Innovare
Ciencia y Tecnología

LA BRECHA EXISTENTE EN LA CIBERSEGURIDAD EN HONDURAS

Carlos Marlon Raudales Centeno[1]

Facultad de Postgrado, Universidad Tecnológica Centroamericana (UNITEC), Campus de La Ceiba

(Recibido: Enero, 2017/ Aceptado: Diciembre, 2017)

Resumen

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

Según algunos cálculos, el cibercrimen le cuesta al mundo hasta US$575.000 millones al año, lo que representa 0,5% del PIB global. Eso es casi cuatro veces más que el monto anual de las donaciones para el desarrollo internacional. En América Latina y el Caribe, este tipo de delitos le cuesta alrededor de US$90.000 millones al año. A falta de una política nacional de seguridad cibernética o un equipo de respuesta a incidentes, el Gobierno de Honduras tiene una capacidad limitada para abordar de manera proactiva las amenazas a su seguridad cibernética.

Palabras Claves: *Ciberseguridad, Cibercrimen, Tecnologías de la Información, Honduras, Desarrollo.*

Abstract

Cybersecurity has become an ever increasing important issue in information society. Threats to cybersecurity undermine the ability of governments, businesses, and individual users to take full advantage of Information Technology.

According to some estimates, cybercrime costs the world up to US $ 575,000 million a year, representing 0.5% of global GDP. That's almost four times the annual amount of donations intended to international development. In Latin America and the Caribbean this type of crime will cost about US $ 90,000 million a year. In the absence of a national policy on cybersecurity or incident response team, the Honduran Government has a limited ability to proactively address threats to their cybersecurity.

Keywords: *Cybersecurity, Cybercrime, Information Technology, Honduras, Development.*

[1] Autor para correspondencia. Email: Carlos.Raudales@unitec.edu

1. Introducción

El mundo sufre transformaciones constantes y existen esfuerzos para que muchos países puedan optar a niveles de vida estándares. Los gobiernos de los países en desarrollo buscan continuamente catalizadores para su desarrollo sostenible. En cada país — especialmente los más globalizados — también el sector privado requiere modernizarse y las empresas existen para crear valor para sus partes interesadas. En consecuencia, cualquier empresa—comercial o no — tendrá la creación de valor como objetivo de gobierno. La creación de valor significa obtener beneficios a un coste óptimo de recursos mientras se optimiza el riesgo. Los beneficios pueden tomar muchas formas, por ejemplo, financieros para empresas comerciales, o de servicio público para entidades del gobierno. (ISACA, 2013)

Las organizaciones tienen muchas partes interesadas, y 'crear valor' significa cosas diferentes —y a veces contradictorias—para cada una de ellas. El gobierno debe negociar y decidir entre los diferentes intereses, dependiendo del valor de las partes interesadas. En consecuencia, el sistema de gobierno debería tener en cuenta a todas las partes cuando se tomen decisiones relacionadas con la evaluación de beneficios, riesgos y recursos. Para cada decisión, las siguientes preguntas pueden y deberían hacerse: ¿Para quién son los beneficios? ¿Quién asume el riesgo? ¿Qué recursos se requieren? En esto, las Tecnologías de la Información (TI) juegan un papel fundamental.

La inclusión digital y el acceso, la ciberdelincuencia y la ciberseguridad, la privacidad de los datos y su uso, el cambio en los modelos de negocio, y, por último, la creación de políticas eficaces y sólidas para las tecnologías, son tendencias que están transformando la sociedad de la información (World Economic Forum, 2015). A medida que la revolución de las TI se desarrolla, ésta conllevará ventajas, pero también traerá consigo riesgos y desafíos. Algunos de éstos se ven en el aumento de casos relacionados con violaciones de la seguridad cibernética o la guerra cibernética, y en cuestiones relacionadas con la privacidad y la neutralidad de Internet. Según algunos cálculos, el cibercrimen le cuesta al mundo hasta US$575.000 millones al año (Center for Strategic and International Studies & McAfee, 2014), lo que representa 0,5% del PIB global. Eso es casi cuatro veces más que el monto anual de las donaciones para el desarrollo internacional. En América Latina y el Caribe, este tipo de delitos le cuesta alrededor de US$90.000 millones al año (Prandini & Maggiore, 2011).

Las ventajas de la conectividad son innegables, y los latinoamericanos y caribeños adoptan estas nuevas tecnologías con entusiasmo. Hoy, este territorio es el cuarto mayor mercado móvil del mundo, la mitad de su población usa el Internet y los gobiernos emplean cada vez más medios digitales para comunicarse y brindar servicios a los ciudadanos. Pero existen brechas significativas — muy amplias en Honduras — para prevenir y mitigar los riesgos de la actividad delictiva o maliciosa en el ciberespacio. Este trabajo, que presenta un resumen de dos importantes reportes del estado de la ciberseguridad, es un buen punto de referencia para comenzar a encontrar soluciones que permitan remediar esta situación.

