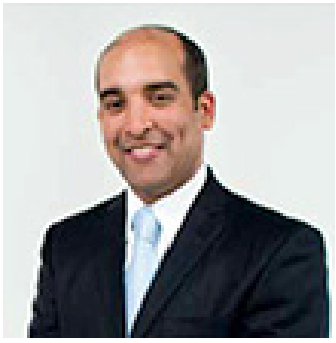
La Educación en Tecnología Aplicada a la Seguridad y Defensa en el Siglo XXI

EDUCATION IN TECHNOLOGY APPLIED TO SECURITY AND DEFENSE IN THE 21ST CENTURY

Recibido: 19/ 11 / 2018 ***Aprobado: 00 / 00 / 2018***



Ing. José Armando Tavárez Rodríguez, MBA, PhD(c),
República Dominicana

El autor es Rector del Instituto Tecnológico de Las Américas (ITLA), con Estudios Avanzados (DEA) Programa Doctorado en Ingeniería (2005) de la Universidad Pontifica de Salamanca (UPSAM), España, Certificado en Políticas de Ciencia y Tecnología (2008) de la Harvard University – Kenedy School of Goverment, Cambridge en Estados Unidos, Ingeniería de Sistemas y Computación (1997) de la Pontificia Universidad Católica Madre y Maestra (PUCMM), República Dominicana, Presidente (2015-2017) de la Asociación Dominicana de Rectores de Universidades (ADRU). Ha realizado publicaciones en revistas: Universidad 4.0, CONECTADOS, Artículo portada; ha dictado charlas y conferencias nacionales e internacionales. jtavarezr@gmail.com

RESUMEN

Las tecnologías de la información y comunicación (TIC) aplicadas a la seguridad y defensa se convierten en una realidad imperante en el mundo digital en que vivimos. El incremento constante de las amenazas y los ataques en el ciberespacio obligan a los gobiernos y diferentes organismos de seguridad pública y privada a desarrollar innovaciones tecnológicas y acciones de formación que permitan incrementar un frente de ciberdefensa que permita incrementar la seguridad de los ciudadanos que toca defender y proteger.

En el curso de los últimos treinta años el mundo se ha digitalizado de manera progresiva. Se ha producido un desarrollo importante de ecosistemas de innovación y desarrollo en torno al tema de cómo podemos generar innovaciones tecnológicas que puedan ser aplicadas a la seguridad y la defensa. Es por eso que diferentes actores deben trabajar de manera coordinada para asegurar una estrategia de ciberseguridad que permita la construcción de un ciberespacio cada vez más seguro.

El presente artículo se enfoca en analizar la necesidad creciente de profesionales especializados en seguridad informática o ciberseguridad y la respuesta que están dando a esta realidad las diferentes instituciones educativas a nivel nacional e internacional, así como los organismos de gobierno. Se describe a modo de panorama general la realidad educativa nacional en lo que tiene que ver con programas formales de educación en materia de tecnologías aplicadas a la seguridad y defensa, así como el correspondiente marco legal que la sustenta.

Palabras clave:

Seguridad, defensa, tecnologías de la información y comunicación (TIC), ciberterroismo, ciberdefensa, ciberseguridad, ciberguerra.

ABSTRACT

The information and communication technologies (ICT) applied to security and defense become a prevailing reality in the digital world in which we live. The constant increase in threats and attacks in cyberspace oblige governments and deferential public and private security agencies to develop technological innovations and training actions that allow the development of a cyberdefense front that increases the security of citizens who have to defend and protect.

In the course of the last thirty years, the world has been progressively digitized. There has been a significant development of innovation and development ecosystems around the issue of how we can generate technological innovations that can be applied to security and defense. That is why different actors must work in a coordinated manner to ensure a cybersecurity strategy that allows the construction of an increasingly secure cyberspace.

This article focuses on analyzing the growing need for professionals specialized in computer security or cybersecurity and the response that this different reality is giving to different national and international educational institutions, as well as government agencies. The national educational reality is described as a general panorama in what has to do with formal education programs in the field of technologies applied to security and defense, as well as the corresponding legal framework that sustains it.

Keywords:

Security, defense, information and communication technologies (ICT), cyber-terrorism, cyberdefense, cybersecurity, cyberwar.

