpretaciones erróneas. Por ejemplo, la pornografía infantil no debe considerarse un "delito informático", sino un delito grave en sí mismo. De igual manera, la estafa a través de redes sociales o el phishing no encajan dentro de la categoría de "delitos informáticos". Sin embargo, el acceso remoto no autorizado a un sistema informático sí debe ser clasificado como un delito informático.

9.2 Definición sobre los servicios esenciales es vaga y amplia

El enfoque va más allá de la infraestructura crítica al incorporar el concepto más amplio de "servicios esenciales", pero no logra darle el foco necesario. La definición resulta demasiado amplia, y aunque reconoce la importancia de la prosperidad económica y social, no desarrolla este aspecto en profundidad.

La guía "Going Digital" de la OCDE[24] proporciona información relevante sobre este tema: "La noción de infraestructura crítica surgió a finales de la década de 1990, cuando algunos países de la OCDE comenzaron a adoptar políticas de protección de infraestructuras críticas (PIC). Estas políticas abarcaban sectores como energía, finanzas, telecomunicaciones y salud pública. Con el tiempo, se hizo evidente la necesidad de proteger los sistemas de información que respaldan estos sectores, lo

24 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

que llevó a la creación del concepto de 'infraestructuras críticas de información' (ICI). Sin embargo, la dificultad para delimitar las ICI ha obstaculizado su integración en marcos políticos nacionales."

La política debe aclarar la distinción entre infraestructura crítica y el ámbito de la información, que actualmente se alinea con el concepto de actividades críticas o servicios esenciales. Según la OCDE: "La noción de actividad crítica se centra en el riesgo para la prestación de servicios y no en los activos subyacentes. Una actividad crítica es aquella cuyo fracaso tendría consecuencias graves para la salud, la seguridad, la protección de los ciudadanos, el funcionamiento de servicios esenciales, o la prosperidad económica y social."

Es crucial reemplazar el término "infraestructura crítica" por "actividad crítica", tal como lo sugiere la OCDE. Esto incluye actividades que, aunque no esenciales para el funcionamiento inmediato de la economía, son fundamentales para la prosperidad social y económica, como la fabricación de automóviles o la minería en países donde estas actividades representan una parte significativa del PIB.

10) Seguridad por diseño

El plan debe priorizar 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 plan 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 plan debe incluir medidas para desincentivar a los fabricantes que comprometan la seguridad de los usuarios, 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.

11) Comentarios de estilo en el documento

Página 11:

Es importante respaldar la afirmación sobre el aumento del porcentaje de usuarios de Internet del 74.7% en 2022 al 78.1% en 2023 con fuentes verificables. Además, se debería incluir una limitación de la muestra utilizada, ya que no se especifica si los usuarios se conectan a través de una conexión a Internet con tarifa plana o solo por acceso gratuito a aplicaciones como WhatsApp. Esta omisión es relevante, ya que las limitaciones en el acceso a Internet pueden afectar el desarrollo de habilidades digitales. Esta situación impacta directamente las políticas de ciberseguridad, ya que, si CONATEL no sanciona el abuso del principio de neutralidad de la red por parte de los ISP[25], la precarización del acceso continuará. Como resultado, las políticas y planes del MITIC no llegarán efectivamente a la población más vulnerable, que no tiene acceso a paquetes de datos adecuados. Es esencial abordar las barreras relacionadas con la capacidad adquisitiva y las habilidades tecnológicas, aunque no se considere en esta medición.

Página 13:

Se sugiere reemplazar la palabra “firmó” por “ratificó” en relación a Paraguay, ya que la firma es solo el primer paso para mostrar interés en un instrumento internacional, pero es el Congreso quien ratifica el acuerdo, otorgándole fuerza de ley. Por lo tanto, la palabra “ratificó” es más precisa una vez que el instrumento es vigente y tiene efectos legales.

Se propone incluir y definir la apropiación digital como un proceso social intencionado, en el que diferentes actores colaboran para intercambiar y modificar conocimientos, implicando activamente a las personas usuarias en la adaptación de estas herramientas a sus realidades. A diferencia de la simple popularización impuesta por entidades gubernamentales o algoritmos, la apropiación digital es un proceso en el que las personas usuarias juegan un papel protagónico.

Por otro lado, el acceso a internet debe entenderse más allá de la conectividad técnica. Un acceso real implica no solo la conexión, sino también la capacidad de modificar tecnologías, comprender su funcionamiento y acceder a contenidos relevantes. La “barrera de los usos” hace referencia a la habilidad de las personas para aprovechar efectivamente las TIC en su vida diaria.

Página 53:

En el bloque sobre datos personales se cita una ley que fue derogada en 2021 (Ley N° 1682/2001, que reglamentaba la información de carácter privado). Por lo tanto, se sugiere eliminar dicha referencia.

25 TEDIC (2018) Zero rating es una forma de precarizar internet. https://www.tedic.org/zero-rating-es-una-forma-de-precarizar-internet/