Superación profesional en ciberseguridad, análisis y experiencias en la Universidad de las Ciencias Informáticas

Henry Raúl González Brito
Universidad de las Ciencias Informáticas
henryraul@uci.cu

Raydel Montesino Perurena
Universidad de las Ciencias Informáticas
raydelmp@uci.cu

María Teresa Pérez Pino
Universidad de las Ciencias Informáticas
mariatpp@uci.cu

Resumen- **En el artículo se realiza un estudio sobre la importancia de la superación profesional en ciberseguridad para mantener niveles adecuados de protección. Se fundamenta la superación profesional como un proceso educativo continuo para graduados universitarios, la cual debe ir evolucionando a la par de las amenazas emergentes y el avance de las TIC. Se observa que la superación es dinámica, adaptándose a nuevas tecnologías y desafíos y se proponen cinco períodos para el estudio de la evolución de la superación profesional en ciberseguridad. Se analiza los marcos de referencia principales como CSEC2017, NICE y CyBOK, esenciales para programas académicos de ciberseguridad. Se abordan resultados alcanzados por la Universidad de las Ciencias Informáticas en la superación profesional continua en ciberseguridad, enfocándose en la actualización constante de sus programas de pregrado y posgrado alineadas con las tendencias internacionales.**

***Index Terms*- jornadas, ciberseguridad, superación profesional, posgrado**

Tipo de contribución: *Formación e innovación educativa*

I. Introducción

El desarrollo de la universidad cubana contemporánea, se sustenta, entre otros aspectos, en el uso pertinente y novedoso de las Tecnologías de la Información y la Comunicación (TIC), en correspondencia con el perfeccionamiento de los procesos de la Educación Superior y la informatización de la sociedad cubana [1].

Desafortunadamente, el uso de las TIC también ha significado el incrementado de los incidentes de ciberseguridad nivel mundial, caracterizándose este hecho por el surgimiento constante de nuevas amenazas en el ciberespacio y ataques dirigido tanto a organizaciones como a los usuarios [2], [3], [4] Por ello, actualmente, la ciberseguridad constituye un desafío creciente para las Instituciones de Educación Superior (IES) [5], [6], [7]

En los últimos años, el número de ciberataques en el sector educativo aumentó casi cinco veces [8]. En julio del 2021, la empresa Check Point registró como promedio 1739 ataques semanales dirigidos a institución educativa, lo que representa un aumento del 29% en comparación con el primer semestre de dicho año [9]. Puede afirmarse, por tanto, que las IES se enfrentan actualmente al reto de garantizar el acceso compartido a la información y los servicios telemáticos y al mismo tiempo evitar las amenazas que puedan poner en riesgo sus activos de información [10], [11], [12].

En la bibliografía consultada hay consenso sobre el importante papel que desempeña el factor humano para garantizar la seguridad de la transformación digital en las organizaciones. Por ello, la superación profesional constituye la piedra angular para alcanzar niveles de ciberseguridad razonables en las IES [13], [14], [15], [16].

En el artículo abordamos la importancia que reviste las TIC para las IES y el importante papel que juega el factor humano en contrarrestar las amenazas de ciberseguridad que la afecta. El resto de las secciones se organizan como sigue: en la Sección II se desarrolla el concepto de superación profesional. La Sección III aborda la evolución de la superación profesional en la ciberseguridad, donde se proponen cinco etapas de estudio en función de los cambios cualitativos inferidos a partir de la bibliografía consultada. Posteriormente en la sección IV se analizan los principales marcos de referencia para la superación profesional en ciberseguridad. En la sección V se analizar los resultados y experiencias alcanzados en la superación profesional en ciberseguridad en la Universidad de las Ciencias Informáticas (UCI) y se concluye con la sección VI, donde se plasman las conclusiones y trabajos futuros.

II. Superación Profesional

En un mundo caracterizado por la constante evolución de la ciencia y la tecnología, la superación profesional representa un pilar esencial para garantizar el desarrollo científico y tecnológico en correspondencia con las demandas del desarrollo sostenible local, territorial y del país [17], [18].

