Comentarios al Borrador del plan de ciberseguridad 2016

TEDIC

TECNOLOGÍA & COMUNIDAD

Problemas serios y desafíos que tiene el Plan de Ciberseguridad en Paraguay

Junio de 2016

Sumario

La definición de ciberseguridad....3

El enfoque negativo....4

Narrativa de crisis hacia una narrativa positiva....4

Vigilancia masiva....5

Relaciones internacionales....5

Hacktivismo....6

Protección a grupos vulnerables....9

Lo público y lo privado....9

Gobernanza de Internet....9

Seguridad por diseño....10

Errores conceptuales....11

Metodología de trabajo....11

Bibliografía....12

Este documento ha sido desarrollado por la ONG TEDIC a partir de su participación en el grupo de la sociedad civil para el desarrollo del Plan de Ciberseguridad en Paraguay, liderado actualmente por la Secretaría Nacional de Tecnología y Comunicación (SENATICs), con el apoyo de la Organización de los Estados Americanos (OEA).

La definición de ciberseguridad

Si bien utilizamos la definición de ciberseguridad en el entorno internacional de la Unión Internacional de Telecomunicaciones (ITU), cada Estado tiene intereses distintos, ya sea sobre cómo se va a regular una actividad, sobre cuál debería ser su conceptualización y alcances, y sobre qué actividades podrían constituir delitos. Por eso llegar a un acuerdo sobre una definición resulta una tarea compleja y se deben considerar múltiples factores.

El concepto está en pleno desarrollo a nivel mundial y una definición específica ocultaría el hecho de que el concepto, es objeto de disputas entre diferentes miradas, perspectivas e intereses.

Por otro lado, esta variación en la definición, ha permitido la incorporación de diversos temas en discusión: agendas políticas, estabilidad del Estado, seguridad de las aplicaciones y servicios, seguridad de los usuarios, seguridad de infraestructura nacional, infraestructura de Internet, entre otros. Eso arroja como resultado una mezcla de objetivos legítimos y preocupaciones secundarias, fusionando tipos y niveles de riesgos en un mismo objetivo.

Por su parte, la Relatoría Especial para la libertad de expresión de la Comisión Interamericana de Derechos Humanos (CIDH), de la Organización de los Estados Americanos (OEA), estableció en su publicación "Libertad de expresión e Internet" lo siguiente:

"*El concepto de ciberseguridad suele emplearse como un término amplio para referirse a diversos temas desde la seguridad de la infraestructura nacional y de las redes a través de las cuales se provee el servicio de Internet, hasta la seguridad o integridad de los usuarios. No obstante, desarrollo posteriores sugieren la necesidad de limitar el concepto exclusivamente al resguardo de los sistemas y datos informáticos (…) este enfoque acotado permite una mejor compresión del problema así como una adecuada identificación de las soluciones necesarias para proteger las redes interdependientes y la infraestructura de la información*"[1]

Actualmente el plan de Paraguay tiene un enfoque del daño: citando incidentes cibernéticos, crímenes, negligencias y ataques de delincuentes, y todo esto mitigado por programas de Educación. Sin embargo, el núcleo esencial debería ser la confidencialidad, integridad y disponibilidad de la información como la clave del componente técnico en la definición de Ciberseguridad.

El contexto es importante para su definición; la misma debe se matizada y escalonada contemplando disposiciones, actores y tipo de riesgos. También debe incluir el enfoque de Derechos Humanos (en particular los derechos de intimidad, privacidad y libertad de expresión), así como el enfoque económico, siendo ambos parte del núcleo de la definición. Es necesario una aproximación holística a la política de ciberseguridad.

Por tanto la falta de terminología clara, que ilumine y permita establecer alcances y limitaciones de las acciones del estado podría tener desafortunadas derivaciones e implicaciones. Por ejemplo la superposición e incluso contradicción en criterios de implementación entre las diferentes reparticiones, la adopción de medidas discrecionales

1 OEA. CIDH. Libertad de expresión e Internet. 31 de diciembre de 2013. Disponible en PDF.

por parte de funcionarios de turno sin ningún tipo de control o supervisión, el mantenimiento de prácticas opacas y falta de transparencia, entre otros. En definitiva se puede generar un escenario propicio para la vulneración de los derechos humanos.

