Formación de profesionales

DOI: 10.29236/sistemas.n160a6

Programas posgraduales en seguridad/ciberseguridad. Repensando sus bases y alcance

Resumen

En la actualidad la formación de profesionales en seguridad/ciberseguridad implica reconocer los desafíos de transformación, inestabilidad y de las tensiones que impone una sociedad cada vez más digital y tecnológicamente modificada. En este sentido es necesario revisar los enfoques de formación profesional, con el fin de analizar si los programas educativos ofrecen escenarios posibles de educación, más allá de los tradicionales estándares y buenas prácticas y, en su defecto, proponer alternativas temáticas y pedagógicas viables. En consecuencia, este documento plantea algunas ideas para renovar la formación posgradual en seguridad/ciberseguridad, teniendo en cuenta el enfoque de las asignaturas de sus programas académicos; ofrece cuatro escenarios en los que se pueden situar las ofertas curriculares actuales y futuras, como una forma de motivar reflexiones que saquen de la zona cómoda las propuestas educativas en etapa de diseño o actualización.

Palabras clave

Ciberseguridad, formación, estándares, incertidumbre, educación

Jeimy J. Cano M.

Gabriela María Saucedo Meza.

Introducción

Estudios internacionales recientes revelan una falta de profesionales en seguridad/ciberseguridad requeridos para cubrir la demanda generada por cuenta de una mayor superficie digital que se debe asegurar en los diferentes sectores de la dinámica actual de las naciones (Maurer et al., 2021; Payne et al., 2021). En este momento muchos de ellos tienen la oportunidad para encontrar nuevos horizontes o reinventar sus prácticas actuales con el fin de movilizarse y ubicarse en el sitio que mejor se ajuste a sus expectativas y retos.

De otra parte, los cambios acelerados en las tecnologías de información, las tecnologías emergentes y disruptivas, los nuevos comportamientos de las personas, las exigencias regulatorias, el incremento global de la radicalización política (nueva geopolítica), sumados al interés monetario (grupos organizados, mafia) entre otros aspectos (Briggs et al., 2020), demandan que la incorporación de esta nueva fuerza de trabajo especializada se encuentre a la altura de los desafíos y exigencias del mercado para responder a las organizaciones frente a los riesgos propios de un contexto más digital y tecnológicamente modificado.

Los interesados en acceder a la profesionalización de las áreas del saber mencionadas (seguridad/ciberseguridad) podrán encontrar opciones educativas especializadas, comúnmente a nivel posgradual con asignaturas o temarios que introducen al conocimiento general y detallado, en algunos casos, con base en contenidos y prácticas evaluativas asociadas con estándares y recomendaciones soportadas en hechos conocidos, desde una perspectiva de valoración retrospectiva y, en su mayoría, con un enfoque técnico (Mouheb et al., 2019).

Esta realidad de la formación en seguridad/ciberseguridad interroga a la academia sobre su capacidad para entregar nuevos profesionales en esta área del conocimiento cuya demanda viene en crecimiento hace un par de años, y cuyas respuestas esperadas se deben considerar desde escenarios inciertos y riesgos poco conocidos, pero no por ello inexistentes (Dragoni et al. 2021).

Con el fin de establecer propuestas que contribuyan a las necesidades profesionales requeridas, este artículo indaga en los detalles de la formación de este nuevo perfil profesional, concentrándose más en “cómo deben aprender”, que en “qué deben aprender”, enfatizando en “el qué y cómo deben pensar”, que en “qué y cómo deben responder”. Adicionalmente, busca profundizar en una propuesta sobre el desarrollo de capacidades necesarias para enfrentar las realidades inciertas, inestables e incrementalmente complejas en las que se verán expuestos, sin perjuicio de

los fundamentos o bases naturales propias de la disciplina de la seguridad de la información.