En Cuba, la superación se concibe en el Decreto-Ley 350/2017 como una forma de capacitación que constituye la base principal por donde transitan *los graduados universitarios, en dependencia de las necesidades de capacitación, de acuerdo con los cargos que desempeñan o para los que se estén preparando* [19].

Autores como [20] conciben la superación profesional como *un conjunto de procesos de enseñanza-aprendizaje que posibilitan a los graduados universitarios la adquisición y perfeccionamiento continuo de los conocimientos y habilidades*. Esto es refrendado por [21] cuando plantea que l*a finalidad de la superación profesional es el desarrollo del sujeto para su mejoramiento profesional y humano y sus objetivos se orientan a ampliar, perfeccionar, actualizar, complementar conocimientos, habilidades y capacidades, consolidar valores, promover el desarrollo y modos de*

actuación profesional.

En el marco jurídico cubano, la superación profesional está asociada a la educación de posgrado. Esto puede constatarse en el Decreto Ley No. 350 del 2017 cuando se enuncia la superación profesional como *aquella que aborda resultados de investigación relevantes o aspectos trascendentes de actualización* que pueden ser *impartidos como actividades de posgrado*. En varios acápites también se hace referencia explícita como *superación profesional de posgrado* [19].

III. Evolución de la Superación Profesional en la Ciberseguridad

La superación profesional en ciberseguridad fue evolucionando a la par de las transformaciones que iba sufriendo este campo, definido por la evolución tecnológica y el impacto creciente en los procesos económicos, productivos y sociales. Tomando como punto de partida la bibliografía consultada, se proponen los siguientes periodos de estudio:

A. Período de 1960-1980

Este periodo se caracteriza por el surgimiento de las bases conceptuales de la seguridad informática [22]. Según [23], [24], [25] puede afirmarse que un evento significativo en este proceso fue la realización de la Spring Joint Computer Conference en el año 1967 donde se hicieron demostraciones de vulnerabilidades en computadoras de tiempo compartido y tuvieron lugar varios debates respecto a la seguridad alrededor de las tecnologías computacionales y su impacto en la seguridad nacional [26], lo que provocó el surgimiento de investigaciones lideradas por el sector de la defensa de EE.UU, culminando en una serie de reportes publicados en los años de 1970 que establecieron conceptos y fundamentos teóricos que son utilizados en la actualidad [27], [28].

En este periodo, aunque se reconoce el papel de las personas para prevenir los incidentes de seguridad, el enfoque principal de los controles seguridad son de tipo físico y tecnológico y las preocupaciones principales estaban en la forma de limitar las filtraciones por emanaciones electromagnéticas, escuchas por líneas de transmisión o el control de acceso a los datos [27], [29].

No se reportan programas de estudio por lo que puede inferirse que la capacitación se realizaba en función de utilizar los medios de cómputo y de manera empírica desde el puesto de trabajo.

B. Período de 1980-1990

Este periodo se caracteriza por el crecimiento y proliferación de tecnologías computacionales en organizaciones de todo tipo y existe una mayor concientización sobre los peligros que extraña la materialización de diversas amenazas de ciberseguridad en un entorno altamente automatizado y de complejidad creciente [30], [31].

Cobran auge las publicaciones electrónicas especializadas como Phrack, a través de las cuales se comparten conocimientos sobre seguridad informática, exploits, técnicas de hacking y otros temas relacionados. A diferencia del periodo anterior, ahora la información detallada sobre vulnerabilidades técnicas y sus formas de explotación son de conocimiento público y se utilizan particularmente por jóvenes para irrumpir en redes corporativas y educativas [32], cuestión que inicia el debate sobre el uso seguro y ético de las Tecnologías de la Información y la Comunicación (TIC) [31], [33].

Se pone de manifiesto, por tanto, la necesidad de capacitar a los usuarios en el uso seguro de las TIC [34], [35] y varios autores plantean la pertinencia de incluir en los currículo universitario temáticas relacionados con la seguridad de la información debido a la importancia que esta tendrá para los futuros graduados en su desempeño laboral [36], [37], [38] [39].

