8-9-2021

Reflexiones y retos para la academia en la formación de profesionales de seguridad/ciberseguridad en Colombia: 2010 - 2020

Jeimy Cano
Universidad de los Andes, jjcano@yahoo.com

Andrés Almanza
Asociación Colombiana de Ingenieros de Sistemas, andres_almanza@hotmail.com

Reflexiones y retos para la academia en la formación de profesionales de seguridad/ciberseguridad en Colombia: 2010 - 2020

Artículo Completo

Jeimy J. Cano M.
Universidad de los Andes/ACIS
jcano@uniandes.edu.co

Andrés Almanza
Universidad Externado de Colombia/ACIS
andres.almanza@uexternado.edu.co

Abstract

The evolutionary study of the role of the academy and its challenges in the training of security/cybersecurity professionals in Colombia is an effort made by the Colombian Association of Systems Engineers (ACIS in spanish), which for more than 20 years has been applying a national information security survey in order to study and understand the behavior of security in the Colombian context. The analysis of the results of the last 10 years in the selected topic shows the most relevant trends in the country, based on the challenges that the academy has faced in the formation of security/cybersecurity programs, as well as the data related to the creation of training programs in security/cybersecurity registered by the Ministry of National Education. The reflections that are raised reveal, among others, the most outstanding challenges such as research levels, required infrastructure and strategic alliances, which are contrasted with the readings of international reports and research articles in order to place some concrete proposals for higher education institutions in Colombia in this area.

Keyword

Cybersecurity; Security; Evolution; Colombia; Analysis; Colombia; Academia.

Resumen

El estudio evolutivo del rol de la academia y sus retos en la formación de profesionales seguridad/ciberseguridad en Colombia es un esfuerzo realizado por la Asociación Colombiana de Ingenieros de Sistemas (ACIS), quien durante más de 20 años ha venido aplicando una encuesta nacional de seguridad de la información con el fin de estudiar y entender el comportamiento de la seguridad en el contexto colombiano. El análisis de los resultados de los últimos 10 años en la materia seleccionada muestra las tendencias más relevantes en el país, basadas en los retos que ha tenido la academia en la formación de los programas de seguridad/ciberseguridad, así como los datos relacionados con la creación de programas de formación en seguridad/ciberseguridad registrados por el Ministerio de Educación Nacional. Las reflexiones que se plantean revelan entre otros, los desafíos más destacados como son los niveles de investigación, la infraestructura requerida y las alianzas estratégicas los cuales se contrastan con las lecturas de reportes internacionales, y artículos de investigación con el fin de situar algunas propuestas concretas para las instituciones de educación superior en Colombia en esta temática.

Palabras Clave

Ciberseguridad; Seguridad; Evolución; Colombia; Análisis; Longitudinal; Academia.

Introducción

El aumento de la densidad digital en el desarrollo de la dinámica social, el creciente número de brechas de seguridad y control, y el uso del ciberespacio como nuevo teatro de operaciones cibernéticas, establece un escenario de tensiones y retos que la ciberseguridad como disciplina emergente debe atender con el fin de motivar mejores prácticas, generar elementos que aumenten la confianza digital y desarrollar un pensamiento sistémico que permita comprender la perspectiva relacional y anidada de conexiones entre los diferentes actores y componentes de la realidad digital (Cano, 2021).

En este sentido, formar los nuevos profesionales en seguridad/ciberseguridad, no sólo exige revisar los planes de estudio, sino las estructuras estratégicas y operativas necesarias para darle la profundidad y efectividad a las experiencias y prácticas requeridas en las diferentes industrias, así como la promoción de la investigación, desarrollo e innovación necesaria para mantener el interés y el avance de este nuevo campo del conocimiento (Catota et al., 2019). La limitada oferta actual de habilidades en los temas de seguridad/ciberseguridad restringe la puesta en operación de procesos y actividades que habiliten propuestas de productos y servicios digitales que cambien la manera de hacer las cosas (Oxford Martin School, 2018).

Al estudiar la percepción de la industria frente al reto de la academia en la formación de profesionales en seguridad/ciberseguridad, se pueden encontrar algunos vacíos y oportunidades en los planes de estudio actuales de los programas de formación, así como alternativas para aumentar la motivación de las personas para ingresar a este tipo de carrera. De acuerdo, con estudios recientes los profesionales en mención buscan demostrar su experiencia a medida que la tecnología cambia y las tendencias de la industria emergen, con el fin de mantenerse actualizados y con habilidades claves para responder a los retos de eventos adversos y ataques novedosos que terminen comprometiendo la promesa de valor de las empresas (Švábenský et al., 2020).

Los resultados de la Encuesta Nacional de Seguridad Informática (ENSI) ejercicio de exploración y análisis de las prácticas y gestión de la seguridad informática en Colombia, que se ha venido realizando en los últimos 20 años con el apoyo de la Asociación Colombiana de Ingenieros de Sistemas (ACIS), establecen algunas tendencias en sus diferentes variables estudiadas. Particularmente, para este estudio se ha tomado la variable relacionada con el rol de la academia en la formación de los profesionales de seguridad de la información en Colombia, entre los años 2010 a 2020, en los cuales se indaga sobre el ofrecimiento de programas, las capacidades disponibles para su desarrollo, difusión de los mismos, las alianzas requeridas y la tensiones permanentes con las certificaciones generales y de producto.