2. Marco Teórico

El Desarrollo Sostenible sugiere la contribución a mejorar la calidad de vida en general, así como también en aspectos ambientales y para volver más eficientes los procesos de diferente tipo (tecnológicos, jurídicos, comunicacionales, financieros, etc.). Este concepto se complementa con la definición utilizada por la Comisión Internacional sobre Educación para la Práctica del Desarrollo Sostenible, según la cual, "desarrollo sostenible" se define como "satisfacer a las necesidades del presente sin comprometer la capacidad de futuras generaciones para satisfacer a las necesidades propias"[2]. Se basa en tres resultados: crecimiento económico, cuidado del medio ambiente y desarrollo social, que equivale a decir prosperidad, planeta y personas.

Miles de millones de ciudadanos del mundo, sus gobiernos y las organizaciones que los emplean no serían capaces de trabajar, si no tuviera acceso a redes. La imaginaria "autopista de la información" de la década de 1980 se ha convertido, en realidad, en un elemento crítico de la infraestructura nacional y global. El acceso a las redes mundiales es, sin duda, un catalizador para el crecimiento y aprovechamiento de oportunidades. Uno de los grandes desafíos actuales es cómo asegurarse de que el crecimiento es justo, amplio, e inclusivo. Este no debe favorecer exclusivamente a ninguna de las cuadrículas económica, grupo social, o perfil de la empresa (Alvarez, 2015), al aprovechar las Tecnologías de la Información.

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 de los desafíos en pos de ese desarrollo, sacar la mayor ventaja posible de la llamada cuarta revolución industrial, propicia la creación de una infraestructura digital no solo moderna y robusta, sino también segura para proteger al gobierno y demás organizaciones e individuos del cibercrimen, como un elemento clave para el desarrollo (Moreno, 2016).

La mayoría de los Informes, guías o publicaciones sobre este fenómeno comienzan definiendo el término "cibercrimen". Una definición bastante común para este término es la de entenderlo como una actividad delictiva cualquiera, en la que se utilizan como herramienta los computadores o redes, o aquella, en la que éstos aparatos son las víctimas de la misma, o bien el medio desde donde se efectúa dicha actividad delictiva. También puede definirse como la gama de actividades delictivas incluidas las infracciones contra los datos y sistemas informáticos, delitos relacionados con la informática, delitos y faltas de contenido y contra los derechos de autor[3].

[2] Comisión Brundtland. *Our Common Future*. London, England: Oxford University Press; 1987. La Comisión Brundtland fue convocada por las Naciones Unidas en 1983 para abordar la creciente preocupación "en torno al acelerado deterioro del medio ambiente humano y los recursos naturales y las consecuencias de ese deterioro para el desarrollo económico y social." Esta Comisión, y su posterior Informe, fueron los primeros que esbozaron claramente la idea de "desarrollo sostenible".

[3] Más detalles de la definición de cibercrimen en http://aic.gov.au/crime_types/cybercrime/definitions.html

Según la UIT (2009), la ciberseguridad desempeña un papel importante en el desarrollo de las TI, así como de los servicios de Internet. Mejorar la ciberseguridad y proteger las infraestructuras críticas de la información, es esencial para lograr la seguridad y el bienestar económico de cada país. Conseguir un servicio de Internet más seguro (y proteger a los usuarios de Internet) se ha convertido en parte integral del desarrollo de nuevos servicios, así como de la política gubernamental. La disuasión del ciberdelito es una componente integral de la ciberseguridad nacional y de la estrategia de protección de la infraestructura de la información crítica. En particular, ello incluye la adopción de las medidas jurídicas adecuadas contra la utilización fraudulenta de las TI a efectos delictivos o de otro tipo y contra las actividades destinadas a afectar la integridad de las infraestructuras críticas nacionales.

En relación con lo anterior, la ciberseguridad puede definirse como la colección de instrumentos, políticas, conceptos de seguridad, medidas de seguridad, directrices, enfoques de gestión de riesgos, acciones de formación, mejores prácticas, garantía y las tecnologías que se pueden utilizar para proteger el medio ambiente y la organización cibernética y los bienes de los usuarios. Los activos de la organización y de los usuarios incluyen dispositivos informáticos, personal, infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones, y la totalidad de la información transmitida y / o almacenada en el entorno cibernético conectados. La ciberseguridad garantiza la consecución y el mantenimiento de las propiedades de seguridad de la organización y los activos de los usuarios contra los riesgos de seguridad relevantes en el entorno cibernético. Los objetivos generales de seguridad comprenden: disponibilidad, Integridad – que puede incluir la autenticidad y el no repudio– y la confidencialidad, de acuerdo a la UIT (2016).

Las organizaciones internacionales como la Organización de Estados Americanos (OEA), el Banco Mundial, la Unión Internacional de Telecomunicaciones (UIT) y el Banco Interamericano de Desarrollo (BID), han lanzado y están financiando proyectos para cerrar la brecha de la conectividad y aprovechar los beneficios derivados de la utilización de las TI para estimular el crecimiento económico, mejorar la prestación y la capacidad de servicios, impulsar las ganancias de la productividad y la innovación y para promover el buen gobierno. Muchos de sus informes y publicaciones alaban el papel que desempeñan las Tecnologías de la Información y la Comunicación en la promoción de estrategias de desarrollo de estos países y en la responsabilidad de gobierno, y proporcionan indicadores fuertes para apoyar una mayor conectividad a Internet y ecosistemas digitales más extensos.