El incidente de ciberseguridad provocado por el malware Morris en 1988 puso de manifiesto las debilidades técnicas de la incipiente Internet, dando lugar al surgimiento de una mayor concienciación y enfoque de la comunidad de las TIC, en los problemas relacionados con la seguridad informática [40]. En 1989 se crea el Consorcio internacional de Certificación de Seguridad de Sistemas de Información o $(ISC)^2$ con un cuerpo de conocimiento común para validar las competencias de los profesionales de seguridad informática [41].

C. Período de 1990-2000

En el año 1994 surge el Estándar de Formación para Profesiones de Seguridad de Sistemas de Información (NSTISSI No. 4011), dirigido a la capacitación de profesionales en las disciplinas de seguridad de telecomunicaciones y sistemas de información automatizados (AIS), abarcando temas como amenazas, vulnerabilidades, características de la información crítica, confidencialidad, integridad, disponibilidad, transmisión, almacenamiento y procesamiento de información [42].

En este periodo se reportan los primeros programas de maestría en seguridad de los sistemas de información [43], [44], pero es necesario señalar que todavía no existe consenso sobre los contenidos que se deberían impartir, ni la forma de hacerlo [37], [45], [46].

El NSTISSI No. 4011, de obligatorio cumplimiento para las entidades del gobierno, comienza a ser utilizado como mecanismo de certificación de programas académicos en las universidades por el Centro de Excelencia Académica en Educación de Seguridad de la Información (CAE/IAE por sus siglas en inglés). Esto permite que empiece a producirse un alineamiento progresivo en los esfuerzos de superación profesional en EE.UU [47], [48].

Existe un reconocimiento de la necesidad de la formación continua de los profesionales de la seguridad de la información en la NIST 800-16, publicada en el año 1998 y enfocada en la requisitos de capacitación en seguridad de tecnologías de la información bajo un modelo basado en roles y desempeño [49].

D. Período de 2000-2010

En este periodo las amenazas de ciberseguridad en el ciberespacio son más sofisticadas y frecuentes. Los ataques de malware, phishing y robo de datos aumentaron significativamente [50]. Surgen normativas y estándares como la ISO 27001 que van influyendo en la superación profesional a nivel organizacional [51], [52] y se consolidan los programas académicos certificados a través del CAE/IAE [53].

E. Período de 2010-Actualidad

Este periodo se caracteriza por el surgimiento de marcos de referencias y cuerpos de conocimiento que comienzan a ser utilizados como estándares para el abordaje de la formación y superación profesional a nivel internacional. En el año 2010 se crea la Iniciativa Nacional para la Educación en Ciberseguridad (NICE por sus siglas en inglés) [54]. Posteriormente en el año 2017 se publica el Cybersecurity

Curricula 2017 (CSEC2017) [55] de la ACM. En el 2017 se publica también la primera versión del Cyber Security Body Of Knowledge (CyBOK) en el Reino Unido. Estas propuestas se convierten en referencias de obligatoria consulta para las iniciativas de formación, tanto en el pregrado como en el posgrado en la actualidad, por lo que serán analizadas en más detalles en la siguiente sección.

IV. Principales Marco de Referencia para la Superación Profesional en Ciberseguridad

A. *Cybersecurity Curricula 2017*

El reporte titulado Cybersecurity Curricula 2017. Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity [55], fue diseñado por un equipo de expertos de reconocidas organizaciones en el campo de las ciencias informáticas tales como la ACM, IEEE CS, AIS SIGSEC e IFIP. El CSEC2017 tiene como misión ser una guía curricular integral y flexible, base para el desarrollo de una amplia gama de programas de formación en el campo de la ciberseguridad. En esta se establece que un programa de estudio en ciberseguridad debe contener:

1) Una base de conocimientos en ciencias informáticas.
2) Conceptos transversales que son aplicables en todas las especialidades de la ciberseguridad.
3) Un cuerpo de conocimientos y habilidades esenciales en ciberseguridad.
4) Una relación directa con la variedad de especialidades que debe cubrir la fuerza laboral.
5) Un fuerte énfasis en la conducta ética y las responsabilidades profesionales asociadas con el campo.