Cada una de las temáticas estudiadas alrededor del rol de academia muestran patrones de interés para las instituciones de educación superior (IES), donde se advierte que el nivel de investigación en el área es escasa o insuficiente, que existen limitados laboratorios e infraestructura para soportar los cursos especializados y que existen pocas o nulas alianzas con proveedores de tecnología de seguridad y/o asociaciones o entidades relacionadas con el tema. Lo anterior, establece ventanas de oportunidad para mejorar las estrategias de las IES de cara al fortalecimiento de la oferta de programas en seguridad/ciberseguridad en Colombia, como elemento estratégico de la política pública relacionada con seguridad y confianza digital (CONPES, 2020).

En resumen, este artículo se desarrolla desde una vista general de antecedentes que contextualiza el estudio, seguidamente se detallan sus aspectos metodológicos, se hace una breve mención sobre el instrumento utilizado para la investigación, así como de la población encuestada, para finalmente terminar con los resultados, su análisis y las conclusiones más relevantes.

Antecedentes

La formación de los profesionales de seguridad/ciberseguridad es un elemento indispensable e importante en el desarrollo de las capacidades de las organizaciones y las naciones (OEA, 2020). Conocer los retos de esta formación y cómo estos se adaptan en el tiempo es clave para preparar no solo a los profesionales del presente sino del mañana, quienes harán frente a los eventos disruptivos de los ambientes digitales existentes y emergentes.

Así mismo, el contraste de estos resultados con las tendencias y artículos internacionales configura un espacio de análisis extendido que enmarca la realidad de este estudio para situar los retos que la academia tiene de cara a formar profesionales en materia de formación seguridad/ciberseguridad.

Metodología

En esta sección se presentan los aspectos metodológicos de esta investigación, describiendo los detalles del proceso realizado, la preparación del instrumento de recolección, la estrategia de recolección de la información, así como los ejercicios propios de la tabulación de los datos.

Perspectiva metodológica

Este estudio, hace una lectura cualitativa del entorno basado en una encuesta de selección múltiple, cuyos resultados son revisados con apoyo de elementos cuantitativos de estadística básica para comprender los factores o fenómenos relevantes a los retos de la academia en el tema de seguridad/ciberseguridad contexto colombiano. En este sentido, se considera que la percepción de estos retos se funda en las interacciones e interrelaciones que las empresas y las personas desarrollan para construir y manifestar una realidad particular y propia del país, sin perjuicio de sus semejanzas con otras naciones en el mundo. Por tanto, bajo esta perspectiva se busca entender la experiencia que las personas comparten en ciertas temáticas consideradas claves en materia de seguridad y ciberseguridad. En particular, se toman las respuestas de la Encuesta Nacional de Seguridad Informática (ENSI) realizada por la Asociación Colombiana de Ingenieros de Sistemas (ACIS), en el componente relativo a la percepción que se ha tenido de las instituciones de educación superior en cuanto a la formación de profesionales de seguridad de la información.

Instrumento de investigación

Este estudio se realiza basado en una de las variables de la encuesta nacional de seguridad informática que consta de un cuestionario de 40 preguntas, con selección múltiple (incluida la opción abierta para otros, cuando es necesario), donde cada participante de la encuesta en línea puede indicar sus preferencias y establecer, basado en su experiencia, las respuestas con las que más se identifique. Lo anterior corresponde a la observación de fenómenos tal y como se dan en un entorno, sin la intervención directa de los investigadores, con el fin de examinar los cambios que se dan a lo largo del tiempo en grupos específicos que están vinculados con las labores relacionadas con la gestión y el gobierno de la seguridad de la información en Colombia.

En relación con el análisis del rol de la academia en la formación de los profesionales de seguridad de la información en Colombia, tenemos:

- Ofrecimiento de programas: Si las universidades están ofreciendo programas de pregrado y postgrados en el tiempo, duración de estos.
- Capacidades: Relacionadas con el nivel de investigación, las infraestructuras para realizar la investigación y la formación, el nivel de los docentes para impartir los contenidos.
- Difusión: Que tanto las poblaciones de profesionales conocen los programas que existen
- Alianzas con múltiples sectores: Creación de vínculos para fortalecer el crecimiento de la seguridad de la información en el país
- Tensión existente entre certificaciones y formación

Población encuestada

La ENSI año tras año es distribuida a través de correo electrónico, a una comunidad de más de 3000 profesionales registrados en la Asociación Colombiana de Ingenieros de Sistemas (ACIS), redes sociales y grupos o comunidades de ciberseguridad/seguridad de la información en Colombia, más de 10 grupos y/o comunidades de alrededor de 500 personas o más, para ser diligenciada de manera virtual, a través de un formulario en la Web configurado a través de la plataforma Surveymonkey. La población seleccionada

responde a la comunidad de seguridad de la información que se tiene en Colombia, que se coordina desde la ACIS hace 20 años, quienes están al frente de las operaciones y gerencia del área en el país, de los cuales, en promedio participan 186 profesionales a nivel nacional (Cano & Almanza, 2020).

