IPANDETEC
CENTROAMÉRICA

Paso a paso para una política de ciberseguridad integral

HONDURAS

Edición: Aquilino Rodríguez
Diagramación: Juan Pablo Hoyos C.
Coordinación: Abdías Zambrano
Investigación y revisión realizada con la cooperación del International Human Rights Advocates at the University of Pennsylvania Law School

IPANDETEC
CENTROAMÉRICA

IPANDETEC Centroamérica es una organización sin fines de lucro, basada en la Ciudad de Panamá, que promueve el uso y regulación de las TIC y la defensa de los Derechos Humanos en el entorno digital a través de la incidencia, investigación, monitoreo y seguimiento legislativo de Políticas Públicas de Internet en Centroamérica.

Este policy paper se realizó gracias al apoyo del Fondo Indela.

INTRODUCCIÓN

El presente 'policy paper' está encaminado a desarrollar de manera compleja la ciberseguridad en la República de Honduras. Se trata de un momento sumamente importante, en que el mundo tecnológico ha tenido cambios radicales y habituales, lo que ha traído consigo son implicaciones en el entorno social como laboral. De esta manera la información digital se ha convertido en la principal materia prima de los servicios digitales, y también se ha convertido en un recurso que debe ser controlado y protegido.

Prácticas buenas de ciberseguridad que respetan los derechos humanos se forjan confianza en tecnologías de información y comunicación y mejorar seguridad y resiliencia. El 'paper' resume las actuales obligaciones e iniciativas de ciberseguridad internacional y nacional en Honduras y ofrece recomendaciones para maneras en que partes interesadas puedan asegurar que los esfuerzos de ciberseguridad abrazan, protegen y avanzan los derechos humanos. Examina las leyes y las políticas actuales y propuestas y considera las mejores prácticas y normas internacionales en el contexto hondureño.

I. REGULACIÓN NACIONAL

Aunque no tiene un equipo nacional dedicado solamente a la ciberseguridad, Honduras cuenta con un órgano regulador, Comisión Nacional de Telecomunicaciones (CONATEL), que supervisa el sector de las telecomunicaciones. Además, en 2018, el país anunció una nueva ley que estableció una comisión encargada de crear una estrategia de ciberseguridad nacional.

La comisión supervisa la ejecución de sus políticas.[1] El Instituto Hondureño de Ciencia, Tecnología e Innovación es un ente estatal especializado en TIC's que promueve el desarrollo de ciencia y tecnología en el país pero no ha sido incluido en la estrategia de ciberseguridad. Honduras tiene un Comité Interinstitucional de Ciberseguridad, pero el comité ha resultado de la acción del gobierno y no hay una garantía que los intereses de sociedad civil o consumidoras son representados.

La única ley existente para proteger la ciberseguridad se aplica solamente a las redes sociales (Ley de Estrategia de Ciberseguridad Nacional de Prevención de Campañas de Odio y Discriminación en Redes Sociales).[2] También, Honduras no cuenta con una ley de datos personales. En 2006, Honduras aprobó la Ley de Transparencia y Acceso a la Información Pública (Decreto 170-2006), [3] que estableció el Instituto de Acceso a la Información Pública (IAIP). Individuales interesados pueden solicitar el Instituto de Acceso a la Información Pública sobre qué agencias públicas tiene acceso a cuál datos personales.

1. UNIDIR Cyber Policy Portal: Honduras. (2018, December). United Nations Institute for Disarmament Research https://unidir.org/cpp/en/states/honduras.
2. Ley de Estrategia de Ciberseguridad Nacional, El Pais (2018), https://www.elpais.hn/tag/ley-de-estrategia-de-ciberseguridad-nacional/.
3. Ley de Transparencia a Acceso a la Información Pública (2006), https://portalunico.iaip.gob.hn/assets/docs/leyes/ley-de-transparencia-y-reglamento.pdf.