Para ello se propone un marco de trabajo curricular en ciberseguridad, el cual se representa en la Fig. 1 Este se divide en tres dimensiones: áreas de conocimientos, conceptos transversales y lentes disciplinarios [56].

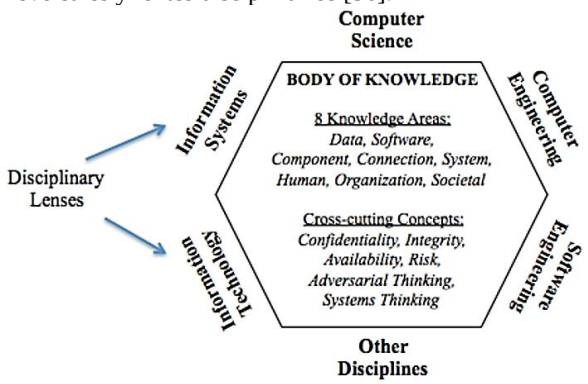

Fig. 1. Cybersecurity Curricula 2017.

Las áreas de conocimiento del modelo son ocho y abarcan desde el nivel básico de protección de datos, hasta el impacto en la sociedad. Por cada área también se identifican cuáles son las competencias esenciales que el estudiante necesita alcanzar, con independencia del programa:

1) Seguridad de los datos: protección de datos en reposo, durante el procesamiento y en tránsito.
2) Seguridad del software: desarrollo y uso de software que preserve de manera confiable las propiedades de seguridad de la información y los sistemas que protege.
3) Seguridad de componentes: diseño, adquisición, prueba, análisis y mantenimiento de componentes integrados en sistemas más grandes.
4) Seguridad de la conexión: seguridad de las conexiones entre componentes, incluidas las conexiones físicas y lógicas.
5) Seguridad del sistema: aspectos de seguridad de los sistemas que integran componentes, conexiones y software.
6) Seguridad humana: proteger los datos y la privacidad de las personas en el contexto de las organizaciones y la vida personal, además del estudio del comportamiento humano en relación con la ciberseguridad.
7) Seguridad organizacional: proteger a las organizaciones de las amenazas a la ciberseguridad y gestionar el riesgo para respaldar el cumplimiento exitoso de la misión de la organización.
8) Seguridad Social: aspectos de la ciberseguridad que afectan ampliamente a la sociedad en su conjunto, para bien o para mal.

El modelo integra también conceptos transversales, los cuales se representan como una base para que los estudiantes puedan identificar las conexiones entre áreas de conocimiento y comprenderlas, independientemente de la lente disciplinaria. Los conceptos transversales propuestos son:

1) Confidencialidad: reglas que limitan el acceso a los datos e información del sistema a las personas autorizadas.
2) Integridad: los datos y la información son precisos y confiables.
3) Disponibilidad: los datos, la información y el sistema son accesibles.
4) Riesgo: potencial de ganancia o pérdida.
5) Pensamiento adversario: proceso de pensamiento que considera las acciones potenciales de la fuerza opuesta trabajando contra el resultado deseado.
6) Pensamiento sistémico: proceso de pensamiento que considera la interacción entre las limitaciones sociales y técnicas para permitir operaciones seguras.

El lente disciplinario es la tercera dimensión del modelo. Representa la disciplina informática subyacente a partir de la cual se pueden desarrollar los programas de ciberseguridad. El lente disciplinario impulsa el enfoque, la profundidad del contenido y los resultados de aprendizaje resultantes de la interacción entre los temas, conceptos esenciales y transversales. El modelo abarca las disciplinas informáticas identificadas por la ACM: ciencia de la computación, ingeniería informática, sistemas de información, tecnología de la información e ingeniería de software.