Así las cosas, se exploran algunas de las características más recurrentes de los programas educativos activos enfocados a las áreas del saber mencionadas, considerando aquellos que incorporan un currículo mediante el cual los estudiantes están en la capacidad de dar respuestas en un marco de trabajo conocido y validado en aspectos como valoración de riesgos cotidianos y estrategias alineadas con los estándares y prácticas internacionales (McDuffie & Piotrowski, 2014). Si bien los egresados de estos programas concluyen su formación con un conjunto de respuestas esperadas que los conecten con lo que demandan algunas empresas, tendrán retos importantes cuando la realidad los exponga a escenarios no convencionales.

Como aporte, se elaboran algunas propuestas de formación basadas en tres conceptos básicos de la seguridad/ciberseguridad: la inevitabilidad de la falla, la vulnerabilidad inherente y la incertidumbre. Además, la necesidad de integrar dichos conceptos con un pensamiento sistémico, de tal forma que el estudiante pueda ir desarrollando su capacidad para reconocer los sesgos permanentes a los que está expuesto en su ejercicio profesional, teniendo en cuenta que, dados los riesgos latentes y emergentes, los planes de seguridad y control podrían no ejecutarse de acuerdo como está previsto. Esta contribución incluye una formación que ofrece una ventana de aprendizaje permanente orientada a ver puntos ciegos en los modelos de seguridad y control vigentes en las organizaciones; busca habilitar a un profesional formado en estos fundamentos para mantenerse en movimiento, a pesar de los desafíos que le impongan los eventos adversos.

En resumen, este texto propone una reflexión crítica y práctica sobre la formación de los profesionales de seguridad/ciberseguridad, como una apuesta para el futuro inmediato y un insumo para aquellos que quieran diseñar programas de formación en esta área que respondan a los interrogantes conocidos y emergentes de la dinámica nacional e internacional, en vista de que las tecnologías disruptivas se han vuelto de lectura cotidiana, y la convergencia tecnológica en el normal de las estrategias de negocios y desarrollos sociales y humanos.

Formación posgradual en seguridad/ciberseguridad. Perspectiva actual

Cuando se revisa un conjunto base de los programas nacionales e internacionales de formación posgradual en seguridad/ciberseguridad, se identifica un ciclo básico de asignaturas en que se le da forma a la práctica y al pensamiento de los futuros profesionales de esta área.

Entre las materias que se desarrollan están: (Hajny et al., 2021)

- Fundamentos de seguridad/ciberseguridad (*como nivelación de saberes previos*)
- Estándares y buenas prácticas de seguridad/ciberseguridad
- Seguridad en redes
- Criptografía
- Gestión de riesgos cibernéticos/seguridad

En cada una de estas asignaturas se parte de un fundamento conceptual de saberes que definen la práctica general en la disciplina de la seguridad. Una práctica que contiene listados de acciones concretas, probadas y muchas de ellas validadas formalmente en un marco de acción confiable que se puede usar y recomendar frente a situaciones conocidas que las organizaciones y las personas enfrentan en la actualidad y posiblemente en el futuro.

El *reto de estas asignaturas* es orientar acerca de cómo gestionar el riesgo digital de las personas y organizaciones. En este ejercicio, cada una de las acciones detalladas en los contenidos programáticos le ofrecen al estudiante múltiples escenarios de certezas y recetas de acción que tendrán los efectos deseados y, por tanto, posibles respuestas a las inquietudes de sus futuros empleadores que demandan una disminución sustancial de escenarios inciertos en lo que a la seguridad de la información se refiere (Payne et al., 2021). En otras palabras, al contar con un personal especializado, un ejecutivo puede estar tranquilo porque hay alguien que le ayudará a entender mejor la posible brecha de seguridad que puede existir en una situación particular.

Por lo general, la *enseñanza de estos cursos* está asistida en el uso de casos aplicados a empresas, en los que los diferentes participantes reconocen una situación específica de algo que ocurre en la dinámica de su organización. La finalidad es que el estudiante pueda identificar dentro de la "caja de herramientas" que se facilita para cada caso, alguna(s) estrategia(s) relevante(s) ya sea para cerrar la brecha identificada en su organización o para mejorar el desempeño actual de los controles implementados. En relación con la evaluación contempla alternativas y opciones que posiblemente han tomado en situaciones similares en su práctica profesional (Dark & Mirkovic, 2015).