Aunque Honduras aún no cuenta con una legislación general integral en materia de privacidad, ha promulgado leyes muy por el contrario, inmunizando a las autoridades estatales de responsabilidad en las investigaciones penales. En 2011, Honduras aprobó la Ley Especial para la Intervención de las Comunicaciones Privadas, que permite el acceso y la búsqueda de comunicaciones privadas (particularmente grabadas, electrónicas) sin consentimiento.[4]

Es importante destacar que el nuevo código penal de Honduras sí codifica varios delitos cibernéticos, incluyendo piratería, phishing, robo de identidad, pornografía y provocación sexual.[5] Sin embargo, periodistas, activistas y miembros del público se han pronunciado en contra del código penal promulgado más recientemente en 2019, que penaliza el insulto y la calumnia[6] y añade una pena mayor por conducta criminal en línea. Muchos caracterizaron las disposiciones relevantes como afrentas a la libre expresión. De hecho, la legislatura hondureña ha intentado, en múltiples ocasiones, aprobar una ley de ciberseguridad que obligaría a las empresas a bloquear o eliminar el "contenido ilegal" publicado en las plataformas dentro de las 24 horas de recibir una denuncia; este período puede ampliarse a 7 días si está debidamente justificado.[7]

La ley está aparentemente dirigida a regular "actos de odio y discriminación" en Internet; sin embargo, los comentaristas internacionales han impugnado las verdaderas motivaciones de la ley, afirmando que el objetivo de la ley es censurar la libertad de expresión en la web.[8]

La propuesta continua de esta ley llega después de que 40 periodistas hayan sido asesinados en la última década en relación con su trabajo. Parece claro que en el actual clima político y social de Honduras con respecto a la libertad de expresión, la implementación de leyes de seguridad cibernética ostensiblemente bien intencionadas que regulan el habla en línea debe considerarse con precaución. **En respuesta, el Congreso eliminó estas disposiciones después de la promulgación.[9]**

En 2015, una iniciativa deley para la protección de datos personales fue presentada al Congreso para crear protecciones uniformes con la cooperación de AECID (la Agencia Española de Cooperación Internacional para el Desarrollo), pero la última conversación sobre esta ley ocurrió en 2018. Aunque, protecciones para datos personales están disponibles en el contexto del gobierno y el derecho penal según una decisión del Corte Suprema de Justicia que crea un derecho constitucional (Habeas Data), y la Ley Transparencia, como se mencionó anteriormente.

4. Ley Especial sobre Intervención de las Comunicaciones Privadas (2011), https://www.tsc.gob.hn/web/leyes/Ley%20Especial%20sobre%20Intervenci%C3%B3n%20de%20las%20Comunicaciones%20Privadas.pdf.
5. El Código Penal (Decreto No. 130-2017), https://www.tsc.gob.hn/web/leyes/Decreto_130-2017.pdf.
6. Honduras enacts penal code maintaining 'crimes against honor', Committee to Protect Journalists (2020), https://cpj.org/2020/06/honduras-enacts-penal-code-maintaining-crimes-against-honor/.
7. Dictamen, La Ley Que Establece Medidas Para Prevenir los Actos de Odio y Discriminación en Redes Sociales e Internet (2018), https://tinyurl.com/ftwt5eew.
8. Comunicado: Ley que regula los actos de odio y discriminación en Internet de Honduras, AccessNow (2018), https://www.accessnow.org/comunicado-ley-que-regula-los-actos-de-odio-y-discriminacion-en-internet-de-honduras/
9. Congreso elimina los articulos que violentaban libertad de expresion, La Prensa (2019), https://www.laprensa.hn/honduras/1314332-410/congreso-nacional-eliminara-delitos-injuria-calumnia-nuevo-codigo-penal-honduras-.