Por último, en el CSEC2017 se proponen siete áreas de aplicación del modelo a la práctica profesional: políticas públicas, adquisiciones, administración, investigación, desarrollo de software, seguridad de las operaciones TIC y arquitectura empresarial.

Diversos investigadores han manifestado la relevancia del CSEC2017 para el desarrollo de los programas de formación en ciberseguridad [57], [58], [59], [60], [61], [62], [63], [64]. En las publicaciones consultadas se evidencia su utilización para el diseño de currículos de posgrado, a pesar de no ser su enfoque principal [65].

B. *The Cyber Security Body Of Knowledge*

El Cuerpo de Conocimientos de Ciberseguridad (CyBOK) [66] es un proyecto financiado por el gobierno del Reino Unido con el objetivo de mapear las áreas de conocimiento existentes en este campo. En este documento se plantea que los contenidos de ciberseguridad se encuentran aún fragmentados y por tanto

resulta difícil diseñar currículos coherentes de ciberseguridad. El proyecto comenzó en el año 2017 y la última versión publicada data del año 2021.

CyBOK define 21 área de conocimiento en ciberseguridad, clasificadas en cinco grupos, como se representa en la Tabla I. La sistematización de estos conocimientos se realiza a través del análisis de libros de texto, artículos de investigación académica, informes técnicos, libros blancos y estándares y con un enfoque de referencia o mapeo de cada contenido, sin pretender replicar completamente todo lo que se ha escrito sobre un tema. Proponen su aplicación para el diseño de programas educativos que pueden ir desde la enseñanza secundaria hasta el pregrado y el posgrado.

Tabla. I
ÁREAS DE CONOCIMIENTO Y CATEGORÍAS DE CYBOK.

Categorías		Áreas de conocimiento	
I.	Aspectos Humanos, Organizativos y Normativos	1)	Gestión de Riesgos y Gobernanza
		2)	Ley y regulación
		3)	Factores humanos
		4)	Privacidad y derechos en línea
II.	Ataques y Defensas	5)	Malware y tecnologías de ataque
		6)	Comportamientos adversarios
		7)	Operaciones de seguridad y gestión de incidentes
		8)	Forense
III.	Seguridad de Sistemas	9)	Criptografía
		10)	Sistemas Operativos y Virtualización
		11)	Seguridad de sistemas distribuidos
		12)	Métodos formales para la seguridad
		13)	Autenticación, Autorización y Responsabilidad
IV.	Seguridad de software y plataforma	14)	Seguridad del software
		15)	Seguridad web y móvil
		16)	Ciclo de vida del software seguro
V.	Seguridad de la infraestructura	17)	Criptografía aplicada
		18)	Seguridad de la red
		19)	Seguridad de hardware
		20)	Seguridad de sistemas ciber físicos
		21)	Seguridad de la capa física y las telecomunicaciones

C. National Initiative For Cybersecurity Education

La Iniciativa Nacional para la Educación en Ciberseguridad (NICE por sus siglas en inglés) es un marco de trabajo desarrollado por el gobierno, la academia y la industria de EE. UU con el objetivo de proveer orientaciones y principios para el desarrollo profesional, la educación, capacitación y diseño de programas de acreditación en ciberseguridad. Los orígenes del NICE se remontan al año 2010 y es coordinado por el NIST [54]. La última versión fue publicada en el año 2020 [67].

Surgió para responder a la problemática que representaba contar con enfoques diversos y desconectados en relación a las responsabilidades y actividades que deben desempeñarse en la ciberseguridad [68]. Esto ocasionaba que la academia tuviera dificultad para obtener una visión holística sobre que enseñar y por tanto, no fuera capaz de formar adecuadamente en los estudiantes, las habilidades y conocimientos necesarios para los puestos de trabajos que iban a ocupar [54].

Para resolver esta problemática, el NICE brinda una descripción detallada sobre el trabajo de ciberseguridad por categoría, área de especialidad y función laboral. Como se muestra en la Fig. 2, agrupa las tareas, conocimientos y habilidades de ciberseguridad mediante el uso de un léxico común y coherente.