Las *reflexiones que se plantean* en el desarrollo de estas asignaturas generalmente se realizan desde un ejercicio de causa y efecto. Esto es, se identifican las posibles situaciones de riesgos conocidos, se analizan las medidas actualmente instaladas y en operación, para luego emitir la recomendación para evitar que el efecto no deseado se materialice (Cano, 2015). Como resultado de esta reflexión se suele presentar como fuente de error a las

personas, quienes con frecuencia ejecutan las acciones de control y, en consecuencia, se motiva la implementación de contramedidas que tiendan a ser automáticas y con reportes en línea de las acciones que deben tomar.

Revisado lo anterior, y teniendo en cuenta que estas asignaturas (y otras más que no se han mencionado) son necesarias y claves en las actuales ofertas curriculares, conviene que sus contenidos sean revisados, pues sus fundamentos posiblemente fueron concebidos en momentos y tiempos diferentes a los actuales, y por lo tanto, resulta necesario interrogarlos y buscar puntos ciegos de las prácticas que definen, no sólo como un ejercicio de crítica constructiva, sino como una oportunidad para enriquecer y abrir nuevas perspectivas de actualización en las que se considere que las organizaciones se encuentran bajo situaciones de inestabilidad e incierto (Colom, 2002).

Así mismo es pertinente que los criterios y métricas de evaluación, así como el énfasis de las reflexiones puedan ser revisadas dado que, si bien dotan al futuro profesional de capacidades necesarias para dar respuestas frente a la materialización de escenarios previstos, deben también prepararse para aquellos no concebidos o frente a una cultura de seguridad corporativa no implementada en una organización (Kam & Katerattanakul, 2014).

Formación retadora en seguridad/ciberseguridad. Una nueva perspectiva.

Cambiar la perspectiva de la formación de los profesionales en esta área implica, en primer lugar, reconocer los logros y éxitos del modelo tradicional en la generación de la mano de obra disponible a la fecha y, en segundo lugar, identificar perspectivas distintas encaminadas a abrir espacios de construcción de saberes y ventanas de aprendizajes y desaprendizajes que habiliten la transición de un estudiante contenedor de conocimiento, a uno habilitador de capacidades personales y organizacionales (Medina, 2010). En complemento de lo anterior, es recomendable que los responsables del diseño de ofertas académicas tengan presente los cambios, desafíos y escenarios presentados previamente, en especial aquellos derivados de un mundo cada vez más digital y tecnológicamente modificado.

Para dar respuesta a los escenarios emergentes en torno a la seguridad/ciberseguridad, se propone un nuevo conjunto de asignaturas retadoras, que deberían incorporar temáticas relacionadas con:

- Gestión de riesgos latentes y emergentes en seguridad/ciberseguridad
- Deconstrucción de la seguridad/ciberseguridad
- Desinstalando los estándares y buenas prácticas de seguridad/ciberseguridad (Saydjari, 2018)

- Inseguridad en la cuarta revolución industrial (Nube, internet de las cosas, realidad aumentada, inteligencia artificial, cadena de bloques)
- Criptovirología (Young & Yung, 2004)

En cada una de estas posibles nuevas asignaturas resulta oportuno partir del saber previo del estudiante para plantear aquellas preguntas que aún no tienen respuesta en su práctica cotidiana, con el fin de darle sentido práctico y conceptual al reto de la protección de la información ajustado con la realidad (Daimi & Francia III, 2020). En este contexto, las preguntas le dan forma al conjunto de casos pertinentes que tanto las personas como las empresas tienen, para desde allí, observar las buenas prácticas y estándares disponibles. Adicionalmente se proponen tres recomendaciones para esta nueva perspectiva curricular:

- Que la búsqueda de respuestas y reflexiones se realice en doble vía: considerando, tanto la perspectiva de un analista tradicional, como la visión de un atacante, para que sea posible desarrollar las estrategias que mejor se ajusten al reto por resolver.
- Que se enseñe a reconocer la inevitabilidad de la falla como fundamento de las acciones en seguridad, para hacer más resistentes los modelos de protección y control.
- Que se reconozca el "error" como una oportunidad natural de aprendizaje, con el fin aprender más rápido del entorno y del adversario.