II. ESTANDARES INTERNACIONALES

Acuerdos Internacionales Bilaterales y Multilaterales con Honduras

Honduras ha suscrito varios acuerdos con otras naciones en materia de seguridad cibernética a nivel nacional. Muchos de estos países tienen una valencia de seguridad nacional y tratan, en parte, con la preparación militar contra las amenazas de seguridad cibernética. Por ejemplo, el Memorando de Entendimiento entre Honduras y México trata de la defensa nacional.[10]

Organización de los Estados Americanos

En 2004, la Asamblea General aprobó la Resolución AG / Res. 2004 (XXXIB - O/04), titulada "La Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética", y al hacerlo, proporcionó un mandato pidiendo a la Secretaría del CICTE que comience a trabajar en el tema de la Seguridad Cibernética.

La Secretaría del CICTE reconoce que la seguridad del ciberespacio radica en una amplia gama de entidades nacionales y regionales de los sectores público y privado que trabajan tanto en cuestiones políticas como técnicas.

Los objetivos principales de la secretaría incluyen la creación de una red de alerta formada por equipos de respuesta a incidentes de seguridad, prestar apoyo a técnicos de seguridad cibernética de todas las Américas y cultivar y apoyar el desarrollo de estrategias nacionales de seguridad cibernética.

Reconociendo la naturaleza cambiante de las amenazas a la seguridad cibernética, los Estados Miembros de la OEA renovaron su compromiso con la seguridad cibernética al adoptar, en 2012, una declaración sobre "Fortalecimiento de la seguridad cibernética en las Américas" y 2015, la "Declaración sobre la protección de la infraestructura crítica frente a las amenazas emergentes" (2015). Estos instrumentos son cruciales para la promoción de políticas de seguridad cibernética políticamente cohesivas en las Américas.[11]

10. Memorandum of Understanding be Honduras-Mexico. Secretaría de Defensa Nacional (National Defense Secretariat) Cooperation, including aid by Mexico in cybersecurity and cyberdefense. 9 February 2018 (reported)
11. https://www.sites.oas.org/cyber/EN/Pages/contacts.aspx

Principios de Ciberseguridad en Europa

La Unión Europea (UE)ha adoptado medidas positivas y admirables para hacer frente a los riesgos de seguridad cibernética a nivel nacional.[12]

La UE promulgó la Ley de Ciberseguridad el 27 de junio de 2019. La Ley logra dos objetivos principales: (i) reforzar el mandato del organismo de vigilancia de la seguridad cibernética de la UE, ENISA, para apoyar a los Estados miembros de la UE en la lucha contra las amenazas y los ataques cibernéticos; y (ii) establecer un marco de certificación cibernética a escala de la UE en el que la ENISA desempeñará un papel clave.[13] ENISA es la agencia de la UE dedicada a lograr un alto nivel común de ciberseguridad en toda Europa.[14]

ENISA se creó en 2004 y promueve la ciberseguridad en la UE contribuyendo a la ciberpolítica, aumentando la fiabilidad de los productos, servicios y procesos de las TIC en los sistemas de certificación de la ciberseguridad, y coopera con los Estados miembros y los organismos de la UE, y ayuda a Europa a prepararse para futuras amenazas cibernéticas.

Los principales métodos para obtener resultados finales eficaces son el intercambio de conocimientos, el fomento de la capacidad y la sensibilización. Con arreglo al nuevo marco, la ENISA coordinará la preparación de los sistemas de certificación de la ciberseguridad candidatos que se presentarán a la Comisión Europea para su adopción.

La ley también dará a las empresas la oportunidad de certificar que sus productos cumplen las normas de ciberseguridad de la UE. La Ley de Ciberseguridad y el ecosistema cibernético más amplio de la UE es un marco progresivo que podría ser un modelo para la emulación.

Principios Internacionales (la ONU)

La Organización de Naciones Unidas(ONU) ha reconocido la ciberseguridad como un grave problema internacional y ha emitido cinco resoluciones para abordar el tema.[15] Además, como parte de su estrategia para garantizar un entorno de TIC moderno y receptivo que apoye la labor básica de las Naciones Unidas, la Oficina de Tecnología de la Información y las Comunicaciones (OICT) está dirigiendo los esfuerzos para crear capacidad, reforzar la coordinación y fomentar la colaboración para mejorar la preparación, la resiliencia y la respuesta en materia de seguridad cibernética.

12. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN
13. https://www.jonesday.com/en/insights/2019/06/the-eu-cybersecurity-act-is-now-applicable
14. https://www.enisa.europa.eu/about-enisa
15. https://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx

En asociación con otras entidades de las Naciones Unidas, el programa Digital Blue Helmets (DBH) amplía los conocimientos y perspectivas cibernéticos de las Naciones Unidas.[16] El programa ayuda a intercambiar información y protege contra las amenazas cibernéticas a las naciones mediante la armonización de las operaciones cibernéticas de las organizaciones y los marcos de política cibernética.[17]

III. PROYECTO DE LEY IMPLEMENTADOS

La República de Honduras cuenta con variada legislación conexa que regula la materia de ciberseguridad, estas disposiciones específicas la podemos buscar y encontrar en el libro del Código Penal, como en el libro de Procedimiento Penal Hondureño.

De igual forma se hará mención de estas disposiciones específicas que se consagran en el Código Penal Hondureño: La interferencia de Datos se consagran en el Artículo 214, del Código Penal, posteriormente está el abuso de dispositivos, la misma se encuentra estipulado en el Artículo 254, del Código Penal.

Para dar inicio a la investigación no debemos vulnerar o alterar los procedimientos para la investigación de delitos informáticos que se encuentran regulado con formalidad en el código procesal penal, dentro del mismo se dependen disposiciones específicas como la interceptación de Datos sobre el contenido que se consagra en el Artículo 223, del Código Procesal Penal.

IV. BUENAS PRÁCTICAS APLICADAS EN EL PAÍS

Recomendaciones para el sector financiero

Las instituciones financieras deben garantizar que existan numerosas redes de seguridad y niveles de supervisión en caso de violación, ya que independientemente de cuán preparados estén, habrá brechas que probablemente explotarían los cibercriminales. La armonización de la seguridad cibernética, la privacidad de los datos y la legislación sobre tecnología de la información y las comunicaciones (TIC) son un componente fundamental para facilitar el desarrollo de una industria cibersegura de servicios financieros.

16. https://unite.un.org/digitalbluehelmets/cyberrisk
17. https://unite.un.org/digitalbluehelmets/sites/unite.un.org.digitalbluehelmets/files/docs/digitalbluehelmets_brochure_final.pdf

Recomendaciones para el sector de salud

Instituciones públicas en el sector de salud, como el Colegio Médico de Honduras, deben garantizar que médicos y otros profesionales en el sector de salud cumplira con las leyes existentes se garantizan la protección de datos personales del salud, como información sobre condiciones médicas. El sector de salud tiene leyes que garantizan la confidencialidad del paciente, pero el sector debe crear un garantiza para la protección de datos personales almacenado en registros hospitalarios digitales.[18]

Recomendaciones para todos los sectores

Desarrollar y publicar una visión nacional para orientar la priorización en inversiones de seguridad. El gobierno de turno debe tomar la iniciativa directa de formar un grupo de líderes de opiniones nacionales para discutir la visión de la ciberseguridad y relacionarla con los demás participantes presentes. Si bien es cierto las asociaciones cívicas como entidades gubernamentales podrían desarrollar materiales o seminarios empresariales para capacitarlos a cada líder empresarial lo preocupante y riesgoso ser víctima de ciberseguridad.

Establecer un modelo de gobernanza y condiciones que faciliten la colaboración, coordinación y cooperación entre todas las partes interesadas. Incluso hasta en las entidades gubernamentales, se puede aplicar este modelo para lograr avances más eficientes en la aplicación y ejecución de las normas legales y reglamentarias en todos los niveles gubernamentales. Además este mismo modelo de gobernanza puede establecerse o aplicarse como un epicentro de una nueva coordinación para la entidad gubernamental..
Se necesitan nuevos enfoques para perseguir a los delincuentes.

