Aportes a la ENC.

por Mauro D. Ríos.-

Comentario general: el documento resulta de fácil lectura, pero tiene carencias de cohesión, donde se identifican claramente secciones con estilos diferentes y en algunos casos se hace notar la falta de un hilo conductor temáticos y hasta conceptual.

4. Principios Rectores

Sugerencia de redacción del párrafo: "La ENC refleja el firme compromiso de Uruguay y de los actores del ecosistema de ciberseguridad para proteger al país, a sus ciudadanos y a sus instituciones en el ciberespacio."

Cita: "la resiliencia frente a los desafíos digitales", entiendo que se está asumiendo la resiliencia como la capacidad de adaptarse y recuperarse frente a situaciones adversas, desafíos o cambios significativos, en tal sentido la frase queda limitada en su coherencia sino se es más explícito. Sugiero algo como "…, se pretende fortalecer la capacidad de resiliencia ante los desafíos digitales que nos expongan a dificultades o cambios abruptos, para construir un futuro digital seguro y confiable para todos."

Cita: "Abarcan al sector público y privado", así como el concepto de seguridad de la información, madre de la ciberseguridad, abarca a todos los sectores de la sociedad, la ENC no puede desconocer ninguno de los sectores, por lo que debería siempre hacerse referencia a todos los sectores en cada cita en el documento, lo cual no sucede, como en este caso que falta la academia, sociedad civil, etc. (Nota: en otras pasajes si se hace mención a todos los sectores).

4.1 Centrado en las personas

El concepto de "al servicio de las personas" ha caducado de diferentes maneras, si bien obviamente entendemos de que se trata y su espíritu. La tecnología avanza de tal manera que su desarrollo deriva en tecnologías como la IA, la cual, por primera vez en la historia de la humanidad, una tecnología desarrollada por el ser humano tiene la capacidad de evolucionar por sí sola al servicio de sí misma en su perfeccionamiento, siempre supeditada a ser auxiliar y coparte del accionar del ser humano.

Por tanto, una redacción más aggiornada tal vez sea de conveniencia: "…, toda iniciativa deberá ser respetuosa de la diversidad y los derechos fundamentales, como la libertad de expresión, el acceso a la información, la preservación de la privacidad y la protección de la propiedad, con el fin de erigir una sociedad digital inclusiva y segura, basada en los principios de equidad y justicia social, donde la tecnología, como aliada, sea clave y contribuya en el desarrollo pleno de las personas en los diferentes ámbitos y roles sociales."

4.2 Enfoque holístico

Sugerencia: “La ciberseguridad se entiende hoy como un conjunto amplio y que comprende elementos y actores diversos, donde resulta transversal a diversas ciencias y disciplinas, su alcance escapa a la tecnología misma y genera estructuras complejas que requieren métodos y sistemas que faciliten una necesaria gobernanza. La toma de decisiones al respecto de la estrategia a seguir en materia de ciberseguridad implica necesariamente la participación de las múltiples partes involucradas, lo que exige coordinación y acuerdos.”

5 Pilares

Creo que es un error estratégico circunscribir la ENC al “ciberespacio”, y un error conceptual que no debería quedar plasmado así en un documento tan relevante dando a entender una idea equivocada ya que ciberseguridad, sin traer aquí la definición, abarca a todo sistema informático, redes, dispositivos, datos e informaicón en medios digitales. Lo que incluye mucho más allá de William Gibson y su novela “Neuromante”.

Tomemos por ejemplo el “Marco de ciberseguridad” o las “Políticas de ciberseguridad”, en este caso sólo 1 refiere específicamente al ciberespacio de las casi 20 que recuerdo en la Administración Central y si tomamos las de organismos como ANEP o URSEC, entre más de 15 a 20, sucede lo mismo.

De hecho, esta “delimitación” va a colidar desde el inicio con varios de los propios pilares de la ENC, donde son por naturaleza y definición más amplios que el propio ciberespacio.

Entiendo necesario subsanar este problema conceptual poniendo en sintonía el real alcance de la ENC con tal vez este y otros pocos pasajes donde se emplea el término “ciberespacio” de manera incorrecta (a mí entender).

5 Pilares – 1.Gobernanza

Reitero mis aportes sobre el punto 4, pero agregaría que, si bien es correcto mencionar el desarrollo de los mecanismo y políticas, la implementación de la Gobernanza del ecosistema de ciberseguridad muy probablemente requiera promulgación o adecuación de un nuevo marco normativo especifico al punto, decretos o leyes, por lo que agregaría este especto a la redacción.

Sugiero: “Gobernanza: Establecer los mecanismos, políticas y marco normativo legal necesarios, para la rectoría de la ciberseguridad a nivel nacional, y la definición de los roles y responsabilidades de todos los actores involucrados de los diferentes sectores de la sociedad, tanto públicos, privados, academia, sociedad civil y otros.”