El *reto de estas asignaturas* no es solamente orientar en cómo gestionar el riesgo digital de las personas y organizaciones, sino comprender la dinámica misma de las relaciones entre estas, que configuran la situación adversa. En este ejercicio, se modela el contexto de la situación y cómo desde diferentes ángulos es posible encontrar acciones contrarias que le permitan al estudiante contemplar múltiples escenarios de inciertos e inestabilidades para los cuales deberá prepararse y, en consecuencia, reconocer las capacidades que se deben desplegar para que las empresas sean más resistentes ante los efectos ocasionados por la materialización de los escenarios comentados (Cano, 2015). Dicho de otra forma, la formación de este nuevo profesional especializado lo habilita tanto para la generación de simulaciones y escenarios inesperados, incorporando de manera sistémica, a los ejecutivos en una práctica de seguridad distinta, como para la creación de estrategias encaminadas al desarrollo de una mejor consciencia situacional que defina los umbrales de operación cuando las cosas no salen como estaban previstas (Angafor et al., 2020).

La *enseñanza de estos cursos* se propone que esté asistida por el desarrollo de escenarios prospectivos

y simulaciones que respondan a riesgos latentes y emergentes, con el fin de identificar, actualizar y reinventar la "caja de herramientas disponible", no para cerrar la brecha conocida, sino para defender y anticipar las acciones de los adversarios que usualmente están fuera de los radares de los estándares y generan inquietudes en los saberes previos de los profesionales; una práctica que motiva la búsqueda de respuestas distintas en lugar de repetir aquellas conocidas (Angafor et al., 2020). En relación con la valoración de conocimientos se plantea que los trabajos se evalúen frente a propuestas no convencionales para situaciones no conocidas, con propuestas de "libros jugadas"[1] alternativos, acciones y tecnologías que traten de sorprender al atacante en su propio terreno.

Las *reflexiones que se plantean* en el desarrollo de estas asignaturas se propone que estén basadas en una perspectiva sistémica, es decir en relaciones y reconocimiento del contexto. En este ejercicio se identifican las posibles situaciones de riesgos latentes y emergentes tanto desde la perspectiva del profesional de seguridad o analista, como desde la del adversario, para reconocer las diferentes formas en las que pueden fallar los controles y crear las zonas de operación confiables, que definan los umbrales de operación permitidos y los límites de sus actuaciones (Cano, 2015). Esto es, el estudiante debe reconocer que las personas que aplican y ejecutan los controles son parte natural del proceso y, por lo tanto, las propuestas que realice deberán incluir sus perspectivas y visiones, como parte fundamental de la capacidad de resistencia del sistema que se quiere asegurar y mantener.

Si bien estas asignaturas pueden ser disonantes frente al conjunto tradicional disponible y conocido, deben ser ocasión para cambiar el discurso y la manera como se construye el nuevo saber en seguridad/ciberseguridad. La propuesta es una estructura conceptual que interroga todo el tiempo el saber previo del participante e incorpora el concepto de incertidumbre como elemento fundamental de su formación y, por lo tanto, motiva la creación de una zona psicológicamente segura (Edmondson, 2018) en la que profesor y estudiante construyen y actualizan las fuentes de un conocimiento parcial a realidades situadas y de interés de cada individuo, que reconoce la inestabilidad de las respuestas y soluciones alcanzadas en cada momento del curso.

Escenarios de formación en seguridad/ciberseguridad

Con el contraste de estas dos perspectivas de la formación posgra-

1 Un "libro de jugadas" o playbook es una respuesta ordenada y coordinada a escenarios latentes y conocidos que busca contestar al menos a cinco interrogantes: a) ¿Qué estamos tratando de proteger?, b) ¿Cuáles son las amenazas claves?, c) ¿Cómo las detectamos?, d) ¿Cómo respondemos? y e) ¿cómo nos organizamos? (Basado en: Bollinger, J., Enright, B. & Valites, M. (2015). Crafting the InfoSec Playbook. Sebastopol, CA. USA: O'Reilly)

dual (una reactiva y otra proactiva) en seguridad/ciberseguridad se procede a esbozar cuatro escenarios de formación para los profesionales de esta área del conocimiento, reconociendo los retos que plantean las tendencias emergentes e inestabilidades globales de mediano y largo plazo. Para ello, se consideran dos ejes de acción: *el pensamiento* (adversario vs analista) y *la seguridad/ciberseguridad* (estándares vs capacidades).