Muchas veces los delincuentes utilizan la tecnología para cambiar de identidad y distribución de materiales de abusos infantiles proporcionando que la ley esté al tanto ante cualquier incidente o acontecimiento que se presente en el servicio digital, cuando se dé esto es donde las autoridades deben focalizarse y perseguir los supuestos responsables que se dediquen a cometer actos delictivos o repugnante para la sociedad, las empresas que son expuestas ante esta situación tan notorio.

Establecer un órgano de coordinación dinámico, nacional de ciberseguridad digital que involucre a todos los sectores gubernamentales.

18. Honduras - Data Protection Overview, Data Guidance, https://www.dataguidance.com/notes/honduras-data-protection-overview.

V. CONSEJOS PARA QUE ESTE PAÍS Y SUS AUTORIDADES TENGAN SU PROPIA REGULACIÓN

Como ya se ha señalado, las amenazas a la ciberseguridad son cada vez más importantes y las esferas que requieren atención inmediata en nombre de los gobiernos. Como resultado, más de 100 gobiernos han desarrollado estrategias nacionales de defensa de la ciberseguridad para combatir los riesgos de ciberseguridad.

Todos los estados tienen necesidades idiosincráticas y, como resultado, los enfoques de ciberseguridad deben adaptarse a esas circunstancias; sin embargo, se pueden discernir cinco posibles mejores prácticas a partir de las prácticas actuales de las naciones.[19]

Primero, una nación debe crear una agencia nacional dedicada a la seguridad cibernética. Las naciones a la vanguardia de la seguridad cibernética dan a una sola entidad la responsabilidad general de definir e impulsar la agenda de seguridad cibernética de toda la nación. Esta entidad debería contar con los conocimientos adecuados en materia de vivienda, así como con asociaciones con el sector privado para llenar las lagunas en la experiencia.

Por ejemplo, la Agencia Nacional de Ciberseguridad del Reino Unido colabora estrechamente con otras entidades gubernamentales, como el Departamento de Asuntos Digitales, Cultura, Medios de Comunicación y Deporte, para mejorar las capacidades de los profesionales de la ciberseguridad en el país.

Segundo, una nación debería instituir un programa nacional de protección de infraestructura crítica. Es sumamente importante centrarse en la infraestructura crítica del país. La perturbación de la infraestructura crítica puede repercutir en la economía, la confianza de las empresas, la sociedad y la seguridad nacional en general.

Los países deberían dar prioridad a los sectores y activos críticos determinando el papel que desempeñan en garantizar la salud del estafador y la seguridad nacional, y exigir que la organización del sector en sectores críticos cumpla las normas de ciberseguridad reconocidas mundialmente (por ejemplo, el Marco de Seguridad Cibernética del Instituto Nacional de Normas y Tecnología de los Estados Unidos), y el establecimiento de mecanismos de gobernanza sólidos.

19. https://www.mckinsey.com/industries/public-and-social-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks

En **tercer** lugar, un gobierno debe tener un plan nacional de respuesta y recuperación de incidentes. Este plan debe centrarse en seis elementos: procedimiento de información claramente definido para ciudadanos y empresas, vigilancia activa de las ciberamenazas, múltiples fuentes de inteligencia de amenazas, esfuerzos proactivos para combatir las ciberamenazas, severidad estandarizada matriz de evaluación, sólido plan de movilización para responder eficazmente a los incidentes cibernéticos.