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) ha modificado el término de Ciberseguridad a Seguridad Digital en el Plan Nacional de Seguridad digital de Colombia, que en su primera parte fue desarrollado con el apoyo de la Organización de Estados Americanos (OEA). Sería interesante analizar esta experiencia, ya que el Gobierno actual de Paraguay está trabajando firmemente en formar parte de esta organización[2].

El enfoque negativo

El problema de seguridad en el borrador del plan se plantea con un enfoque negativo: la seguridad no tiene necesariamente que referirse a la ausencia de daño. En un sentido sustantivo, la seguridad es un concepto positivo: que se refiere a la capacidad de una persona a acceder a un recurso fundamental y utilizarlo de acuerdo a sus necesidades y preferencias. Desde la óptica de los Derechos Humanos, la seguridad se centra en la capacidad de las personas de actuar libremente de forma responsable. La política de seguridad en Internet no debería limitarse a desempeñar un papel defensivo, sino uno facilitador, y que potencie el bienestar de las personas como eje central. De esta forma se aseguran "soluciones" con menos amenazas a los derechos humanos, estructura central de los sistemas democráticos.

Narrativa de crisis hacia una narrativa positiva

La narrativa de inminente crisis en el borrador genera un lenguaje cargado, de sensación de alarma y que a la vez nubla la necesidad objetiva y evidente de fundamentar los peligros que nos ocupan.

Esta insistencia con la crisis se repite en otros planes de ciberseguridad, y muchos gobiernos a nivel mundial están siendo cuestionados por utilizar estas "amenazas" internas y externas como argumentos para justificar cada vez una mayor inversión en ciberseguridad, con énfasis en sistemas de vigilancia masiva, y aumentar así el control de Internet y de las personas.

Además confunde el debate al combinar diferentes retos:

> i) Por un lado se cita *la amenaza* donde la tecnología es parte integral del riesgo. Es decir se refiere a ataques a la infraestructura crítica, ataques DdoS, espionaje, daño o acceso indebido a datos, a equipos o a redes.
>
> ii) Por otro aparecen *las amenazas*, en que la tecnología es simplemente un medio. Ejemplos de esto serían la pornografía infantil, la distribución de correos no deseados, la planificación del robo a un banco, etc..

En estos últimos casos, el riesgo no es la infraestructura, sino la comunicación en sí y la naturaleza del contenido. Si bien la tecnología puede cambiar la naturaleza o el alcance de estos delitos o crímenes, no es parte integral de la definición de ciberseguridad.

En nuestra opinión, es clave cambiar la narrativa actual hacia una narativa positiva - "human centered approach", enfocandose hacia el desarrollo de una política de protección de las personas en linea y fuera de ella (offline) por parte del Estado paraguayo.

---

2 La Nación- Fecha 10 de mayo de 2016. http://www.lanacion.com.py/2016/05/10/cartes-viaja-paris-junio-para-lanzamiento-cooperacion-oecd/

Y por último, creemos que es importante indicar los riesgos creados por un lado, por el Estado y los diferentes organismos y por otro lado, el sector privado a través de sus políticas y prácticas de vigilancia (backdoors, acceso directo etc) y el mantenimiento incorrecto de los sistemas (vulnerabilidades, no usan https, etc).

Vigilancia masiva

Dentro de las problemáticas a la seguridad, no se menciona los riesgos que implican la adquisición de herramientas de vigilancia masiva. A esto se suma el problema del almacenamiento de datos de los ciudadanos con herramientas que cada vez son mas fáciles de adquirir, tanto por el gobierno como las empresas privadas o grupos delictivos. Los casos de la empresa italiana *HackingTeam* y la empresa anglo-germana *Gamma Internacional* publicados en Wikileaks y CitizenLab sobre Paraguay, exponen a nuestras instituciones de persecución penal como clientes frecuentes.

El Plan de Ciberseguridad debe abarcar este tema desde un *análisis bidireccional*: por un lado las agencias y dependencias gubernamentales, deben tener la posibilidad de adquirir herramientas para la persecución de los hechos punibles, siempre que su alcance y uso sean regulados legalmente con un enfoque de derechos. En el otro sentido el Plan debería adelantar un estudio de mejores prácticas respecto de los marcos legales y regulatorios a nivel internacional en torno a i) la protección de la privacidad y los datos personales y a ii) los derechos humanos, el derecho internacional humanitario y los valores fundamentales. También hace falta incorporar la notificación a las partes cuando su información se ve comprometida: para la verificación por la parte afectada y realizar las denuncias en caso de abuso de Instituciones del Estado o empresas privadas.