El Banco Mundial, por ejemplo, estima que cuando el 10% de la población en países en desarrollo está conectado a Internet, el PIB del país crece en un 1% a un 2%, mientras que el Foro Económico Mundial informó que incluso duplicar el uso de datos de banda ancha móvil puede conducir a un aumento del 0,5% del crecimiento del PIB. Al mismo tiempo, sin embargo, el poder transformador de las TI como un catalizador para el crecimiento del PIB y el desarrollo social puede ser socavado fácilmente si los riesgos de seguridad asociados con la proliferación de infraestructura de las TI y de aplicaciones de Internet no se equilibran adecuadamente con un plan integral de seguridad cibernética y resiliencia (Hathaway & Spidalieri, 2016).

Hay dos intereses enfrentados en la realización de la promesa y el potencial de las TI y de Internet. En primer lugar, hay una agenda digital y una visión económica que promete generar ingresos y empleo, proporcionar acceso a los negocios y la información, aumentar la productividad y la eficiencia, permitir el aprendizaje electrónico, mejorar las habilidades de la fuerza laboral, facilitar las actividades del gobierno y extender la prosperidad mediante el crecimiento del PIB y así reducir la pobreza. Sin embargo, la única manera en que los países pueden lograr tales resultados es si su programa de desarrollo de las TI es sostenible de diferentes formas.

Ambientalmente, la sostenibilidad se puede lograr mediante la mitigación de los impactos ambientales negativos del mayor crecimiento de las redes y los dispositivos de las TI (por ejemplo, impactos como las emisiones de gases de efecto invernadero, generación de basura electrónica, degradación del medio ambiente, etc.). En lo económico, al proporcionar un acceso a Internet más asequible, fiable y persistente para todos. En lo social, mediante la maximización de la contribución potencial de las TI a la equidad social y la inclusión. En lo político, al permitir la participación ciudadana en los procesos del gobierno y la toma de decisiones.

En segundo lugar, se encuentra la seguridad. No es suficiente que el aumento de la conectividad a Internet sea sostenible: también es necesario que dicha conectividad sea segura y resistente. De hecho, la dependencia de esta compleja infraestructura ha venido con un precio: al conectar tantos aspectos de la economía y servicios vitales a Internet, también se ha expuesto a una serie de actividades cibernéticas nefastas que pueden socavar la disponibilidad, integridad y resiliencia de esta infraestructura central, lo que ha amenazado los beneficios económicos y también tecnológicos, políticos y sociales de Internet. Por ejemplo, varios de los países del Grupo de los 20 (G-20) han estimado que están perdiendo al menos el 1% de su PIB debido al delito cibernético, el robo de propiedad intelectual y otras actividades electrónicas fraudulentas.

Ninguna nación puede darse el lujo de perder ni un 1% de su PIB por cuenta de actividades ilícitas cibernéticas. A medida que las tecnologías informáticas y de comunicaciones se arraigan más en la economía global y a medida que se entra en la era de la "Internet de las cosas" (IoT, por sus siglas en inglés), seguirán aumentando los incentivos para poner en peligro la seguridad de estos sistemas. Se debe enfrentar que las amenazas a la sociedad conectada están superando las defensas y el crecimiento del PIB se está erosionando cada día. La inseguridad cibernética es un impuesto al crecimiento y los países deben demostrar un compromiso con la seguridad y la resiliencia para preservar la promesa de conexión y realizar todo el potencial de la economía de Internet (Hathaway & Spidalieri, 2016).

3. Metodología

El abordaje de este tema es escaso en América Latina y aunque diversas fuentes han sido investigadas, tres reportes son claves en esta investigación: el Informe Ciberseguridad 2016 (BID; OEA, 2016) del Observatorio de la Ciberseguridad en América Latina y el Caribe auspiciado por el Banco Interamericano de Desarrollo (BID) y por la

Organización de los Estados Americanos (OEA); el Informe sobre las Amenazas a la Seguridad en Internet de 2016, Volumen 21, de la empresa Symantec (Symantec, 2016) y el Global Cybersecurity Index (GCI) de la UIT (2014).

3.1 Enfoque y alcance

La investigación tiene un enfoque cuantitativo, de alcance exploratorio-descriptivo ya que su finalidad es especificar los aspectos más relevantes del estado de la Ciberseguridad en Honduras y su relación con en el desarrollo sostenible. Hernández, Fernández, & Baptista (2014) afirman que este tipo de alcance permite "mostrar con precisión los ángulos o dimensiones de un fenómeno, suceso, contexto o situación basándose en la medición de uno o más atributos del fenómeno de interés.

3.2 Instrumentos

El instrumento base, con el cual se recoge la mayor cantidad de datos de resultados y su respectivo análisis es el *Global Cybersecurity Index* (GCI) (Figura 1). Es una iniciativa de múltiples partes interesadas para medir el compromiso de los países para la seguridad cibernética la cual tiene un amplio campo de aplicación que corta a través de muchas industrias y sectores. y nivel de desarrollo de cada país, analizándose en cinco categorías: medidas legales, medidas técnicas, medidas de organización, desarrollo de capacidades y la cooperación[4].