Cuarto, los gobiernos deben establecer un marco de leyes de seguridad cibernética para prevenir, investigar y tomar medidas contra los delitos cibernéticos. Una clave de estas leyes es una estructura sólida de elementos sustantivos y procesales. Una buena opción al elaborar leyes nacionales de seguridad cibernética es adoptar las directrices establecidas por el Convenio de Budapest. Las leyes sustantivas definen diferentes tipos de posibles delitos cibernéticos y el castigo correspondiente. Las leyes de procedimiento definen la autoridad y las responsabilidades que cada país debe tener en cuenta al aplicar las leyes. Además, la cooperación y colaboración internacionales en materia de legislación es fundamental debido al carácter transnacional del delito cibernético.

Quinto, un dinámico ecosistema de seguridad cibernética constituido por ciudadanos, profesionales y organizaciones del sector privado, que permite a las empresas de seguridad cibernética prosperar es clave para el éxito de una política de seguridad nacional. Para desarrollar un ecosistema vibrante, los gobiernos deben centrarse en promover un ecosistema vibrante de empresas y empresarios de seguridad cibernética a través de programas de capacitación financiados por el estado para profesionales de la seguridad cibernética.

Además, garantizar que los ciudadanos sean conscientes de la cibernética a través de una orientación gubernamental coherente y clara es esencial porque cualquier persona puede ser un punto de ataque para un ataque cibernético.

Otras recomendaciones incluyen:

Cada autoridad gubernamental debe especificar claramente su mando y autoridad con respecto a la seguridad cibernética con el fin de reducir la confusión y eliminar las redundancias innecesarias entre las entidades. **Hacer uso de la regulación**, cuando sea adecuado, para alcanzar los objetivos de política pública, mediante la aplicación de la Recomendación del Consejo para Mejorar la Calidad de la Regulación Gubernamental.

Revisar sistemática y periódicamente el inventario de regulaciones para identificar y eliminar o remplazar aquellas que sean obsoletas, insuficientes o ineficientes.

Desarrollar, implementar y evaluar una estrategia de comunicación para asegurar que las metas de calidad regulatoria cuenten con apoyo sostenido.

Es importante crear canales para una cooperación a varios niveles entre los gobiernos nacionales y las organizaciones internacionales regionales y mundiales que trabajan en este tema, tal como lo sugieren el BID, la OEA, la UIT y las empresas especializadas en ciberseguridad.

El intercambio de información y la cooperación son indispensables para hacer frente a las amenazas transfronterizas. Aunque un determinado país o un sector específico hayan desarrollado y adoptado un marco de ciberseguridad altamente efectivo.

Honduras requiere abordar pronto, en cooperación entre todas las partes interesadas, la construcción de una sociedad de la información más segura, centrándose en medidas jurídicas, medidas técnicas, medidas organizativas, creación de capacidades y cooperación para hacerle frente al cibercrimen, maximizar beneficios, gestionar los riesgos y optimizar los recursos de TI.

Honduras necesita una estrategia de ciberseguridad mas amplia, y que tiene la potencia a regular mas tipos de datos personales en la red.

VI. CONCLUSIONES

A continuación, podemos concluir que:

Mientras la digitalización se expande y madura rápidamente, es esencial que los países establezcan un marco abordando el riesgo cibernético, seguridad y resiliencia en conjunto con los objetivos y el desarrollo sostenible. Muchos países de la región son vulnerables a ataques cibernéticos potencialmente devastadores. Cuatro de cada cinco países no tienen estrategias de ciberseguridad o planes de protección de infraestructura crítica. Dos de cada tres no cuentan con un centro de comando y control de seguridad cibernética. La gran mayoría de las fiscalías carece de capacidad para perseguir los delitos cibernéticos. Cómo tantos desafíos en pos de ese desarrollo.

La ciberseguridad se ha convertido en una cuestión cada vez más importante en la sociedad de la información. Las amenazas a la seguridad cibernética socavan la capacidad de los gobiernos, las empresas y los usuarios individuales para aprovechar plenamente las Tecnologías de la Información.

IPANDETEC Centroamérica apoya la formulación de políticas públicas integrales en materia de ciberseguridad mediante mecanismos abiertos, transparentes y multisectoriales.

IPANDETEC

CENTROAMÉRICA