Finalmente, la relatoría especial de Libertad de expresión e Internet de NNUU expresa:

> "*las respuestas de los Estados en materia de seguridad en el ciberespacio debe ser limitada y proporcionada, y procurar cumplir con fines legales precisos, que no comprometan las virtudes democráticas que caracterizan a la red".*

Relaciones internacionales

También debe incorporarse el esquema de relaciones internacionales, por ejemplo las amenazas de estados *"opositores"*[3]. La adquisición de tecnología de vigilancia también pone en riesgo a todas las partes involucradas. En este sentido es evidente el papel fundamental de la ciberseguridad en relación a la protección de la infraestructura que manejan información y datos sensibles, entre otros.

Como ejemplo, podría citarse un escenario ficticio en que Argentina y Brasil deciden aislar a Paraguay, cortando los dos accesos principales a Internet. Este tipo de problemas deberían plasmarse en el Plan.

Asimismo, creemos desde TEDIC, que es importante hablar sobre el escenario internacional de las "Cyberguerras" y su posicionamiento con relación a esto: pero debe estar en el cuerpo central del plan y no en los anexos. Si bien este término no se encuentra definido, lo importante es tener en cuenta este tipo de situaciones para el desarrollo del Plan.

3 Ejemplo: Rusia-USA, y empresas privadas compiten entre si para esta "clientela"

Hay indicios de que algunos gobiernos han invertido en el desarrollo de programas llamados "Brazos" cibernéticos para ataques ofensivos. Esta tendencia es preocupante desde una perspectiva de derechos humanos, porque conduce al límite de las libertades civiles, ya que los gobiernos argumentan que los límites son necesarios para promover la seguridad a través de las "armas" que podrían desarrollarse, causando daños reales a la arquitectura de Internet. Esto que socava los derechos de los individuos para el uso y la obtención de las prestaciones correspondientes.

Un ejemplo de situaciones de Ciberguerra es el caso de Stuxnet, un virus responsable de sabotear los centrifugadores involucrados en el programa de enriquecimiento de uranio de Irán. Fue probablemente el primer malware diseñado específicamente para infectar equipos industriales que se propagó en forma masiva. Se cree que Stuxnet fue diseñado y propagado con el apoyo de las agencias estatales de EEUU e Israel[4]. El ex-Director del Centro Antiterrorismo de la CIA anunció en una conferencia que Stuxnet marcó "Rubicón de nuestro futuro", admitiendo implícitamente la participación de la agencia en Stuxnet.

Internet es un sistema interconectado, que recibirá el impacto de cualquier llamada guerra cibernética. Cabe rescatar que el Grupo Internacional de Expertos convocado por la OTAN (Manual de Tallin) han realizado los primeros intentos para aplicar los derechos humanos en el espacio en línea[5]. Paraguay debe contemplar y planificar la forma en que se aplican los derechos fundamentales en situaciones de guerra cibernética, asumiendo un liderazgo en la despolarización de la gran escalada de la carrera de armas cibernéticas.

Hacktivismo

El término[6]. "hacktivismo", está mal utilizado y poco fundamentado. El "hacktivismo" aparece a lo largo y ancho del planeta como forma de protesta, a menudo en defensa de los derechos humanos. Es una forma de libertad de expresión que se opone a veces al Gobierno, aunque no siempre. Por ejemplo, en 2015 se realizó una Hackatón Parlamentaria[7] en el Senado, en la que muchos activistas de reunieron para encontrar soluciones ingeniosas a problemas de los sistemas de información del Congreso.

El borrador del Plan de Ciberseguridad plantea el hacktivismo como algo exclusivamente negativo, sin presentar ningún tipo de evidencias.

Políticas de Derechos Humanos

En términos generales aparecen conceptos relacionados con derechos humanos, sin embargo en el Plan no contempla los mecanismos y políticas para la defensa de la privacidad y libertad de expresión de los usuarios.

El Estado debe garantizar la seguridad de las personas dentro de sus límites: las estrategias de seguridad digital y ciberseguridad deben ser diseñados e implementados de manera consistente con el derecho internacional de los derechos humanos. Es decir el derecho a la

---

4 Kim Zetter "How Digital Detective Deciphered Stunex, the most menacing Malware in History", Wire, 11 de julio 2011. https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet

5 NATO Cooperative Cyber Defence, & Centre of Excellence Tallinn. (2013). Tallinn Manual Process. Recuperado a partir de https://www.ccdcoe.org/tallinn-manual

6 Cory Doctorow, Pirate Bay to Anonymous: DdoS is censorship, cut it out, BoingBoing 1 May 2012. Y Jay Leierman, Justicie for the PayPal Wikileaks protesters: why DdoS is free speech, The Guardian, 22 de enero 2013.