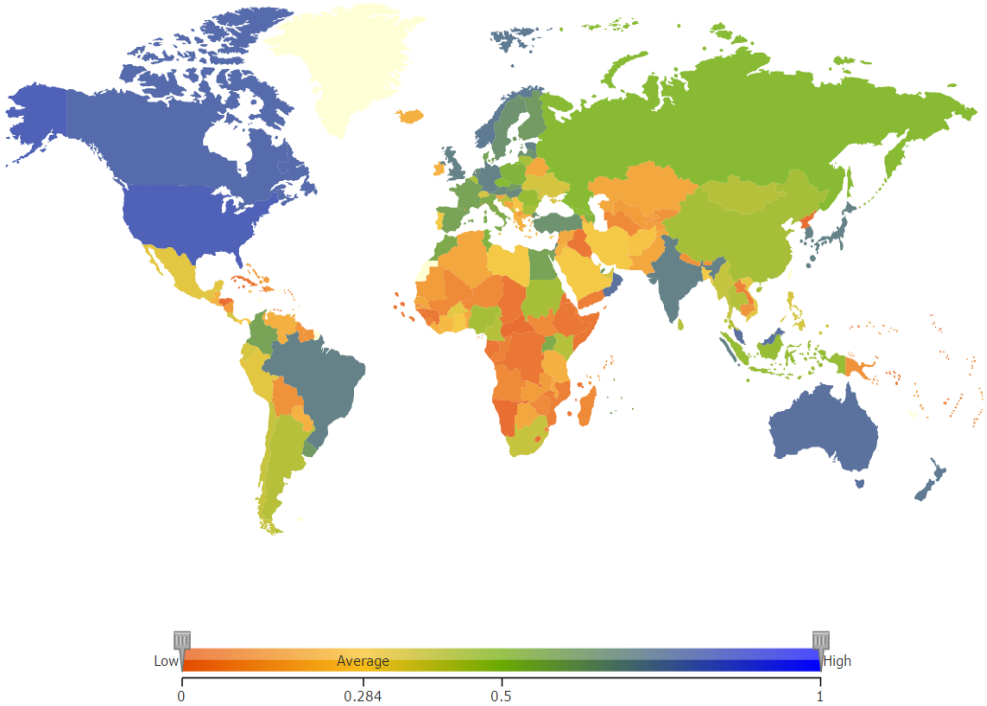

Figura 1. *Índice mundial de ciberseguridad*
Fuente: *Unión Internacional de Telecomunicaciones (UIT)*

[4] Detalles de la metodología para determinar el Índice de Ciberseguridad se encuentra en http://www.welivesecurity.com/la-es/2016/09/02/determinar-nivel-de-ciberseguridad-pais/

3.2 Técnicas empleadas

También se utilizan los datos del Informe Ciberseguridad 2016 "Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?" que recoge información mediante la utilización de encuestas y otros datos aportados por expertos y funcionarios de treinta y dos Estados Miembros de la OEA, el informe examina la "madurez cibernética" —entendiendo que cada dimensión no es necesariamente independiente de las otras— de cada país en cinco dimensiones: 1) política y estrategia de seguridad cibernética; 2) cultura y sociedad cibernética; 3) educación, formación y competencias en seguridad cibernética; 4) marcos jurídicos y reglamentarios; y 5) normas, organizaciones y tecnologías. (BID; OEA, 2016).

Otros datos son recogidos de la 2015 *Global Cybersecurity Status Report—Latin America Data*, de enero del 2015[5]. ISACA realizó una encuesta global de 3.439 empresas y profesionales de TI en 129 países para capturar sus ideas en tiempo real sobre ataques de ciberseguridad, la escasez de habilidades y propuestas del Presidente de Estados Unidos, Barack Obama, quien abordó temas de ciberseguridad como leyes de notificación de violación de datos. La encuesta fue realizada en línea del 13 al 15 de enero de 2015. En un nivel de confianza de 95 por ciento, el margen de error es de +/-1,7 por ciento. (ISACA, 2015)

Otra actualizada fuente primaria es el Informe sobre las Amenazas a la Seguridad en Internet de 2016, Volumen 21, de la empresa Symantec. El Informe sobre las amenazas para la seguridad en Internet proporciona una descripción general y un análisis anual sobre la actividad de las amenazas de todo el mundo. El informe se basa en los datos de la red *Symantec Global Intelligence Network*, que los analistas de Symantec utilizan para identificar, analizar y proporcionar comentarios sobre las tendencias emergentes en el escenario de amenazas dinámico. Dicha herramienta está compuesta por más de 63,8 millones de sensores de ataque y registra miles de eventos por segundo. Esa red monitorea la actividad de amenazas en más de 157 países y territorios a través de una combinación de productos y servicios de Symantec, como *Symantec DeepSight™ Intelligence, Symantec™ Managed Security Services*, productos de consumo Norton™ así como fuentes adicionales de datos de terceros (Symantec, 2016).