Planificación del documento

Anualmente se hace una revisión y análisis del cuestionario utilizado por parte de los investigadores que apoyan el proceso de ejecución y desarollo de la encuesta, con el fin de efectuar los ajustes que sean necesarios y así contar con un instrumento más depurado y acorde con la evolución de las temáticas en seguridad de la información.

Luego de estas adecuaciones y modificaciones se procede configurar la plataforma virtual destinada para tal fin, para realizar las pruebas de funcionalidad y de cohesión en relación con la dependencia de las preguntas. Seguidamente se hace el despliegue de la encuesta en todas las comunidades que se han definido.

Procesamiento

Una vez concluida la encuesta se extraen las respuestas totales del cuestionario en una hoja cálculo, para adelantar el estudio de los datos planeados utilizando otras herramientas de analítica de datos que permitan generar reflexiones particulares a cada una de las temáticas del cuestionario, así como vistas cruzadas de algunos de los temas de interés. En particular, se presentan a continuación los resultados para la variable rol de la academia en la formación de los profesionales de seguridad de la información en Colombia, los cuales se complementan con una revisión de la oferta académica disponible en seguridad/ciberseguridad en Colombia.

Limitaciones de este estudio

El estudio realizado sobre los retos para la academia en los temas de formación en seguridad/ciberseguridad en la última década busca perfilar la dinámica de esta realidad y establecer marcos de acción concretos que sean de interés para la academia. En este sentido, adelantar una correlación con otras variables, si bien puede resultar de interés, los resultados sólo serán revisados en el contexto de la oferta académica de programas de posgrado disponible en Colombia. Una comparación en el escenario latinoamericano deberá ser tema para un siguiente estudio.

Resultados

Los resultados que se presentan a continuación corresponden a los valores promedios más importantes y relevantes de la encuesta en la dimensión relacionada con el rol de la academia en la formación de los profesionales de seguridad de la información en Colombia en el periodo comprendido entre 2010 y 2020.

Rol de la Academia en la formación del Profesional de Seguridad de la Información

Los resultados señalan que en Colombia se reconoce el ofrecimiento de programas en materia de seguridad por parte de la academia con un 35% de promedio en la última década. Sin embargo, se resalta que a pesar de ello el nivel de investigación en la materia es escaso (34%). De igual forma, la infraestructura disponible para desarrollar los procesos de investigación, así como para adelantar los cursos ofertados es limitada (30%). Sin perjuicio de lo anterior, se reconocen alianzas fortalecidas entre la academia, el sector empresarial y el gobierno para desarrollar mejores capacidades en los temas de seguridad de la información (30%).

Las certificaciones generales y de producto se han convertido en un factor determinante para los profesionales en seguridad de la información, tanto que el 27% en promedio considera que han desplazado a los programas formales de educación, el 25% manifiesta que las universidades no hacen los esfuerzos suficientes para divulgar sus programas, y adicionalmente, el 25% asocia los temas de formación en seguridad con cursos cortos que imparten las universidades.

En las líneas finales se observa que el 18% en promedio considera que los profesores tienen poca formación en el tema de seguridad/ciberseguridad, y un 16% en su media manifiesta no tener mucha motivación a la hora de formarse en estos tópicos. Finalmente, un 10% cree que las universidades no ofrecen ningún tipo de programa o curso corto en materia de seguridad. Los datos se muestran en la tabla 1.

Criterios	Valores
Están ofreciendo programas académicos de grado y/o posgrados formales en esta área	35%
El nivel de investigación en el área es escasa o insuficiente	34%
Existen limitados laboratorios e infraestructura para soportar los cursos especializados	30%
Hay pocas (o nulas) alianzas con proveedores de tecnología de seguridad y/o asociaciones o entidades relacionadas con el tema	30%
Se han dejado desplazar por certificaciones generales y de producto	27%
Hacen poca difusión sobre estos temas	25%
La formación se limita a cursos cortos	25%
Los profesores tienen poca formación académica en el tema	18%
Hay poca motivación de los estudiantes para estudiar el tema	16%
No ofrecen programas académicos o cursos cortos en esta área	10%

Tabla 1. Criterios relacionados con el rol de la academia en la formación de profesionales de seguridad

Oferta académica en Seguridad de la Información en Colombia

Al revisar cómo ha evolucionado la creación de programas de postgrado en Colombia, y examinados los datos del Ministerio de Educación Nacional (MEN) a través del Sistema Nacional de Información de Educación Superior (SNIES), tenemos los siguientes resultados fruto de la revisión realizada con corte al 1 de junio de 2021.

Se encuentra que en Colombia existen un total de 87 programas registrados, en todo el territorio nacional, de los cuales se pueden distribuir de la siguiente manera. El 86,21% a la fecha se encuentran activos y solo el 13,79% se encuentran inactivos. El 42,53% son desarrollados por instituciones públicas y el 57,47% son ofertados por instituciones privadas.