El primer escenario (cuadrante I) para analizar nace de la dinámica actual de los programas basados en los *estándares* y mantener la perspectiva del *analista*. La formación de los profesionales en este cuadrante mantiene el *statu quo* de los programas actuales, continuando con la perspectiva de los docentes experimentados que sitúan a sus estudiantes en contextos semejantes a los que ellos han vivido para darle forma a las respuestas esperadas desde la práctica de los estándares (Ackoff & Greenberg). El reto y la perspectiva que se fortalece en los egresados es la mitigación del riesgo, la inevitabilidad de la falla es un enemigo oculto y el adversario es fuente natural de incertidumbre.

El segundo escenario (cuadrante II) surge de la dinámica actual de los programas basados en los *estándares* y el deseo de incorporar la perspectiva de *adversario*. La formación de los profesionales en este cuadrante demanda el reto de desaprender, esto es, dejarse interrogar en sus saberes previos y reconocer la inestabilidad de todo lo que han aprendido (Medina, 2010).

Lo anterior implica, reconocer sus propios sesgos y lanzarse a retar los saberes estabilizados y probados de los estándares y buenas

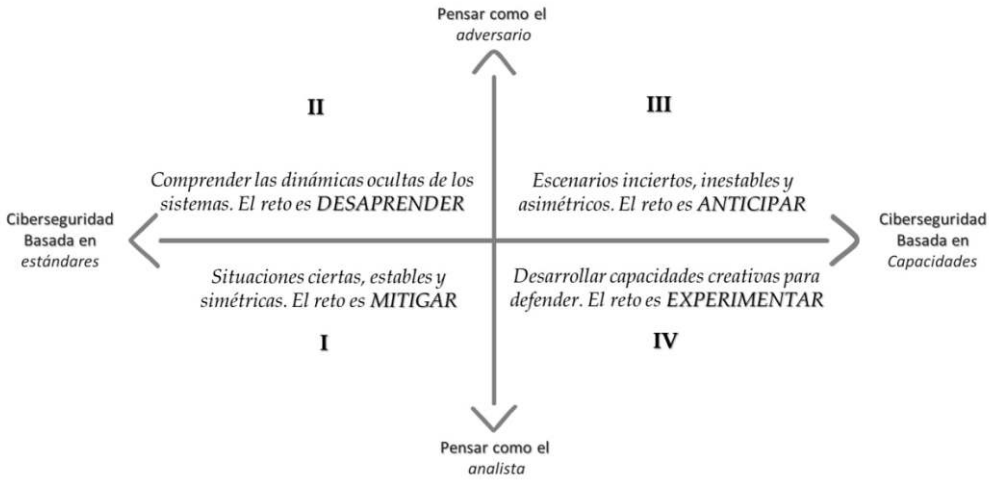

Figura 1. Escenarios de formación en seguridad/ciberseguridad (Elaboración propia)

prácticas. La invitación de los profesores es a superar los propios sesgos y las respuestas estandarizadas para actualizar las prácticas vigentes. La fuerza de los programas estará en habilitar una lectura más sistémica de la realidad para comprender la dinámica oculta de su contexto.