Introducción

Las tecnologías de la información y comunicación (TIC) han transformado radicalmente el mundo en que vivimos. Todas las áreas vitales del ser humano se sirven de las TIC para lograr sus objetivos. La educación, la salud, la administración pública y los negocios son algunos sectores que están haciendo uso intensivo de las tecnologías digitales para el trabajo que tienen que realizar para beneficio de la sociedad.

En este sentido, la seguridad y defensa son unos de los ambientes donde adquieren mayor relevancia las innovaciones tecnológicas. No podemos vivir en un mundo seguro sin el uso eficiente y práctico de las mismas. De hecho, gran parte de las innovaciones que disfrutamos en la vida diaria tienen su origen en los diferentes departamentos de investigación de los ministerios de defensa de varios países del mundo.

Como ejemplo de esta realidad podemos mencionar al Internet. Sus inicios están vinculados a la Defense Advanced Research Projects Agency (DARPA), que es el mayor laboratorio de investigación e innovación del mundo, donde se crearon la mayor cantidad de innovaciones tecnológicas del siglo pasado. Ciertamente, en sus inicios, esos proyectos de investigación tenían el propósito de que sus resultados sean aplicados a la defensa nacional, pero luego muchos de esos resultados se aplicaban a la vida diaria de los ciudadanos.

En un mundo cada vez más digital, existen nuevos peligros y amenazas que esos organismos de defensa y seguridad deben tomar en cuenta. Existen nuevas realidades como el ciberterrorismo y la ciberguerra. Por ejemplo, según un reciente informe elaborado por el Fondo Monetario Internacional, titulado "Cyber Riskforthe Financial Sector: A Framework for Quantitative Assessment", los ataques informáticos podrían representar para el sector financiero mundial pérdidas cercanas a los 100 mil millones de dólares. Estas realidades obligan a los países a plantearse la necesidad de contar estrategias de ciberseguridad y ciberdefensa. En dichos planes se reconoce la necesidad de contar con profesionales debidamente capacitados en estas áreas emergentes e implementar acciones que conduzcan al establecimiento y crecimiento de una clase profesional especializada en ciberseguridad.

Conceptos y términos

La ciberseguridad es "el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras". Una de las instituciones especialistas en temas de ciberseguridad más prestigiosas del mundo señala que es "la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos"[1] . Esta nueva disciplina tecnológica es una más de las diferentes tecnologías emergentes que avanzan actualmente en el planeta como la Inteligencia Artificial, la Robótica, el Internet de las Cosas, la Computación en la Nube y el Big Data o Ciencia de los Datos.

La cibernética es la disciplina que integra la mayor parte de las tecnologías emergentes como la robótica e inteligencia artificial. Algunas universidades, reconociendo la necesidad de personas formadas en estas nuevas tecnologías, han ido creando programas de formación que dan respuestas a esta demanda creciente de profesionales. Como ejemplo podemos citar al Instituto Tecnológico de Massachussets (MIT) que acaba destinar un billón de dólares para la creación de una nueva facultad dedicada a la enseñanza e investigación en inteligencia artificial.

La formación técnica y tecnológica es aquella que desarrolla capacidades laborales y competencias o habilidades en los estudiantes que le permiten desarrollar soluciones concretas a problemas reales en los diversos entornos de trabajo. En lo que respecta a ciberseguridad, necesitamos la diversificación nacional de la oferta educativa en esta materia. Instituciones como el Instituto Nacional de Formación Técnica y Profesional (INFOTEP), las universidades e instituciones de educación superior, así como los politécnicos, escuelas y colegios de nuestro país, deben garantizar la formación en ciberseguridad como elemento fundamental del currículo educativo que ejecutan en las aulas.

Las TIC, la educación técnica y tecnológica

El mundo ha experimentado en los últimos veinte años un proceso de incremento de la demanda de profesionales especializados en tecnologías, ingenierías y ciencias. Según los datos de la secretaria de trabajo de los Estados Unidos de América, el país no está en condiciones de producir la cantidad y calidad de expertos informáticos en las áreas señaladas. Este fenómeno no solo está sucediendo en esa potencia mundial. Afecta por igual a todos los países del mundo. Así lo confirman los últimos reportes en la materia de organismos internacionales como el Banco Mundial (BM) o el Banco Interamericano de Desarrolllo (BID).