En cuanto al carácter académico se tienen definidas 4 categorías (MEN, 2019) presentadas en la Tabla 2.

Carácter Académico	Porcentajes
Institución Técnica Profesional	1,15%
Institución Tecnológica	32,18%
Institución Universitaria/Escuela Tecnológica	34,48%
Universidad	32,18%

Tabla 2. Carácter Académico de las instituciones

El nivel académico está representado en dos categorías, programas de postgrado que representa el 86,21% y el 13,79% representa al nivel de pregrado. En esa misma línea está el nivel de formación, que acorde a las definiciones del MEN (MEN, 2019) cuenta con 5 categorías, representadas en la tabla 3.

Niveles de Formación	Porcentajes
Especialización universitaria	47,13%
Especialización tecnológica	32,18%
Tecnológica	11,49%
Maestría	6,90%
Universitaria	1,15%

Tabla 3. Nivel de Formación

La distribución geográfica de la oferta académica está representada en las principales ciudades del país y algunos de estos programas se encuentran disponibles de manera virtual, para ganar mayor cobertura a nivel nacional. Los detalles se observan en la tabla 4 y tabla 5.

Ciudad del Programa	Porcentajes
Bogotá, D.C.	34,48%
Medellín	11,49%
Cali	6,90%
Barranquilla	5,75%
Bucaramanga	4,60%
Facatativá	3,45%
Popayán	3,45%
Pereira	2,30%
Manizales	2,30%
Valledupar	2,30%
Armenia	2,30%
Cartagena de Indias	2,30%
Girardot	2,30%
Rionegro	1,15%
Dosquebradas	1,15%
Santa Rosa de Osos	1,15%
Envigado	1,15%
Coveñas	1,15%
Barrancabermeja	1,15%
San José de Cúcuta	1,15%
Neiva	1,15%
Sincelejo	1,15%
Tunja	1,15%
Piedecuesta	1,15%
Vélez	1,15%
Ibagué	1,15%
Lenguazaque	1,15%

Tabla 4. Ciudad del programa

Modalidad de los programas	Porcentajes
Presencial	86,21%
Distancia (virtual)	11,49%
Distancia (tradicional)	2,30%

Tabla 5. Modalidad de los programas

Análisis de Resultados

Formación de profesionales de seguridad, una historia para contar.

La formación de profesionales de seguridad en Colombia, según los datos del sistema de información del MEN (SNIES) inicia en el año 1999, hasta su último programa registrado en el año 2020. Para el caso de este estudio, se han revisado 10 años de la creación de programas de ciberseguridad, seguridad de la información y afines, dentro de los cuales ha existido una oferta variada de programas en el país.

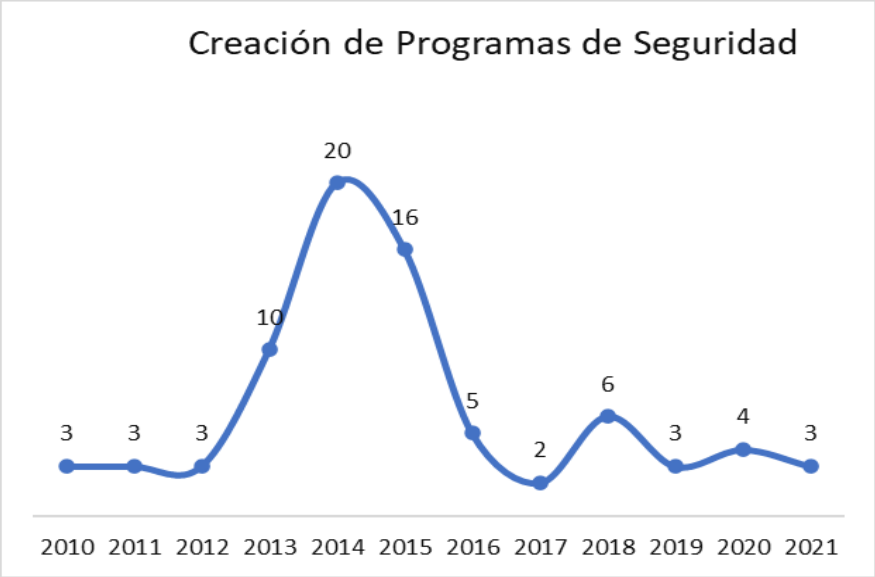

Figura 1. Historia de Creación de Programas

La figura 1, muestra que durante el periodo de estudio se han creado 78 programas en relación con la ciberseguridad y seguridad de la información, con especial atención al rango de años entre 2013 y 2015, en los cuales se crearon un total 46 programas y específicamente el año 2014 con 20 programas en total. En la actualidad, están activos 72 programas.

En la misma línea se encuentra que del total de los 72 programas activos, el 90% son de orientación a los postgrados y el 10% de orientación a los programas de pregrado. En relación con el nivel de formación en ese periodo se encuentra que el 47% de los programas son especializaciones universitarias, el 32% son especializaciones tecnológicas, el 11% corresponden a programas de formación tecnológica, el 8% corresponden a programas de maestría, el 1% asociado con programas de pregrado universitario y el 1% como formación técnica profesional.