El tercer escenario (cuadrante III) surge de la incorporación de programas basados en *capacidades* y el deseo de fusionar la perspectiva de *adversario*. Las iniciativas académicas que se organicen en este cuadrante tienen como fundamento la pedagogía del error (De la Torre, 2004) y la incertidumbre. Los estudiantes estarán expuestos a situaciones inciertas de forma permanente, para lo cual las simulaciones y los escenarios serán la fuente natural de conocimientos y retos para continuar con una espiral de aprendizaje/desaprendizaje ascendente que lleve a cada uno de los participantes a sentirse cómodo con los inciertos, lo que le dará mayores capacidades (patrones de aprendizaje) para desarrollar propuestas que sorprendan al adversario en su propio terreno (anticipar), esto es, aumentar la incertidumbre en su modelo de riesgos. Los profesores en este escenario sugieren alternativas y opciones adicionales que retan los saberes adquiridos, y no respuestas, y así mismo, mantienen un marco de actuación ético y transparente necesario para delinear las acciones de sus estudiantes.

El cuarto escenario (cuadrante IV) surge de la incorporación de programas basados en *capacidades* y mantener la perspectiva del *analista*. En este cuadrante las iniciativas académicas buscan promover la creatividad utilizando la información y datos disponibles con el fin de experimentar e identificar patrones de comportamiento que lleven a los estudiantes a desarrollar habilidades analíticas, que cambien la forma del tratamiento de los riesgos identificados hasta el momento. Lo anterior implica crear zonas de aprendizaje permanente en las que estudiantes y profesores se dejen sorprender por las relaciones posibles que surjan y desde allí, crear conexiones inexistentes que preparen a las empresas para responder, casi en tiempo real, sobre situaciones inéditas que sólo se pueden ver en el tratamiento de los datos de formas distintas (Calvo, 2017). El profesor acompaña el ejercicio y sugiere alternativas para sacar de la zona cómoda al estudiante para luego lograr experimentos más novedosos y desafiantes.

Estos cuatro escenarios de formación dan cuenta de las posibles estrategias y casos evolutivos que pueden tener los programas de formación en seguridad/ciberseguridad. Cada institución de educación podrá revisar donde se ubican sus programas actuales para establecer su referente de formación base y desde allí plantear alternativas que le den mayor profundidad

o énfasis según su interés, bien en las capacidades o en el pensamiento del adversario. Los escenarios no buscan dar respuesta a las necesidades de formación de mediano y largo plazo en seguridad/ciberseguridad, sino plantear alternativas a la dinámica actual de estos programas como una invitación a superar la inercia de lo tradicional en la oferta e impulsar transformaciones en sus currículos.

Reflexiones finales

Formar a los nuevos profesionales de seguridad/ciberseguridad para afrontar los retos más allá de los linderos de la próxima década debe generar espacios de reflexión y desafío en la comunidad académica, los proveedores, los profesionales en ejercicio y los gobiernos, con el fin de responder a la sociedad con la mano de obra y el personal idóneo que dé cuenta con la reinvención permanente de la inevitabilidad de la falla y las enseñanzas inéditas de la inseguridad de la información. Recurrir al viejo paradigma de los saberes estandarizados y los problemas resueltos es limitar la capacidad de los analistas que se requieren para un entorno cada vez más volátil, incierto, complejo y ambiguo (Ackoff & Greenberg, 2008).

La formación en seguridad/ciberseguridad debe responder a un paradigma de la armonía de los contrarios; es decir, una vista sistémica y circular de la seguridad e inseguridad que de forma natural establezca espacios de ruptura para lo conocido, sugiera entornos psicológicamente seguros para aprender y reconozca los sesgos personales. Esto es, un lugar común en el que puedan convivir y nutrirse mutuamente las respuestas de los estándares básicos para los entornos ciertos y el desarrollo de capacidades nuevas (patrones de aprendizajes emergentes) que interroguen los logros previos y afinen cada vez más la sensibilidad frente a las inestabilidades del entorno (Cano, 2015).

De esta forma, no sólo se estarán capitalizando la fuerza y las bondades de las buenas prácticas, sino abriendo oportunidades para repensar, renovar o desinstalar cada una de ellas, con el fin de desconectarlas de las situaciones previas donde fueron creadas, enriquecerlas con las novedades y dinámicas del entorno, con una vista interdisciplinar para conectarlas e introducir nuevas distinciones que cambien la forma como se venía entendiendo la práctica misma de aseguramiento (Payne et al., 2021b). Lo anterior no significa desconocer el pasado del estándar o modelo revisado, sino entenderlo y ajustarlo a los retos actuales, donde se prueban, validan o actualizan sus propios supuestos.