3.3 Procedimientos

Con el objetivo de presentar información relevante y útil, basado en los datos más actuales y completos disponibles para el público, se ha optado por presentar datos de informes confiables de fuentes primarias y secundarias, haciendo uso en forma íntegra del perfil del estado de ciberseguridad de Honduras del Informe Ciberseguridad 2016 del Observatorio de la Ciberseguridad en América Latina y el Caribe.

También fueron consultadas diferentes instituciones del gobierno, por medio de sus respectivas páginas web de transparencia obteniendo respuestas de cada una de ellas, entre ellas la Policía Nacional, El Congreso Nacional y el Poder Judicial, cotejando similares resultados que los reportes mundiales analizados. Los reportes de Symantec, de McAfee y de ISACA y otros también han sido de referencia. Cabe señalar que la

[5] El informe puede descargarse del sitio *www.isaca.org/cybersecurityreport*

respuesta del Congreso Nacional incluye la observación de que actualmente este tema está pendiente de abordar mediante el proceso legislativo

3.4 Resultados

A nivel mundial existe una marcada brecha entre los países desarrollados y los emergentes. La clasificación de los países por índice la encabeza Estados Unidos con 0.824, seguido por Canadá con un índice de 0.794 y el tercer puesto lo comparten Australia, Malasia y Omán con 0.765. Los dos países latinoamericanos que aparecen con mayores adelantos son Brasil, en el lugar 5 con un índice de 0.706 y Uruguay en el lugar 8 con un índice de 0.618. En Centro América aparece primero Costa Rica en el lugar 17 con 0.353, seguido por Panamá con 0.294 en el puesto 19, El Salvador y Guatemala, ambos en el lugar 22 con un índice de 0.206, Belice en el lugar 23 con un índice de 0.176 y Nicaragua en el lugar 24 con un índice de 0.147.

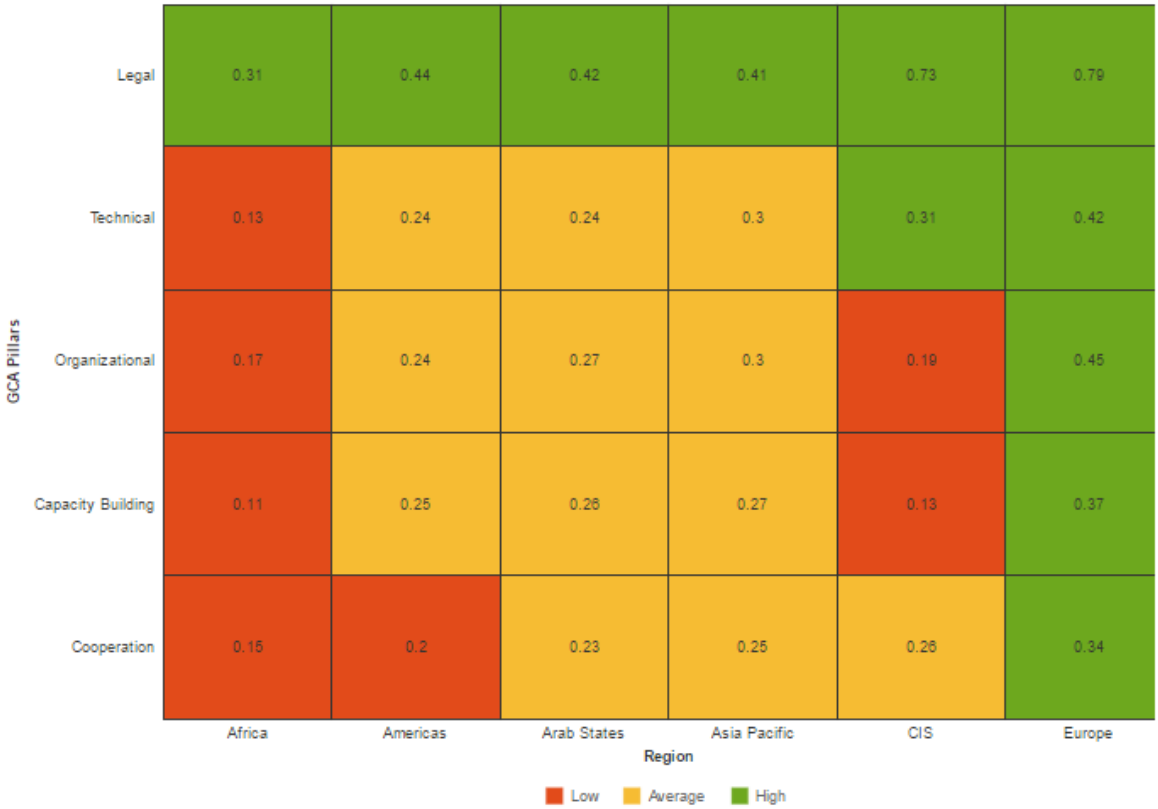

Figura 2. *Matriz regional por pilares del Índice Mundial de Ciberseguridad*
Fuente*: Unión Internacional de Telecomunicaciones (UIT)* *http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI_regional_grid.aspx*

Honduras, junto a otros 8 países, comparte el último lugar de la clasificación mundial (lugar 29) con un índice de 0.000. El índice más alto corresponde a la Región de Europa y el más bajo a la de África (Figura 2). A nivel mundial, la mayor parte del trabajo realizado parece corresponder a los aspectos jurídicos y la menor, a la creación de capacidades.