Los procesos de creación de programas de seguridad para los años 2013 al 2015 pueden explicarse por varios elementos. Primero por la definición de una Política Nacional de Ciberseguridad en 2011, donde uno de sus lineamientos era construir capacidades de ciberseguridad y ciberdefensa y entre ellas, el fortalecimiento del talento humano en ciberseguridad (CONPES 3701, 2011). Este documento daba lineamientos generales para proponer programas de formación y permitir el desarrollo de capacidades y talento humano que pudiera atender la demanda. Un segundo factor global está relacionado con la necesidad ofertar programas de educación superior del tipo posgrado que pudieran atender la demanda que ya se empezaba a notar en materia de talento humano en ciberseguridad (Cabaj et all, 2018).

Esto resultado hace evidente las iniciativas de las instituciones de educación superior para ofrecer programas a todo el conjunto de profesionales que recién empezaban a tener una posición en el mercado laboral, con el fin de cubrir las plazas que se venían ofertando en el país en materia de seguridad de la información (Cano & Almanza, 2020).

Rol de la Educación, aprendizajes de un proceso de largo plazo

Dentro de la Encuesta Nacional de Seguridad Informática y los datos recolectados en el transcurso de la última década, se tienen identificados algunos criterios que son parte del estudio de evaluación para entender la percepción que tiene la industria sobre el rol que desempeña la academia en el contexto de la seguridad/ciberseguridad.

Los desafíos futuros de la fuerza laboral en seguridad/ciberseguridad deben abordarse fomentando carreras de ciberseguridad en los países y estos esfuerzos deben responder en gran medida a las necesidades de cada nación, bien sea porque existan políticas públicas o porque existan iniciativas privadas de formación para responder ante el desafío (OEA,2020).

La figura 2, muestra la evolución de los criterios relacionados al rol que ha desempeñado la educación en Colombia frente al reto de la formación en seguridad/ciberseguridad.

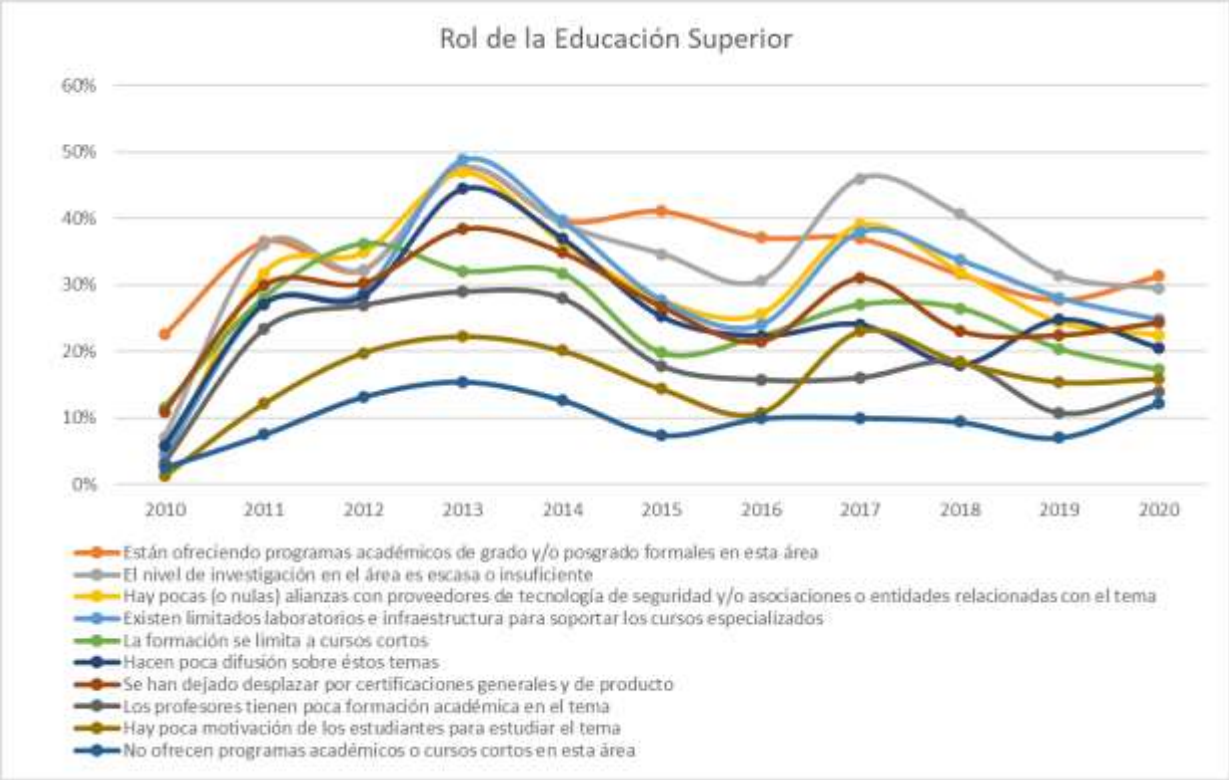

Figura 2. Evolución del Rol de la Educación Superior

Los 10 criterios revisados en el transcurso de los años han mostrado que, los encuestados ratifican que los programas creados en Colombia si son reconocidos (35%) y solo el 10% considera que en el país no se están ofreciendo programas en materia de seguridad/ciberseguridad.