En el NICE, una tarea es una actividad que contribuye al cumplimiento de los objetivos de una organización. Un conjunto de tareas por tanto describe el trabajo que debe realizarse en la ciberseguridad. La descripción de una tarea debe ser clara y concisa, permitiendo su fácil comprensión, incluso si la tarea en sí implica varios pasos.

La descripción de los conocimientos permite que los estudiantes puedan llevar a cabo tareas específicas. El conocimiento se trata en el NICE como un grupo de conceptos que se pueden recuperar de la memoria. Estos pueden ser fundamentales o muy específicos y, en ocasiones, se requiere de múltiples descripciones de conocimientos para completar una sola tarea. Un conocimiento descrito puede ser aplicable a un conjunto de tareas diferentes.

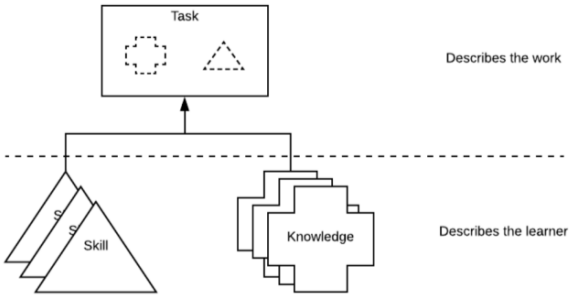

Fig. 2. Enfoque de elementos constitutivos del Marco del NICE. Tomado del NICE.

Las habilidades se manifiestan como la capacidad de llevar a cabo acciones observables y pueden requerir múltiples descripciones para tareas complejas. Además, una sola habilidad puede aplicarse a diferentes tareas. La relación entre habilidades y tareas es fundamental: un estudiante necesita demostrar habilidades concretas para ejecutar tareas específicas.

Tomando como base los marcos de referencias en superación profesional y las demandas existentes de formación se desarrollaron una serie de programas académicos que serán explicados en la siguiente sección.

V. EXPERIENCIAS EN LA SUPERACIÓN PROFESIONAL EN LA UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

La Universidad de las Ciencias Informáticas, IES con sede en La Habana, Cuba, tiene como misión contribuir a la transformación digital de la sociedad cubana, mediante la formación integral y continua de profesionales de las ciencias informáticas comprometidos con su Patria, así como la producción y comercialización de productos y servicios informáticos. En este sentido ha realizado desde su fundación, en el año 2003 diversas acciones de superación profesional en materia de Ciberseguridad.

Específicamente en el año 2016 se realizaron encuestas a estudiantes de posgrados, arrojando como resultado que entre el 80% y el 88% requerían capacitaciones en el campo de la ciberseguridad y más de 85% dijo haber adquirido conocimientos principalmente mediante la autosuperación. El 88% necesitaba formación para detectar la presencia de vulnerabilidades en los sistemas que desarrollan y administran [69]. En este período, la Red Académica Cubana (REDUNIV) señaló también la necesidad de contar con especialistas de ciberseguridad capacitados para el desempeño de su labor, aspecto que ha sido reafirmado en otros espacios nacionales. A partir de los estudios realizados se pudo apreciar:

- Poco nivel de experiencia de los especialistas en seguridad de las TIC y administradores de red, pues estos cambian continuamente.
- Insatisfacciones de los especialistas en seguridad de las TIC con las opciones de superación disponibles para alcanzar un desempeño adecuado en las responsabilidades del cargo.
- Necesidades de profundización del conocimiento sobre ciberseguridad de los directivos que deben aprobar los controles propuestos por los especialistas en seguridad de las TIC.
- Deficiente atención a la seguridad en la etapa de concepción, desarrollo y despliegue de productos de software.

Los aspectos abordados evidenciaron, por tanto, una contradicción entre la necesidad de elevar la ciberseguridad en la infraestructura tecnológica y las deficiencias en materia de superación profesional de los especialistas en seguridad de las TIC y otros profesionales vinculados a la transformación digital en las IES y otras entidades.