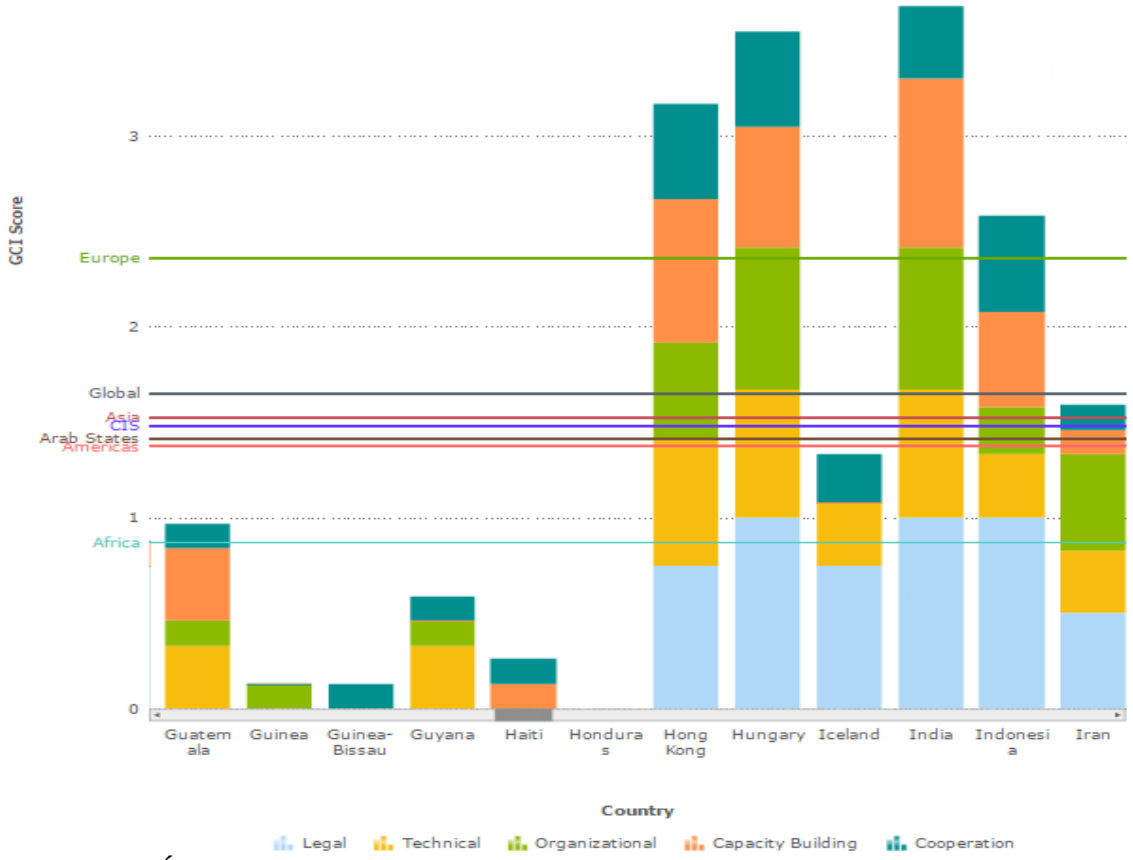

Figura 3. *Índice de Honduras con líneas de tendencia que indican las puntuaciones regionales y globales*

Fuente*: Unión Internacional de Telecomunicaciones (UIT)* http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI_bar_chart.aspx

Dos resultados impactantes del reporte del Estado de Ciberseguridad Global 2015, de ISACA, son los siguientes:

1. Las organizaciones esperan ciberataques. 2015 fue un año para abrir los ojos de muchas organizaciones acerca de las posibles amenazas de seguridad cibernética, debido a los ataques contra Anthem, Ashley Madison, Sony Pictures, T-Mobile, la cuenta personal de email del Director de la CIA John Brennan, casi 300 millones de registros fueron filtrados y cerca de US$ 1 billón robados según Tech Insider (Tech Insider, 2015). Por razones obvias, para muchas organizaciones ya no es una cuestión de si ocurrirá un ataque cibernético, es una cuestión de cuándo. Según ISACA, 46% de las empresas espera un ataque cibernético, 30% no está seguro de si está esperando un ataque y sólo el 24% no tienen expectativas de ser golpeado con un ataque. En Latinoamérica los encuestados contestaron con un 40%, 27% y 33%, en el mismo orden. Por suerte, ese temor ha causado acción y 53% de las organizaciones han aumentado la concienciación de su personal en seguridad cibernética (Figura 4).