En promedio en los últimos 10 años, se identifica que el nivel de investigación es escaso o insuficiente con un 34%, existen limitadas infraestructuras para desarrollar tanto la investigación como los programas ofrecidos (30%), hay pocas o nulas alianzas entre Gobierno, Empresa y Academia con un 30%, solo el 27% considera que las certificaciones han desplazado a la educación superior y el 25% en promedio observa que no se hace la respectiva difusión al respecto.

En cuanto a la duración de los cursos el 25% considera que son cursos cortos, el 18% considera que los profesores que imparten los cursos necesitan mayor formación académica en estos temas, y solo el 16% en promedio de los participantes considera que hay poca motivación para estudiar estos temas.

Al revisar la variación de dichos criterios en el tiempo, es decir cómo cambian los valores en el tiempo y revisar el promedio acumulado de su variación se encuentran tres tendencias marcadas: lo que definitivamente se considera que no varía o varia poco, lo que varía moderadamente y lo que varía o fluctúa con más frecuencia, la figura 3 detalla estas variaciones.

Figura 3. Variación de los criterios

Basado en los datos disponibles frente a aquello que varía muy poco, los encuestados tienen una fuerte creencia que:

1. Colombia tiene una oferta en programas de seguridad de la información, que también puede ser ratificado por los datos del sistema de información del Ministerio de Educación (SNIES).
2. A pesar de que existen programas de cursos de postgrado que tienen al menos 2 semestres de duración, las personas consideran que la oferta está concentrada en cursos cortos. Esto se puede explicar dado que dentro del periodo de estudio más los datos del SNIES, se observa que solo hasta el año 2017 se crean programas de maestrías de duración de 4 semestres en el país.
3. La creencia que las certificaciones han desplazado a la educación formal está fundamentada en la experiencia y percepción de los profesionales de seguridad/ciberseguridad en el mercado laboral, sin embargo, solo son formas distintas de desarrollar un plan de carrera. Cada persona tiene su espacio y su oportunidad para concretar su vida y desarrollo profesional (Ewert & Kominski, 2014)

Frente a las variaciones moderadas, se puede decir que:

1. Existe poco trabajo por parte de las universidades en la difusión de los programas de ciberseguridad y seguridad de la información. El refuerzo y difusión de los programas de seguridad/ciberseguridad en América Latina, se impulsan a través de las políticas públicas, sin embargo, se requiere que muchos más actores intervengan para que haya mayor difusión (OEA, 2020)
2. Definitivamente el nivel de investigación y la infraestructura ocupan un lugar importante y ambos criterios deben ser materia de evolución en Colombia. Si bien los esfuerzos de las distintas políticas públicas en materia de Ciberseguridad (CONPES, 2011), Seguridad Digital (CONPES, 2016; CONPES, 2020) ofrecen lineamientos que apoyan y fomentan este ítem, no se advierten logros visibles, lo que implica seguir trabajando en estos aspectos y acrecentar las ofertas académicas (OEA, 2020).

Frente a las variaciones más marcadas, se puede decir que:

1. Son indispensables las alianzas y estas pueden y deben ayudar a fortalecer el desarrollo de los conocimientos e investigación en los ecosistemas de los países (OEA, 2020). De igual forma, diseñar programas de ciberseguridad con perspectiva interdisciplinar permite expandir sus interacciones con diferentes sectores y así mejorar la capacidad de los profesionales en su práctica cotidiana (Gupta et all, 2020).
2. Definitivamente la motivación de las personas es uno de los aspectos que más ha variado en el transcurso de los años para incursionar en la carrera de ciberseguridad, si bien es cierto que existe

un déficit de posiciones por llenar el cual ha venido disminuyendo con el pasar de los años (ISC2, 2020), también es notorio que la motivación a través de las generaciones es variada (Raytheon, 2017).

Sectores no todos lo ven de la misma manera

Al revisar todos los datos y analizar como los distintos sectores observan el rol de la educación en Colombia a lo largo de los años, se detalla a continuación la tabla 6, la cual muestra los datos más representativos de los criterios en algunos sectores de la industria (se seleccionan 2 criterios por sector).

Criterios	Gobierno	Educación	Financiero	Consultoría Especializada
Están ofreciendo programas académicos de grado y/o posgrados formales en esta área	18,60%		21,08%	
Existen limitados laboratorios e infraestructura para soportar los cursos especializados	16,53%			
Hay pocas (o nulas) alianzas con proveedores de tecnología de seguridad y/o asociaciones o entidades relacionadas con el tema				15,48%
Los profesores tienen poca formación académica en el tema		15,86%		14,73%
Hay poca motivación de los estudiantes para estudiar el tema		15,01%		
No ofrecen programas académicos o cursos cortos en esta área			21,65%	

Tabla 6. Factores más importantes por sectores

Se observa que el sector Gobierno y el sector Financiero reconocen que existen programas de formación en ciberseguridad y seguridad de la información en el país. De igual forma, el sector Educación y el sector de la consultoría especializada muestran que es necesario fortalecer las capacidades y habilidades de los profesores, para poder impartir más formación con mayor calidad.