7 https://ejempla.com/futuro/hackearon-el-parlamento

privacidad es un componente necesario en el desarrollo de una ciudadanía centrada en la política de seguridad. Estos términos deben ser explicitados en el plan tanto en su desarrollo como en sus anexos.

Un ejemplo de ello sería la protección de la población por medio de *políticas de criptografías*: implementar como prioridad el uso del cifrado de las comunicaciones y promover herramientas de criptografía, para que sean más accesibles y fáciles de usar.

La "Autenticación" se presenta como otro problema difícil de resolver, ya que presenta riesgos importantes para las personas: la política debería orientarse a desarrollar e implementar alternativas seguras a las contraseñas.

Derechos humanos y las obligaciones de los Estados.

Para el desarrollo de esta política se deberá tener en cuenta la Resolucion de 2012 del Consejo de Derechos Humanos de la ONU sobre *"online and offline" rights*[8]. Además mejorar el discurso de seguridad que tiene el Plan, hacia un conceptualización mas amplia que integre la protección de los derechos humanos.

Crear iniciativas no solo nacionales, sino regionales o globales para la evaluación de impactos de los derechos humanos. Que incluyan las diferentes etapas de la implementación del Plan: inicio, durante el periodo de ejecución y final, desarrollar buenas prácticas y aprendizajes de los que ha funcionado o no, entre otros.

Y por último recomendamos una lectura regional de esta situación. Y solicitar al programa de ciberseguridad de la OEA a consultar y colaborar con otras dependencias de la misma organización para que sus recomendaciones estén alineadas con los estándares en materia de libertad de expresión y derecho a la intimidad elaborados por la Comisión y la Corte Interamericana de Derechos Humanos y la Relatoría Especial para la Libertad de Expresión de la CIDH.

Políticas Criptográficas

El desarrollo de esta punto en el Plan, debe estar contemplado a través de políticas de cifrado de las comunicaciones y navegaciones en Internet para la protección del derecho a la privacidad e intimidad de los usuarios. Podría ser a través de talleres de privacidad para cifrar por ejemplo el disco externo o duro de los dispositivos de los usuarios.

Es importante resaltar que la criptografía es una parte integral de muchos/todos los sistemas como por ejemplo sistema bancario, e-commerce entre otros, por lo que no puede ser limitado solamente a ciertos grupos, sino debe abarcar a todos las personas[9]. Una navegación o comunicación que no esté cifrado, no es que simplementemente se lo vea como "poco cifrado" sino que significa que está abierta a las "puertas traseras" para todos[10].

Fomentar la anonimización del usuario en Internet y salvaguardas nacionales

---

8 Consejo de NNUU, 2012. https://documents-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement

9 Privacy Internacional, Seguring Safe Space Online. June 2015 https://www.privacyinternational.org/sites/default/files/Securing%20Safe%20Spaces%20Online_0.pdf

10 Privacy Internacional, The pincer movement against encryption. 2015 https://www.privacyinternational.org/node/641

El anonimato en la Internet es un mecanismo que habilita la libertad de expresión. David Kaye, relator especial para la libertad de expresión de NNUU, en su informe sobre la importancia de la encriptación y el anonimato para la libertad de expresión, y manifestó lo siguiente: "*la encriptación y el anonimato proporcionan la privacidad y la seguridad necesarias para el ejercicio de la libertad de opinión y de expresión en la era digital*"[11].

Siguiendo esa premisa, el relator recomienda, entre otras cosas, que "*las legislaciones nacionales deben reconocer que los individuos son libres de proteger la privacidad de sus comunicaciones digitales mediante el uso de tecnologías de cifrado y herramientas que permiten el anonimato en línea*[12]". Y destaca que incluso se debe promover el acceso a estas herramientas y tecnologías. Según Kaye, los debates sobre cifrado y anonimato han sido polarizados en el discurso acerca de su uso criminal potencial, pero que el debate tiene que cambiar para destacar también la protección que ofrecen la encriptación y el anonimato, especialmente para los grupos que viven en situaciones de riesgo de interferencia ilegal de sus comunicaciones. Asimismo incluir políticas de buenas prácticas y salvaguardas nacionales que socaven activamente y directamente el cifrado y otros sistemas utilizados por los usuarios para protegerse. Por tanto es importante que el Plan incluya estas recomendaciones con enfoque de derechos.