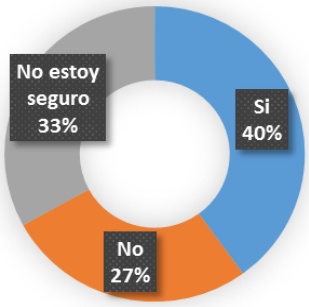

Figura 2. *Las organizaciones esperan ataques cibernéticos*
Fuente: *Elaboración propia con base en el Estado de Ciberseguridad Global 2015, de ISACA*

2. En Latinoamérica las organizaciones no están preparadas para ciberataques sofisticados y se identifica escasez de profesionales cualificados en ciberseguridad. De acuerdo a encuestas de ISACA, el 52% de los encuestados mencionan que las organizaciones no están preparadas para ciberataques sofisticados. El 23% menciona que sí y el restante 24%[6]. El asunto se agrava al identificarse escasez de profesionales cualificados en ciberseguridad. El 86% de los encuestados mencionan que, a su criterio, hay escasez de profesionales cualificados en ciberseguridad. Un abanico de riesgos se ha abierto, especialmente con el aumento de la tecnología móvil y del Internet de las Cosas en el mundo de los negocios. Con tanto como $ 300 millones se robaron más de 100 instituciones financieras en 2015, según el New York Times (The New York Times Company, 2015).

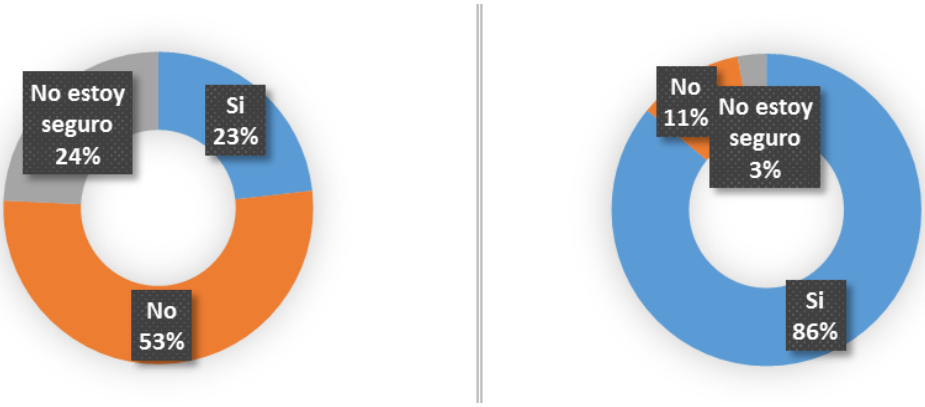

Figura 3. *Latinoamérica no está preparada para ataques cibernéticos sofisticados*
Fuente: *Elaboración propia con base en el Estado de Ciberseguridad Global 2015, de ISACA*

El perfil del estado de bienestar cibernético de Honduras, en absolutamente todas las dimensiones e indicadores del Global Cybersecurity Index (GCI), de la UIT, muestra que el país no cuenta con evidencias para reportar avances en la materia de ciberseguridad, por lo tanto, el índice es de cero, ubicándose en último lugar a nivel mundial. Los resultados obtenidos por el Observatorio de la Ciberseguridad en América Latina y el Caribe, en su Informe Ciberseguridad 2016, muestran similares resultados. A continuación, se presenta el perfil del estado de ciberseguridad de Honduras.

[6] Nota: Debido al redondeo al número entero más cercano, las respuestas no suman 100%.

Tabla 1. *Índice mundial de ciberseguridad y perfiles de ciberbienestar – Honduras*

Pilares del reporte del estado de ciberseguridad	¿Cumple requerimientos?
1.Medidas legales	
1.1 Legislación criminal	No
1.2 Regulación y cumplimiento	No
2. Medidas técnicas	
2.1 Centro de respuesta a incidentes	No
2.2 Marco estándar de ciberseguridad	No
2.3 Requerimientos de certificación y acreditación	No
3 Medidas organizacionales	
3.1 Política de ciberseguridad	No
3.2 Mapa de ruta para gobernabilidad de ciberseguridad	No
3.3 Agencia oficial responsable para ciberseguridad	No
3.4 Estadísticas y medidas oficiales para comparaciones	No
4. Construcción de capacidades	
4.1 Estándares oficiales de ciberseguridad, mejores prácticas	No
4.2 Desarrollo profesional de alto nivel en ciberseguridad	No
4.3 Cuantificación de profesionales certificados internacionalmente	No
4.4 Agencias certificadas en materia de ciberseguridad	No
5. Cooperación	
5.1 Marco oficial de trabajo para cooperación a nivel estatal	No
5.2 Marco oficial de trabajo para cooperación a nivel de agencias	No
5.3 Patrocinio para compartir ciberseguridad entre entes públicos y privados	No
5.4 Cooperación Internacional	Sí

Fuente: *Elaboración propia con base en datos del Índice mundial de ciberseguridad y perfiles de ciberbienestar de la UIT (2005)*

Figura 4. *Perfil del estado de ciberseguridad de Honduras*
Fuente: *Presentación íntegra y completa obtenida del Informe Ciberseguridad 2016 del Observatorio de la Ciberseguridad en América Latina y el Caribe, p.82 (BID; OEA, 2016)*

Figura 5. *Perfil del estado de ciberseguridad de Honduras. Detalle de indicadores*
Fuente: *Presentación íntegra y completa obtenida del Informe Ciberseguridad 2016 del Observatorio de la Ciberseguridad en América Latina y el Caribe, p.83 (BID; OEA, 2016)*

4. Conclusiones y Recomendaciones

Las tecnologías de la información (TI) han dejado de ser solamente de soporte, para convertirse ahora en una fuerza estratégica que impulsa la evolución de las sociedades modernas y sustentan el crecimiento social, económico y político de las personas, organizaciones y gobiernos, por igual. Las TI son, además de omnipresentes, esenciales para el progreso. La ciberseguridad es de máxima importancia para el sostenimiento de un modelo tecnológicamente aceptable. 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.