Por su parte, el Sector Gobierno hace una clara identificación que la infraestructura es una de las deficiencias que existen en el papel de la Academia para la formación y creación de nuevo talento en seguridad de la información y ciberseguridad. La consultoría especializada hace un llamado de atención al reconocer que hay pocas alianzas y por tanto, esto es un factor que puede desfavorecer al desarrollo de capacidades en materia de ciberseguridad.

Por su parte el sector de la Educación identifica que la motivación de los estudiantes no es clara a la hora de seleccionar los programas de ciberseguridad, en muchos casos porque sus esfuerzos en difusión no son lo suficientes, existen pocos estudios de tendencias laborales en el área, y se ven pocas ferias y congresos donde el sector de la academia lo refleje. Por último, el sector financiero si bien reconoce la oferta, llama la atención en que es necesario trabajar en programas o cursos cortos de formación para los profesionales de seguridad/ciberseguridad.

Conclusiones

La educación en seguridad/ciberseguridad definitivamente es un factor fundamental a la hora de desarrollar capacidades, tanto de las naciones, como de las organizaciones frente a una realidad digital que cada vez más es turbulenta, incierta, novedosa y ambigua. Una fuerza de trabajo educada en ciberseguridad es esencial para construir ambientes confiables en contextos como el digital (Schneider, 2013)

En definitiva los datos muestran que es necesario que se trabaje en fortalecer las alianzas entre todas las partes interesadas, no solo la academia de preocuparse por crear programas de formación, también deben estar conectadas con las necesidades de los gobiernos y las tendencias de las industrias. Por tanto, estas

relaciones deben fortalecerse y así producir resultados transformadores, que permitan afianzar el rol de la universidad en el desarrollo de capacidades de seguridad/ciberseguridad de las naciones, empresas y los profesionales que las ejercen (OEA, 2020; Schneider, 2013).

La contribución que puede hacer la industria al desarrollo y fortalecimiento de los programas de seguridad/ciberseguridad, al apoyar las iniciativas de la universidad, es crear esfuerzos de cooperación que terminen en resultados que beneficien a la sociedad y las partes interesadas (Educause, 2021).

La seguridad/ciberseguridad no debe y no puede ser definida como una sola disciplina, es necesario que las universidades empiecen a comprender y entender la ciberseguridad como una familia de disciplinas, como un ejercicio interdisciplinar, que demanda el desarrollo programas que cada vez están más acordes con los fenómenos disruptivos y cambios que se presentan en un contexto digital más amplio y denso (Parrish et all, 2018).

De igual forma, la ciberseguridad y seguridad de la información deben ser consideradas distinciones relevantes en la educación superior y evitar su tratamiento como una temática aislada o exclusivamente técnica en la oferta académica, que termine impactando la incorporación de nuevos profesionales debidamente preparados y entrenados para enfrentar los desafíos venideros (Parrish et all,2018).

La forma cómo evoluciona y desarrolla el adversario su actuar, muestra una consistente y sólida determinación para investigar y experimentar con el fin de actualizar o renovar sus propios saberes y llevar a cabo sus acciones, teniendo efectos cada vez más significativos e impactantes, en las organizaciones, naciones y sociedades (Educause, 2021). Lo anterior, implica que la formación de los profesionales de seguridad/ciberseguridad debe reconocer estos escenarios, lo que supone mantenerlos fuera de la zona cómoda de los estándares, conectados con el reto de la inevitabilidad de la falla y muy atentos al reconocimiento de sus propios sesgos.

Por tanto, es tiempo que las universidades, basados en los resultados de este estudio, den un salto en el fortalecimiento de sus infraestructuras, laboratorios y plataformas para consolidar los programas de seguridad/ciberseguridad y así entregar profesionales con mayores capacidades y competencias para atender los desafíos de la realidad en materia de ciberseguridad.

La difusión de los programas de ciberseguridad es otro de los factores a trabajar, si bien se confirma que existe una oferta académica importante, la poca difusión de los programas se convierte en un factor clave a la hora de tener acceso a ellos. En este sentido, se hace necesario que las universidades se ocupen en conjunto con la industria y el gobierno para realizar ferias, eventos, concursos, entre otras actividades, en donde se muestren las ofertas disponibles y así puedan incrementar e incentivar de una manera más directa el interés por estudiar este tipo de programas.

Viendo las tendencias internacionales como los esfuerzos realizados por la ACM (Schneider, 2013), para delinear programas universitarios de pregrado en materia de ciberseguridad, evento que en Colombia sucedió hasta el año 2020, se hace imperativo incentivar dichos esfuerzos para que existan más iniciativas de esta naturaleza y, la oferta no solo se concentre en la población de postgrado, donde en la actualidad está focalizada la mayor cantidad de estos programas.