Los cuatro escenarios propuestos para los programas de formación en seguridad/ciberseguridad establecen cuatro momentos y dinámicas para las iniciativas académicas

actuales y futuras. Es una forma de modelar la incertidumbre generadas por las exigencias de los cambios y dinámicas actuales con el fin de proponer un abanico de alternativas (muchas de ellas hoy sin escenario natural alguno) para darle sentido y orientación sobre "cómo deben aprender" y "qué y cómo deben pensar" los profesionales de seguridad/ciberseguridad. La intencionalidad de este ejercicio es invitar a los responsables del diseño de programas a reflexionar sobre los nuevos alcances de estos profesionales que exige una capacidad de pensamiento autónomo y respuesta ante escenarios inciertos (Dark, 2014).

El futuro no es un lugar cierto ni cómodo, por lo tanto, los profesionales de seguridad/ciberseguridad deberán estar preparados para actualizar sus mapas de navegación sobre un territorio en el que cualquier cosa puede pasar. Para ello, la academia debe superar sus propias maneras para formar profesionales, no sólo por el bien de la sociedad que demandará mayor capacidad de sus egresados, sino como una forma de reinventarse más allá de los modelos pedagógicos, los currículos, las didácticas y las estrategias de evaluación que responden a una educación escolarizada, y darle paso al "peregrinaje del educando" donde éste crea relaciones posibles, formula relaciones probables, diseña propuestas realizables y encuentra nuevos desafíos alcanzables (Calvo, 2017).

Agradecimientos

Los autores extienden un especial agradecimiento al ingeniero Fernando Nikitin, *Principal Oversight, Audit and Compliance* en la Oficina del Auditor Ejecutivo del Banco Interamericano de Desarrollo, con sede en Washington, D.C., USA por los valiosos comentarios y aportes que permitieron afinar y detallar las reflexiones de este artículo.

Referencias

Ackoff, R. & Greenberg, D. (2008). *Turning learning right side up*. New Jersey, USA: Wharton School Publishing.

Angafor, G., Yevseyeva, I. & He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. *Security and Privacy*. 3:e126. 1-19. https://doi.org/10.1002/spy2.126

Bollinger, J., Enright, B. & Valites, M. (2015). *Crafting the InfoSec Playbook*. Sebastopol, CA. USA: O'Reilly

Briggs, B., Buchholz, S. & Sharma, S. K. (2020). Macro technology forces. A second look at the pillars of the past, current, and future innovation. *Deloitte Insights*. https://www2.deloitte.com/us/en/insights/focus/tech-trends/2020/macro-technology-trends.html

Calvo, C. (2017). *ingenuos, ignorantes, inocentes. De la educación informal a la escuela autoorganizada*. La Serena, Chile: Editorial Universidad de la Serena.

Cano, J. (2015). La educación en seguridad de la información. Reflexiones pedagógicas desde el pensamiento de sistemas. *3er Simposio Internacional en "Temas y problemas de Investigación en Educación: Complejidad y Escenarios para la Paz"*. https://www.researchgate.net/publication/310844543_La_educacion_en_seguridad_de_la_informacion_Reflexion_pedagogicas_desde_el_pensamiento_de_sistemas

Colom, A. (2002). *La (de)construcción del conocimiento pedagógico. Nuevas perspectivas en teoría de la educación*. Barcelona, España: Paidos.

Daimi, K. & Francia III, G. (eds) (2020). *Innovations in Cybersecurity Education*. Switzerland: Springer Nature.

Dark, M. & Mirkovic, J. (2015). Evaluation Theory and Practice Applied to Cybersecurity Education. *IEEE Security and Privacy*. 75-80. Doi: 10.1109/MSP.2015.27

Dark, M. (2014). Advancing Cybersecurity Education. *IEEE Security and Privacy*. 79-83. Doi: 10.1109/MSP.2014.108

De la Torre, S. (2004). *Aprender de los errores. El tratamiento didáctico de los errores como estrategia de innovación*. Buenos Aires, Argentina: Editorial Magisterio del Río de la Plata.