La conciencia de la importancia de desarrollar estrategias de seguridad cibernética está aumentando en los países de América Latina y el Caribe. Algunos de ellos ya tienen una estrategia en operación, como Colombia, Jamaica, Panamá y Trinidad y Tobago. Otros países están en proceso de desarrollo, como Costa Rica, República Dominicana, Perú, Paraguay y Surinam (BID; OEA, 2016). Honduras no cuenta con estrategia de ciberseguridad definida.

Una de las principales preocupaciones planteadas en América Latina y El Caribe ha sido la definición y penalización de los delitos cibernéticos (Symantec, 2014). Brasil, Argentina, México, Paraguay, han tenido experiencias, en algunos casos no del todo exitosas, pero se consideran adelantos en esta materia. En Honduras se comienzan a realizar esfuerzos aislados para materializar procesos legislativos, aunque sin el involucramiento holístico necesario.

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, rara vez suelen intercambiarse esos conocimientos fuera de dicho círculo. 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. Honduras es miembro de ITU-IMPACT[7] y tiene acceso a servicios relevantes de ciberseguridad.

Honduras carece en la actualidad de todos elementos requeridos en el Índice Mundial de Ciberseguridad, entre ellos: legislación criminal, regulación y cumplimiento, centro de respuesta a incidentes, adopción oficial de estándares internacionales, requerimientos de certificaciones para entidades y para profesionales, políticas específicas de ciberseguridad, gobernabilidad y hoja de ruta de ciberseguridad, agencia oficial responsable por la ciberseguridad en el país, estadísticas y mediciones oficiales de ciberseguridad, estandarización en base a mejores prácticas de la industria.

[7] La Alianza Internacional Multilateral contra cibernético (IMPACT) es un socio clave de la Unión Internacional de Telecomunicaciones (UIT), uno de los organismos de las Naciones Unidas (ONU) especializado en el esfuerzo para garantizar la seguridad del ciberespacio para todo el mundo.

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.

5. Bibliografía

Alvarez, L. (2015). Developing the Network for Growth and Equality of Opportunity. En W. E. Forum, *The Global Information Technology Report 2015* (pág. 67). Génova.

BID; OEA. (2016). *Informe Ciberseguridad 2016.*

Center for Strategic and International Studies & McAfee. (2014). *Estimating the Global Cost of Cybercrime.*

Hathaway, M., & Spidalieri, F. (2016). Desarrollo sostenible y seguro: un marco para las sociedades conectadas resilientes. En BID, *Informe Ciberseguridad 2016* (págs. 31-24).

Hernández, R., Fernández, C., & Baptista, M. d. (2014). *Metodología de la investigación.* México D.F.: McGraw-Hill.

ISACA. (2013). COBIT 5. Rolling Meadows, Illinois, Estado Unidos.

ISACA. (2015). *2015 Global Cybersecurity Status Report—Latin America Data.*

Moreno, L. A. (2016). *Informe Ciberseguridad 2016 - Presentación.* BID.

Prandini, P., & Maggiore, M. L. (2011). *Panorama del ciberdelito en Latinoamérica. Documento de trabajo.* Montevideo.

Sidoli, O. C. (2004). Los daños punitivos y el derecho ambiental. *elDial*.

Symantec. (2014). *Tendenccias en Seguridad Cibernética en América Latina y el Caribe 2014.* Obtenido de http://www.symantec.com: http://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Symantec. (2016). *Informe sobre las Amenazas a la Seguridad en Internet de 2016, Volumen 21.*

Tech Insider. (29 de diciembre de 2015). *The 9 worst cyber attacks of 2015*. Obtenido de www.techinsider.io: http://www.techinsider.io/cyberattacks-2015-12

The New York Times Company. (14 de febrero de 2015). *Bank Hackers Steal Millions via Malware*. Obtenido de www.nytimes.com: http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?_r=0

Union Internacional de Telecomunicaciones (UIT). (2014). *Global Cybersecurity Index (GCI)* .

Unión Internacional de Telecomunicaciones (UIT). (29 de 09 de 2016). *Definiciones y términos*. Obtenido de www.itu.int: http://www.itu.int/net/ITU-R/asp/terminology-definition.asp?lang=en&rlink={4B499A4A-3E11-4AE6-9B03-46FB1A662507}

Unión Internacional de Telecomunicaciones, (UIT) División de Aplicaciones TIC y Ciberseguridad. (Abril de 2009). El Ciberdelito: Guía para los países en desarrollo. Ginebra, Suiza.

World Economic Forum. (2015). *The Global Information Technology Report 2015*. Génova.