En reacción a esta situación, las diversas naciones han implementado medidas o políticas públicas que buscan atraer el mejor talento de otros países. Esto se conoce como un proceso de "Brian Gain" que consiste en la capacidad de atracción de talentos humanos que tienen las

1 KasperskyLab. Recuperado de: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

naciones para trabajar en diferentes disciplinas. El efecto contrario es el "Brain Drain" que consiste en la pérdida de talentos humanos y profesionales que experimentan los países cuando éstos deciden migrar a otros lugares del planeta donde se les ofrecen mejores oportunidades sociales y económicas.

Esta realidad nos lleva a reflexionar sobre las grandes necesidades de profesiones en tecnológicas digitales que estén especializados en seguridad y defensa. Es decir, este mismo fenómeno de escasez y consecuente competencia alta por atraer y retener talento humano, se manifiesta en el sector de ciberseguridad.

Nuestro país no cuenta con la cantidad suficiente de expertos y profesionales en el área de seguridad informática. Hace apena dos años que algunas universidades han creado programas de formación profesional en esa materia. Destaca, entre otras, el Instituto Tecnológico de Santo Domingo (INTEC), que posee actualmente una maestría en ciberseguridad.

Por otro lado, el Instituto Tecnológico de las Américas (ITLA) es la única institución de educación superior con una carrera de dos años en seguridad informática o ciberseguridad. Con esta novedosa oferta académica, el ITLA responde de manera satisfactoria a los requerimientos que hacen los sectores productivos nacionales, sobre todo en el área de la banca y de las telecomunicaciones, de profesionales especializados en todas las áreas que tienen que ver con la ciberseguridad.

La pertinencia de estos programas es muy alta. Los diversos sectores de la economía nacional manifestaban la falta, en el mercado laboral, de talentos expertos en defender sus redes y datos electrónicos. Algunas instituciones tenían que atraer talento de otros países o "re-entrenar" algunos profesionales de otras disciplinas, con la consecuencia del aumento de costos en sus negocios y la imposibilidad de ofrecer servicios seguros a sus clientes.

También el Gobierno o la administración pública en sentido general se ha visto afectada por la imposibilidad de contratar personal especializado en ciberdefensa o ciberseguridad. Los organismos de inteligencia, de seguridad nacional y de protección y defensa de los ciudadanos constantemente requerían de las universidades dominicanas e instituciones de formación profesional el establecimiento de programas que permitieran aumentar la cantidad de especialistas en el mercado laboral. Ningún país puede asegurar un ambiente protegido a sus ciudadanos sin contar con los agentes o personal de seguridad debidamente entrenado.

Con especial énfasis se acercaban a las instituciones de formación los diferentes organismos nacionales encargados de investigar y sancionar el delito electrónico o digital. Tanto el ministerio público como la suprema corte de justicia ha establecido proyectos con apoyo de organismos internacionales para impartir talleres, diplomados y cursos para cubrir la necesidad insatisfecha de talentos a nivel nacional. Las instituciones como INTEC e ITLA han reaccionado creando nuevas carreras y supliendo parte de

estas necesidades mediante programas de educación continua o técnica profesional.

Marco regulatorio y proyecto República Digital

En el país se cuenta con un adecuado marco regulatorio en materia de ciberseguridad. Si bien es cierto que todo es perfectible, podemos decir que desde el 2007 la República Dominicana cuenta con una ley contra los delitos y crímenes de alta tecnología, la número 53-07. Dicha ley crea una comisión interinstitucional integrada por todos los organismos que tienen vinculación con la ciberdefensa del país y el combate y persecución del delito electrónico o digital.

Esa comisión está compuesta por la Procuraduría General de la República, la Policía Nacional, la Departamento Nacional de Investigaciones, el Ministerio de Defensa, el Ministerio de Interior y Policía, la Dirección Nacional de Control de Drogas, el Consejo Nacional para la Niñez y la Adolescencia (CONANI), el Instituto Dominicano de las Telecomunicaciones y el Instituto Tecnológico de las Américas (ITLA). La preside la Procuraduría General y el ITLA ocupa la Secretaría General. Tienen la misión de articular todos los esfuerzos en la materia con los diferentes organismos que la componen así como la propuesta de estrategias, planes y acciones que permitan combatir las amenazas de ataques cibernéticos así como la persecución del delito electrónico.