A nivel nacional se pudo constatar la ausencia de publicaciones que abordaran, en el orden teórico, la superación profesional en este campo. Los autores se enfocaron en demostrar la importancia de estos conocimientos [70], [71], [72], [73], [74], [75], [76], [77], [78], la formación de usuarios [74], [76], [79], [80], [81], [82], [83] o la protección de las IES [84], [85], [86] pero no profundizan en las habilidades y modos de actuación requeridos por los especialistas.

Solamente se encontró un artículo que abordaba la capacitación sobre una herramienta específica en este campo [87]. Se apreció, por tanto, un insuficiente tratamiento teórico y metodológico en programas de superación profesional.

En función de ello, se trazó una estrategia con el objetivo de crear programas de posgrado que lograran paliar las necesidades de superación existentes en el corto y mediano plazo. Para ello se crearon cursos generales y especializados para ser impartidos en modalidad presencial y a distancia, así como otras variantes de superación obteniéndose los siguientes resultados:

- 17 ediciones del posgrado Fundamentos de la Ciberseguridad en modalidad a distancia.
- 10 ediciones del posgrado Pruebas de Penetración en Aplicaciones Web en modalidad presencial y semipresencial.
- 9 ediciones del posgrado Gestión de redes y servicios telemáticos.
- Una edición del posgrado Métodos automatizados para la detección de ataques de phishing.
- Se han realizado decenas de conferencias magistrales y talleres de ciberseguridad a nivel de organizaciones y congresos nacionales e internacionales en Cuba.
- Se han incorporado posgrados en programas de maestrías y diplomados relacionados con las TIC.
- Se han beneficiado más de 1350 profesionales con estas acciones de superación.

Es necesario destacar que estas acciones de superación han contado también con la participación de estudiantes de México, Colombia, Honduras y Angola.

Teniendo en cuenta que el enfoque de la superación profesional en el campo de la ciberseguridad tiene un alto componente práctico, se diseñó y se empezó a impartir, en el año 2018 una Especialidad de Posgrado en Seguridad Informática, la cual está compuesta de los siguientes cursos y entrenamientos:

- Curso Fundamentos de la Seguridad Informática
- Curso de Metodología de Investigación Científica
- Entrenamiento en Hacking Ético
- Entrenamiento en Elementos de Criptografía
- Entrenamiento en Seguridad en Redes
- Entrenamiento en Gestión Automatizada e Integrada de Controles de Seguridad Informática
- Entrenamiento en Gestión de Incidentes de Seguridad Informática
- Entrenamiento en Seguridad en Aplicaciones para Dispositivos Móviles
- Entrenamiento en Gestión de Configuraciones de Seguridad
- Entrenamiento en protección contra Programas Maliciosos
- Entrenamiento en Sistemas de Detección de Intrusiones

En el año 2023 se graduaron los primeros 25 especialistas de posgrado. A partir de estas experiencias en la superación profesional en ciberseguridad se ha podido constatar:

- Existe la necesidad permanente de superación profesional en ciberseguridad a nivel nacional y regional.
- Las IES juegan un papel importante, garantizando la formación permanente de los profesionales en este campo.
- Los estudiantes de posgrado se motivan más cuando la formación tiene un carácter práctico, reconocen la calidad y exigencia del claustro en la impartición de los contenidos y su evaluación.
- Para el desarrollo de las actividades de laboratorio se requieren tecnologías, servicios telemáticos y redes especializada que no siempre están disponibles por lo que es necesario maximizar las variantes de virtualización de servicios.
- Es necesario fomentar en los estudiantes habilidades de investigación y redacción científica para lograr competencias profesionales integrales.
- La vinculación con especialistas de alto reconocimiento técnico y científico externos a la universidad, aporta valiosos conocimientos y de calidad en las actividades de superación profesional.
- Es esencial la impartición de cursos en modalidad a distancia para lograr cubrir la demanda de superación profesional existente.