Las certificaciones y la formación no son enemigos, por el contrario son aliados que fomentan el desarrollo y amplían el potencial del profesional de seguridad (ISC)2 (OEA, 2020). Mientras que la formación universitaria desarrolla capacidades para aprender y facilitar el pensamiento crítico alrededor de una temática, las certificaciones desarrollan las habilidades esenciales asociadas con un cuerpo de conocimiento base generados acordes con un momento del tiempo y unas situaciones específicas. Así las cosas, no deben ser vistas como realidades irreconciliables, sino más bien como elementos complementarios en la formación.

Finalmente, es necesario entender que los adversarios digitales, siguen y seguirán desarrollando nuevas formas de materializar sus acciones, para lo cual estarán innovando en la forma de generar retos que afecten a las organizaciones de todos los sectores (Cano & Almanza, 2020). Por tanto, las universidades deben estar mucho más enfocadas en formar y entregar profesionales de ciberseguridad y seguridad de la información que sepan responder, anticipar, adaptar y monitorear las amenazas y riesgos claves de los negocios y las naciones, y así estar mejor preparados frente a la inevitabilidad de la falla.

Referencias

(ISC)2 (2020). Strategies for Building and Growing Strong Cybersecurity Teams. (ISC)2 Cybersecurity Workforce Study. https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

Cabaj, K., Domingos, D., Kotulski, Z. & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs, *Computers & Security*, 75. 24-35, https://doi.org/10.1016/j.cose.2018.01.015.

Cano, J. & Almanza, A. (2020). Estudio de la evolución de la Seguridad de la Información en Colombia: 2000 - 2018. *Revista Iberoamericana de Sistemas y Tecnologías de Información*. E27. Marzo. 470-483

Cano, J. (2021). *Ciberseguridad empresarial. Reflexiones y retos para los ejecutivos del siglo XXI*. Bogotá, Colombia: Lemoine Editores.

Catota, F., Morgan, M. & Sicker, D. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment, *Journal of Cybersecurity*. 5(1). 1-19. https://doi.org/10.1093/cybsec/tyz001

CONPES 3701. (2011). Lineamientos de política para ciberseguridad y ciberdefensa. DNP. https://www2.icfesinteractivo.gov.co/Normograma/docs/pdf/conpes_dnp_3701_2011.pdf

CONPES 3854 (2016). Política nacional de seguridad digital. DNP. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

CONPES 3995 (2020). Política nacional de confianza y seguridad digital. DNP. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf

EDUCAUSE (2021). Educause Horizont Report. Information Security Edition. https://library.educause.edu/-/media/files/library/2021/2/2021_horizon_report_infosec.pdf?la=en&hash=6F5254070245E2F4234C3FDE6AA1AA00ED7960FB

Ewert, S. & Kominisky. R. (2014). Measuring Alternative Educational Credentials: 2012. *Household Economic Studies*. Issued January. https://connectingcredentials.org/wp-content/uploads/2015/02/Measuring-Alternative-Credentials.pdf

Gupta, R., Pal, S. K. & Muttoo, S. K. (2020). Cyber Security Assessment Education for E-Governance Systems. En Daimi K., Francia III G. (eds) *Innovations in Cybersecurity Education*. Springer, Cham. https://doi.org/10.1007/978-3-030-50244-7_10

Ministerio de Educación Nacional - MEN (2019). Niveles de la Educación Superior. https://www.mineducacion.gov.co/portal/Educacion-superior/Sistema-de-Educacion-Superior/231238:Niveles-de-la-Educacion-Superior

OEA (2020). Educación en Ciberseguridad, Planificación del Futuro mediante el desarrollo de la fuerza laboral. https://www.oas.org/es/sms/cicte/docs/20200925-ESP-White-Paper-Educacion-en-Ciberseguridad.pdf

Oxford Martin School (2018). Global Cybersecurity Education – Lessons from the CMM. https://gcscc.ox.ac.uk/global-cybersecurity-education-lessons-cmm

Parrish, A., Impagliazzo, J., Raj, R., Santos, H., Asghar, M., Jøsang, A., Pereira. T. & Stavrou, E. (2019). Global Perspectives on Cybersecurity Education for 2030: A Case for a Meta-discipline. En: *Proceedings companion of the 23rd Annual Conference on Innovation and Technology in Computer Science Education*. 36–54. https://doi.org/10.1145/3293881.3295778

Raytheon (2017). Securing Our Future: Cybersecurity and the Millennial Workforce. https://www.raytheon.com/sites/default/files/2017-12/2017_cyber_report_rev1.pdf

Schneider. F. (2013). Cybersecurity Education in Universities. *IEEE Security & Privacy*. *11*(4), pp. 3-4, July-Aug. doi: 10.1109/MSP.2013.84.

Švábenský, V., Vykopal, J. & Čeleda, P. (2020). What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences. En *The 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20)*, March 11–14. Portland, OR, USA. ACM. New York, NY, USA. 2-8. https://doi.org/10.1145/3328778.3366816