El objetivo de dicha ley es "la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de esas tecnologías en perjuicio de personas físicas o morales, en los términos previstos en esta ley. La integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten, a través de éstos, las transacciones y acuerdos comerciales o de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de éstos, son todos bienes jurídicos protegidos".

Por otro lado, en este año, el presidente de la República Dominicana, licenciado Danilo Medina, creó por decreto número 230-18, la Estrategia Nacional de Ciberseguridad. República Dominicana es uno de los 10 países de la región con una estrategia de Ciberseguridad. Decreto-230-18. Ese decreto "establece la Estrategia Nacional de Ciberseguridad, para fortalecer las capacidades nacionales de prevención, detección y respuesta a los ataques cibernéticos al Estado, a los ciudadanos y a los sectores productivos". Además, el decreto crea el Centro Nacional de Ciberseguridad para ejecutar, desarrollar, actualizar y evaluar esa estrategia. Su misión es "establecer los mecanismos adecuados de ciberseguridad que protejan al Estado, sus habitantes y en general, del desarrollo y la seguridad nacional". Y su visión al 2021 es que la República Dominicana cuente con un "ciberespacio más seguro, en el que estén implementadas las medidas necesarias para el desarrollo

confiable de las actividades productivas y lúdicas de toda la población, de conformidad con la Constitución y demás leyes del ordenamiento jurídico dominicano".

La antes mencionada Estrategia Nacional de Seguridad Cibernética está articulada a la Estrategia Nacional de Desarrollo y se apoya en el proyecto República Digital, así como las diferentes directrices de seguridad y defensa de la República Dominicana, como se muestra en la siguiente ilustración.

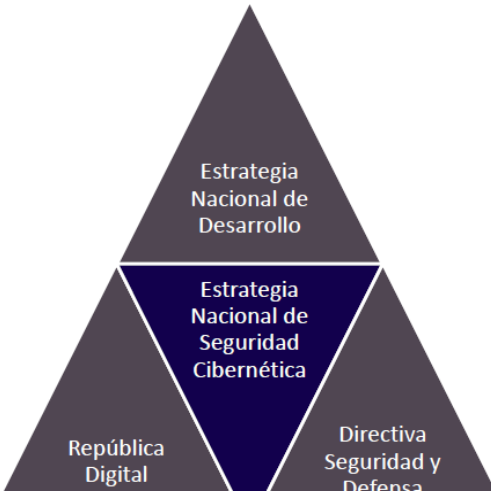


Fig. 1 Estrategia Nacional de Seguridad Informática. Fuente: República Digital.

Además, esa estrategia descansa en 4 pilares que permiten garantizar la operatividad de la misma y el consecuente éxito en el logro de sus objetivos o metas. Los pilares de la estrategia son: marco legal y fortalecimiento institucional, protección de infraestructuras críticas nacionales e infraestructuras TI del estado, educación y cultura digital de ciberseguridad, y alianzas nacionales e internacionales.

Para el presente artículo, se enfatiza más el tercer pilar de educación y cultura digital en ciberseguridad. El mismo ofrece una visión amplia y holística de la necesidad detectada de formación de las conciencias de los ciudadanos, así como la creación de una masa crítica de talentos tecnológicos en materia de Ciberseguridad. Es importante señalar que esa competencia corresponde al Instituto Tecnológico de las Américas (ITLA) según el artículo 35 de la ley 53-07.

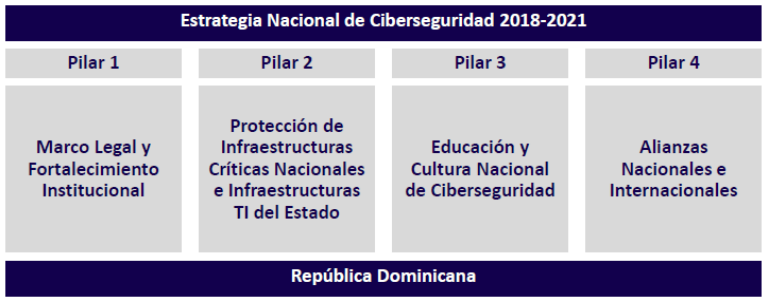


Fig. 2 Los cuatro pilares de la Estrategia Nacional de Ciberseguridad 2018-2021. Fuente: República Digital.