Hace falta explicitar un fuerte apoyo a la política de SENATICs de promoción de software libre y código abierto. Se ha demostrado que la seguridad por transparencia es más eficaz y permite solucionar los fallos de seguridad con mayor velocidad[13]. Por otra parte, cualquier política criptográfica debe basarse necesariamente en el código abierto.

Fomentar la notificación a los usuarios

El fomento de las notificaciones a sus usuarios si sus datos personales fueron accedidos con el tiempo y la información suficiente para que puedan impugnar la decisión o buscar otras soluciones y deben tener acceso a los materiales presentados en apoyo de la solicitud de autorización. La obligación de notificar recae en el Estado, pero los proveedores de servicios de comunicaciones debe tener la libertad de notificar a las personas.

El retraso en la notificación solo se justifica en las siguientes circunstancias[14]*:*

1. *La notificación pondría en serio peligro la finalidad para la que se autoriza la vigilancia, o existe un riesgo inminente de peligro para la vida humana; y*
2. *La autorización para retrasar la notificación es otorgada por la autoridad judicial competente en el momento en que se concede la autorización para la vigilancia; y*
3. *El usuario afectado se notifica tan pronto como el riesgo desaparece según lo determinado por la autoridad judicial competente.*

---

11 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

12 Idem 8.

13 Challet, D., & Du, Y. L. (2005). MICROSCOPIC MODEL OF SOFTWARE BUG DYNAMICS: CLOSED SOURCE VERSUS OPEN SOURCE. Recuperado 2 de marzo de 2013, a partir de http://arxiv.org/pdf/condmat/0306511.pdf

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

Protección a grupos vulnerables

Si bien en los anexos aparece una política de protección de la niñez en el entorno en línea pero no se toma en cuenta otros grupos vulnerables como por ejemplo los defensores de derechos humanos, periodistas, activistas, opositores políticos y otros ciudadanos.

Un grupo vulnerable, que presenta gran riesgo ante la violencia en el entorno en línea, son las mujeres[15]: la mitad de la población paraguaya que no está siendo protegida a través de este Plan.

Vale la pena recordar la declaración aprobada por el Consejo de Derechos Humanos de la ONU, resolución del 29 de junio de 2012:

> "[…] *Los mismos derechos que tienen las personas fuera-de-línea, también deben ser protegidos en-línea, en particular la libertad de expresión, que debe ser aplicable sin consideración de fronteras y por cualquier medio que se elija [...]*"[16]

En líneas generales es necesario revisar la agenda de ciberseguridad a la luz de las normas de derechos humanos y sus valores.

Lo público y lo privado

Por otro lado el borrador no contempla las relación público-privado para el intercambio de información: desarrollo y garantías adecuadas. Solo se encuentra de manera general en el anexo numeral 6C y 6D la importancia de colaboración entre ambos sectores. Tampoco se expone en el Plan que la mayoría de los problemas de infraestructura se generan por el sector privado, por desarrollar sistemas débiles, falta de mantenimiento del hardware y software y demás vulnerabilidades. El plan debe incluir mecanismos para promover mayor intercambio entre las empresas privadas y organismos públicos para permitir una mejor respuesta a las amenazas de la seguridad en Internet con enfoque de Derechos Humanos.

Los dos sectores tienen roles importantes para detectar con éxito y controlar las amenazas. Es clave que cualquier mecanismo esté bien definido y sea sometido a escrutinio y que tenga las salvaguardas adecuadas. Por ejemplo: sanciones si se fugan informaciones personales; cuando haya abusos, reparaciones del daño, entre otros.

Gobernanza de Internet

El plan menciona la cooperación internacional pero no relaciona los esfuerzos la Naciones Unidas para generar espacios de discusión sobre ciberseguridad y gobernanza en Internet a través de sus foros mundiales y locales, y la Cumbre Mundial sobre la Sociedad de la Información (Con siglas en ingles WSIS[17]). Queda citado pero de forma general en el anexo 1: la importancia de la cooperación internacional, pero solo para soluciones de amenazas y delitos informáticos.