Dragoni, N., Lafuente, A., Massacci, F. & Schlichtkrull, A. (2021). Are We Preparing Students to Build Security In? A Survey of European Cybersecurity in Higher Education Programs. *IEEE Security & Privacy*. 81-88. Doi: 0.1109/MSEC.2020.3037446

Edmondson, A. (2018). *The fearles organization. Creating psychological safety in the workplace for learning, innovation, and growth*. Hoboken, New Jersey. USA: John Wiley & Sons.

Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L. & De Nicola, R. (2021). Framework, Tools and Good Practices for Cybersecurity Curricula. *IEEE Access*. 9. 94723-94747. doi: 10.1109/ACCESS.2021.3093952

Kam, H. J., & Katerattanakul, P. (2014). Diversifying cybersecurity education: A non-technical approach to technical studies. *2014 IEEE Frontiers in Education Conference (FIE) Proceedings*. doi:10.1109/fie.2014.7044197.

Maurer, C., Sumner, M., Mazzola, D., Pearlson, K. & Jacks, T. (2021). The Cybersecurity Skills Survey: Response to the 2020 SIM IT Trends Study. En *Proceedings of the 2021 on Computers and People Research Conference (SIGMIS-CPR'21)*. Association for Computing Machinery, New York, NY, USA, 35–37. DOI: https://doi.org/10.1145/3458026.3462153

McDuffie, E. L. & Piotrowski, V. P. (2014). The Future of Cybersecurity Education. *IEEE Computer*. 47(8). 67–69. Doi: 10.1109/MC.2014.224

Medina, J. (2010). El desaprendizaje: Aproximación conceptual y notas para un método reflexivo de generación de saberes profesionales. En Armengol, C. & Gairín, J. (2010) *Estrategias de formación para el cambio organizacional*. Madrid, España: Wolters Kluwer.

Mouheb, D., Abbas S. & Merabti M. (2019). Cybersecurity Curriculum Design: A Survey. En Pan Z., Cheok A., Müller W., Zhang M., El Rhalibi A. & Kifayat K. (eds) (2019) *Transactions on Edutainment XV*. Lecture Notes in Computer Science. 11345. 93-107. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-59351-6_9

Payne, B., He, W., Wang, C., Wittkower, D. E. & Wu, H. (2021). Cybersecurity, Technology, and Society: Developing an Interdisciplinary, Open, General Education Cybersecurity Course" *Journal of Information Systems Education*. 32(2). 134-149. https://aisel.aisnet.org/jise/vol32/iss2/6

Payne, B., Mayes, L., Paredes, T., Smith, E., Wu, H. & Xin, C. (2021b). Applying High Impact Practices in an Interdisciplinary Cybersecurity Program. *Journal of Cybersecurity Education, Research and Practice*, 2020(2). https://digitalcommons.kennesaw.edu/jcerp/vol2020/iss2/4

Saydjari, O. (2018). *Engineering Trustworthy Systems: Get Cybersecurity Design Right the First Time*. New York, USA: McGraw Hill.

Young, A. & Yung, M. (2004). *Malicious Cryptography: Exposing Cryptovirology*. Indianapolis, IN. USA: John Wiley & Son.

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Business Administration por Newport University, CA. USA. y Ph.D en Educación por la Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*

***Gabriela María Saucedo Meza, Ph.D, MDOH**. Licenciado en Sistemas Computaciones y Maestría en Desarrollo Organizacional y Humano por la Universidad del Valle de Atemajac, México. Doctora en Educación por la Universidad Santo Tomás, Colombia. Certificada en Consultoría General por el Consejo Nacional de Normalización y Certificación de Competencia Laboral (CONOCER), México. Cuenta con más de 28 años de experiencia en gestión educativa, docencia e investigación en seguridad de la información, auditoría de TI, liderazgo educativo, cambio y cultura organizacional. Actualmente es miembro del Grupo de Investigación en Organizaciones, Gestión Educativa y del Conocimiento (OGEC) de la Universidad Santo Tomás en Colombia.*