La educación y cultura nacional de Ciberseguridad

Uno de los elementos fundamentales para el desarrollo de la Estrategia Nacional de Ciberseguridad es contar con los profesionales debidamente formados tanto en cantidad como en calidad. Ya mencionamos que el país cuenta con dos universidades que ofrecen programas de grado y postgrado en la materia. También existen muchas instituciones que ofrecen diplomados, cursos, webinarios, talleres, con-

ferencias y congresos en ciberseguridad. Existe en el país una amplia oferta de certificaciones internacionales sobre los diferentes enfoques de capacitación en ciberseguridad,

Existe en la oferta académica de las universidades dominicanas una Maestría en Ciberseguridad ofrecida por INTEC y un tecnólogo en seguridad informática ofrecido por el ITLA. Ambas son ofertas novedosas y de reconocida calidad con una demanda creciente de personas que quieren adquirir esos conocimientos, habilidades y destrezas, así como la correspondiente acreditación o certificación académica.

Sin embargo, se podría afirmar que donde existen mayores posibilidades de avance en materia formativa radica en la educación ciudadana. Las personas necesitan estar concientizadas de la importancia que tiene la implementación de mejores prácticas que permitan atenuar la incidencia de crímenes o delitos cibernéticos. El comportamiento ciudadano es fundamental para que esto pueda tener el impacto esperado. Además, la formación del liderazgo nacional, tanto público o privado, es fundamental para que puedan asumir con responsabilidad las medidas para combatir ese mal cibernético.

CONCLUSIÓN

En la República Dominicana, al igual que en muchos países de la región, se han establecido las normativas y los marcos regulatorios que permiten un desarrollo adecuado de las tecnologías aplicadas a la seguridad y defensa, así como la formación adecuada de los ciudadanos en la materia. No basta con un proceso de cultura digital y concientización sobre la ciberseguridad. Se necesita establecer un plan nacional de formación a nivel profesional en TIC aplicadas a la defensa y seguridad de nuestro país. El país necesita al menos cinco mil profesionales que puedan ayudar a mantener y aumentar el desarrollo de nuestra nación. Para estos fines y luego de analizar la realidad nacional en la materia, podemos afirmar que:

- Se hace necesario aplicar lo contenido en la ley 57-03 contra crímenes y delitos de alta tecnología, donde confiere al Instituto Tecnológico de las Américas (ITLA) la responsabilidad de diseñar y coordinar la implementación de un plan nacional de formación en esta materia.
- Es importante fortalecer los apoyos que los diversos sectores están dando al proyecto de República Digital. El mismo crea un ambiente propicio para el fortalecimiento del país en materia de ciberseguridad y la consecuente mejora de los indicadores a nivel global.
- Todos los actores de la sociedad deben aunar esfuerzos para que los ciudadanos estén comprometidos con la ciberseguridad y aprendan cuáles son las prácticas más adecuadas que debemos ejecutar como sociedad para defendernos de las posibles amenazas o ataques.

Referencias Bibliográficas

Amorós, M. R. A. (2005). Ciberseguridad. El compromiso de los Estados a partir de la Cumbre Mundial sobre la Sociedad de Información. Telos: *Cuadernos de comunicación e innovación*, (63), 101-109.

Banco Mundial (2017). *Informe "Momento Decisivo" sobre la Educación Superior en América Latina y el Caribe*. Washington, EUA.

Cano, J. J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. SISTEMAS *(ASOCIACION COLOMBIANA DE INGENIEROS DE SISTEMAS)*, 119, 4-7.

Feliu Ortega, L. (2012). *La ciberseguridad y la ciberdefensa*. España: Ministerio de Defensa de España.

Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en Enfoque Top-Down desde una visión global a una visión local. *Revista Latinoamericana de Ingeniería de Software*, 3(4), 161-176.

Ley No. 53/07. Sobre crímenes y delitos de alta tecnología. *Gaceta Oficial*. Santo Domingo, República Dominicana, 23 de abril de 2007, núm. 10416, pp 17-40

Ubiñas, D. B. (2013). La protección de sistemas de información crítica y la Ley 53/07 de la República Dominicana sobre crímenes y delitos de alta tecnología. *Revista Penal*, (32), 60-71.

"What is Computer security?", Matt Bishop, *IEEE Security and Privacy Magazine* 1(1):67 - 69, 2003. DOI: 10.1109/MSECP.2003.1176998

KasperskyLab.https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security