---

15 Ejemplos de lo que se viene realizando. Reportes ONU MUJERES. 2015 http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf

16 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. Recuperado a partir de http://ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc

17 Ver http://www.itu.int/wsis/index.html

La característica definitoria del discurso del plan es la noción de un Estado poderoso y benévolo que proporciona seguridad a sus ciudadanos, como era en la época pre-Internet. Pero este relato no concuerda mucho con la realidad de la naturaleza de la Internet, que es una red global de información y que está en gran medida en manos del sector privado. Ni las amenazas, ni las soluciones son fáciles de definir, ubicar o regular como lo fueron en épocas anteriores.

Viendo esta complejidad y sus actores a nivel local e internacional, es importante debatir sobre la gobernanza de Internet y una mayor cooperación por parte de la Comisión Nacional de Ciberseguridad en esta área. Estos foros proporcionan oportunidades para empresas, gobiernos y miembros de la sociedad civil puedan discutir soluciones y compartir conocimiento y mejores prácticas. Esto permite construir escenarios sobre los caminos a seguir y concentrarse en la no renovación del estilo tradicional de control del gobierno.

Un ejemplo de gobernanza de Internet, se da en ICANN donde el Estado se encuentra como un actor crucial y con múltiples responsabilidades, al mismo nivel que otros actores. En este espacio existe una mesa de trabajo en Ciberseguridad en la que Paraguay podría participar.

En el borrador, la comisión Nacional de Ciberseguridad no incluye a ningún actor que forma parte de la Internet como la Academia, sociedad civil, sector privado, ni comunidad técnica: solo cita en el anexo que podrían conformar mesas de trabajo.

Ron Deibert[18] —experto en ciberseguridad y director de CitizenLab de la Universidad de Toronto— propone avanzar hacia un enfoque distribuido de la ciberseguridad, que se basa fundamentalmente en los controles y equilibrios entre una variedad de actores, tanto a nivel nacional como internacional, a fin de evitar la aparición de "poder político sin control y concentrado". Lo interesante de este enfoque es que permite evitar que agentes individuales sean capaces de tomar el control, a menos que las otras *múltiples partes* estén de acuerdo y colaboren entre sí. Uno de sus puntos fuertes es que permite reconocer una vez más al usuario como un actor importante, a la vez que genera una sistema de pesos y contrapesos multi-capas.

Con el fin de abordar los temas centrales del plan, es clave el diseño de un modelo dinámico de coordinación y cooperación en que se definan roles, responsabilidades y funciones, así como una matriz de comunicación y seguimiento entre las instancias de máximo nivel del Gobierno: a) con los ministerios y departamentos administrativos de orden nacional y b) con el sector privado y la sociedad civil.

Otro preocupación es que ni en el Consejo, ni a través de sus comités, ni en los ejes de acción se plantea un órgano de control y supervisión que garantice la protección y promoción de los derechos humanos en Internet.

Seguridad por diseño

El plan debe enfatizar la seguridad desde el diseño. Si bien el anexo habla de estándares de certificación, sería importante ver que los mismos estén garantizados entre el Estado y expertos de sociedad civil y academia, y no solamente a través de una certificación de una empresa con los ISO 27001.

18 Ron Deibert, "Towards a cyber security strategy for civil society" in Alan Finlay (ed.) Global Information Society Watch 2011: Internet rights and democratization, APC & HIVOS, http://www.giswatch.org/en/freedomexpression/towards-cyber-security-strategy-global-civil-society

El verdadero desafío que enfrenta la ciberseguridad no tiene que ver solamente con el terrorismo internacional, el espionaje promovido por los Estados, o los delincuentes cibernéticos. El problema muchas veces radica en el código fuente del software y hardware que se utilizan todos los días, ya sea del sistema operativo y diversas aplicaciones. El plan debe contemplar mecanismos de solución para garantizar la seguridad de la información que vayan más allá de la instalación de antivirus para Windows.

Debe definir las medidas de seguridad y auditar los sectores críticos, para asegurar la protección de la infraestructura por parte de la Comisión Nacional, e inclusive se debería incorporar expertos de la sociedad civil para el cumpliendo el principio de supervisión pública.

Se podrían incentivar económicamente a la empresas locales que cumplan con los estándares de seguridad y protección de los DDHH, así como promover este enfoque en los diferentes centros educativos y universidades.