5 Pilares – El pilar ausente

Si bien se hace referencia en ocasiones a lo largo del documento, no figura como pilar y creo fundamental que se incluya como principio rector de la ENC la consideración de los Derechos Fundamentales y la ética.

“9. Derechos Fundamentales: Toda iniciativa de ciberseguridad, enmarcada en la ENC, deberá cumplir estrictamente con el marco normativo vigente. Además, estas iniciativas se fundamentarán en el respeto absoluto de los derechos fundamentales, tales como la privacidad, la libertad de expresión, el acceso a la información y la diversidad. Asimismo, se garantizará que todas las acciones y políticas adoptadas sean éticas y transparentes, promoviendo una cultura de cooperación entre partes y responsabilidad social.” Obviamente luego desarrollar el pilar en el apartado específico como el resto.

Pilar 1. Gobernanza

Se utiliza el término “instaurar” en ocasiones, lo que deja la duda fundada si se refiere a una obligatoriedad o no. El término puede dar lugar a una interpretación laxa o dual, sugeriría ser explícito ya que la ENC y tomando en cuenta el fondo del asunto y lo que está en riesgo, no puede quedar librado a supuestos o doble interpretación, pero sobre todo no puede quedar, en los casos de criticidad, al voluntariado de las partes involucradas.

Ejemplo, cita: “Instaurar que la ciberseguridad sea efectivamente incorporada como un objetivo de gestión, en el gobierno corporativo, de las organizaciones relevantes,…”

Si de instituciones relevantes se trata, es decir que tienen un nivel de criticidad dentro de la infraestructura crítica de TI del país para la ciberseguridad, en estos casos la ciberseguridad y le ENC como tal, deberá estar obligatoriamente como parte de los objetivos de gestión institucionales. Sin dudas hablamos de instituciones públicas como ANTEL, URSEC, AGESIC, UTE, pero también privadas como las compañías de comunicaciones, proveedores de infraestructura tecnológica y sin dudas estarán incluidas las grandes de TI que están arribando al país.

Sugerencia: “Adecuar el marco normativo y regulatorio para establecer de manera obligatoria la ciberseguridad y la propia ENC, como parte fundamental de las líneas estratégicas organizacionales, los objetivos de gestión y en el gobierno corporativo, de las organizaciones de carácter crítico en la infraestructura tecnológica nacional, que formen parte del ecosistema de ciberseguridad del país,…”

Pilar 6. Cultura de ciberseguridad

Si bien se habla de capacitación y de desarrollar iniciativas colaborativas voluntarias por parte de la Academia y otros sectores, así como se menciona el trabajo sobre la oferta educativa, el punto puede ser reforzado desde la redacción en tanto la educación en ciberseguridad, al nivel que se desee, es clave desde la perspectiva de una sociedad con consciencia de seguridad de la información.

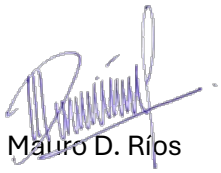
Guardando la autonomía de la Educación y otras instituciones por ejemplo a nivel de gobiernos departamentales, el involucramiento de la Educación Pública no puede ser voluntario en la ENC, la educación es pilar fundamental, tanto para la perspectiva del ciudadano común como el especializado a niveles pre y universitario, por lo que debe establecerse claramente este punto en la ENC.

Cita: “Desarrollar un programa de voluntariado para organizaciones, sociedad civil y academia, que colaboren en el fomento de la cultura de ciberseguridad en la sociedad.”

Sugiero: “Asistir a las entidades de educación pública en todos los niveles, desde la educación básica hasta la universitaria, para la incorporación definitiva de la formación en seguridad de la información y ciberseguridad en sus currículos. A nivel terciario, esta temática deberá estar incluida en los planes de estudio de todas las carreras y orientaciones, con la profundidad y desarrollo que determinen los especialistas educativos, y con el asesoramiento de instituciones técnicas públicas como AGESIC, CERTuy y SOC. En el ámbito educativo privado, se buscará promover un plan de voluntariado que permita realizar adecuaciones curriculares equivalentes.”

Cita: “Trabajar en la actualización de los programas y planes de estudios en todos los niveles (educación primaria, secundaria y terciaria), para que se incluyan aspectos de ciberseguridad asociados a su línea de estudio (derecho, diplomacia, salud, comunicación, administración, etc.)”

Sugiero: “Se trabajará con las instituciones públicas educativas, en la actualización de los programas y planes de estudio en todos los niveles educativos (primaria, secundaria, técnica y terciaria) para incluir la seguridad de la información y la ciberseguridad como temas o asignaturas, asociadas a cada línea de estudio. En este sentido, se procurará diseñar de manera colaborativa con las instituciones educativas la asignatura de seguridad de la información para las carreras y orientaciones técnicas, así como para otras orientaciones, tales como las jurídicas, de comunicación, administración, contabilidad y salud. Asimismo, se desarrollarán acciones colaborativas y voluntarias para sumar a estas iniciativas al sector educativo privado.”



Mauro D. Ríos