Un ejemplo sería desincentivar a los fabricantes locales que perjudican a los propios usuarios: cuando por ejemplo las empresas comprometen la seguridad de los mismos a través de la instalación de puertas traseras u otros mecanismos de vigilancia. Esto es muy delicado porque muchos gobiernos conocen la existencia de estas vulnerabilidades no lo denuncias porque las usan por sus propios beneficios.

Otro ejemplo, sería incentivar a las empresas y otras organizaciones a que utilicen mejores sistemas de conexión con los usuarios, como ser conexiones cifradas como https, comunicación cifrada, y autenticación de doble factor, o similiar, iniciativas de e- “smart” como smart cities entre otros deben ser cifradas.

Errores conceptuales

Encontramos errores que confunden un poco al lector y posiblemente en su implementación que es la ambigüedad en la utilización de términos como: “delitos informáticos”, “ciberdelitos” y “delitos cibernéticos”. Valdría la pena apuntar a su correcta conceptualización y unificación.

Por ejemplo, la pornografía infantil no es un delito informático. Es un delito a secas y demasiado grave. La estafa a través de una red social o de phishing tampoco lo es. Finalmente, el acceso remoto indebido a un sistema informático sí conformaría un delito informático.

Metodología de trabajo

La metodología de construcción del plan debería ser revisada: si bien el documento cita que se desarrollaron consultas y mesas de trabajo, los tema y ejes centrales no fueron definidos de forma conjunta. No hubo consenso para las acciones prioritarias, deseables o urgentes.

Es necesario que en esta segunda etapa de comentarios, las partes interesadas puedan dialogar entre sí, que haya consultorias abiertas y con metodología “multi-stakeholder”para la construcción del mejor plan posible para Paraguay.

Bibliografía

- Declaración Conjunta de la Sociedad Civil a la Organización de Estados Americanos (OEA) y a los gobiernos de los países miembros sobre temas de seguridad digital en América Latina. Marzo (2016) https://www.tedic.org/declaracion-sobre-ciberseguridad-en-america-latina/
- Frank La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" (2013) http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf
- 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
- Anonymity and encription. Comentarios entregados a la relatoria especial de promoción y protección del derecho a la libertad de expresión y opinión de NNUU. Febrero de 2015. http://www.ohchr.org/Documents/Issues/Opinion/Communications/EFF.pdf
- Recomendaciones sobre Gestión de Riesgos de Seguridad Digital para la Prosperidad Económica y Social OCDE. 17 de septiembre (2015).
- A cybersecurity a agenda for civil society, what is a stake? (2013) https://www.apc.org/en/system/files/PRINT_ISSUE_Cyberseguridad_EN.pdf
- Ryan Gallagher, cyberwar's gray market, Slate (2013),http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_mar-ket_be_regulated.html;
- Andy Greenberg, Meet the Hackers Who Sell Spies the tools to crack Your Pc (And Get Paid Six-Figure Fees), Forbes 21 March (2012)
- OECD (2012), "non-governmental Perspectives on a new Generation of national cybersecurity Strategies",oEcd digital Economy Papers, no. 212, OECD Publishing, http://dx.doi.org/10.1787/5k8zq92sx138-en, p6.
- Unpacking "cybersecurity": threats, responses, and Human Rights considerations. (2013)
- "Privacy Principles for Identity in the Digital Age" (2007) https://www.cdt.org/files/pdfs/20071201_IDPrivacyPrinciples.pdf
- Cyber Security, Cyber Surveillance and Online Human Rights http://www.gp-digital.org/wp-content/uploads/pubs/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf
- UN Human Rights Council (2012). The Promotion, Protection and Enjoyment of Human Rights on the Internet (A/HRC/20/L.13). New York, United Nations General Assembly, (2012)

- Sobre cibeseguridad en Colombia: mucho ruido y pocas nueces. (2016). https://karisma.org.co/sobre-ciberseguridad-en-colombia-mucho-ruido-y-pocas-nueces/
- Politica Nacional de Seguridad Digital de Colombia. Borrador 2015 http://www.mintic.gov.co/portal/604/articles-14481_recurso_1.pdf
- Cybersecurity: What we (may not) know we (do not) know An overview of the cybersecurity challenge. Geneva Internet Platform. Por Eduardo Gelbstein. (2013)
- Ciberseguridad en la era de la vigilancia masiva. https://adcdigital.org.ar/portfolio/ciberseguridad-la-la-vigilancia-masiva/ (2016)

Maricarmen **Sequera**
Luis Pablo **Alonzo**