A partir de estas experiencias, la UCI decidió extender las opciones de capacitación al pregrado mediante el diseño de una carrera de Ingeniería en Ciberseguridad, única de su tipo en el país, la cual comenzó en el año 2021 y va a tener sus primeros graduados en el presente año 2024. Este nuevo programa académico va a impactar de manera muy positiva en la protección y ampliación de los procesos de Transformación Digital nacionales.

Aunque se tuvieron en cuenta los principales marcos de referencia para la superación profesional en ciberseguridad en el diseño de los programas académicos antes descritos, se tiene como trabajo actual la compatibilización y enriquecimiento de los contenidos del currículo con las propuestas contenidas en dichos marcos, de manera tal que cada vez más, los graduados de pregrado y posgrado cuenten con una formación integral y atemperada a los conocimientos y tendencias actuales en este campo.

VI. Conclusiones

En este artículo se presentó la importancia que reviste la superación profesional para garantizar niveles razonables de ciberseguridad. Se fundamentó el concepto de superación profesional como un proceso de formación dirigido a los graduados universitarias. El estudio de la evolución de la superación profesional en ciberseguridad evidenció que esta fue desarrollándose a la par que surgían nuevas amenazas y desafíos y en especial estuvo muy asociada a la expansión creciente de las TIC en diferentes sectores de la sociedad. Esto significa a su vez que se trata de un proceso en permanente desarrollo, en la medida en que surjan nuevas tecnologías y aplicaciones, será necesario abordar nuevas temáticas emergentes de superación en este campo.

Durante la investigación pudo apreciarse que los principales marcos de referencia para la superación profesional en ciberseguridad (CSEC2017, NICE y CyBOK) se erigen como referencias imprescindibles para cualquier programa académico de pregrado y posgrado.

Finalmente se analizaron los resultados y experiencias alcanzados en la superación profesional en ciberseguridad en la Universidad de las Ciencias Informáticas, IES con una importante experiencia y liderazgo nacional en la formación continua de profesionales. Se constata el enfoque en la formación tanto en el pregrado como el posgrado, los cuales están en permanente perfeccionamiento a partir de las principales tendencias internacionales en este campo.

Referencias

[1] J. R. Saborido Loidi, «Universidad y Desarrollo Sostenible. Visión desde Cuba», presentado en Universidad 2020, La Habana, 2020, pp. 15-15.

[2] R. Ali, «Looking to the future of the cyber security landscape», *Network Security*, vol. 2021, n.º 3, pp. 8-10, mar. 2021, doi: 10.1016/S1353-4858(21)00029-5.

[3] T. Hall, B. Sanders, M. Bah, O. King, y E. Wigley, «Economic geographies of the illegal: the multiscalar production of cybercrime», *Trends in Organized Crime*, vol. 24, n.º 2, pp. 282-307, jun. 2021, doi: 10.1007/s12117-020-09392-w.

[4] H. R. González Brito, «Ciberseguridad: en el centro de la transformación digital», en *Habilitando la Transformación Digital*, A. R. Gutiérrez Rivera, Ed., La Habana: Editorial UH, 2022, pp. 225-255.

[5] A.-A. Adel Ismail, A. M. Arpita, y A.-B. Sara Abdulrahman, «Cybersecurity: Cybercrime Prevention in Higher Learning Institutions», en *Implementing Computational Intelligence Techniques for Security Systems Design*, A. Yousif Abdullatif y A. Wasan, Eds., Hershey, PA, USA: IGI Global, 2020, pp. 255-274. doi: 10.4018/978-1-7998-2418-3.ch013.

[6] I. Bandara, C. Balakrishna, y F. Ioras, «The Need For Cyber Threat Intelligence For Distance Learning Providers And Online Learning Systems», presentado en 15th International Technology, Education and Development Conference, en INTED2021 Proceedings. IATED, mar. 2021, pp. 9312-9321. [En línea]. Disponible en: https://library.iated.org/view/BANDARA2021NEE

[7] N. S. Fouad, «Securing higher education against cyberthreats: from an institutional risk to a national policy challenge», *Journal of Cyber Policy*, pp. 1-18, 2021, doi: 10.1080/23738871.2021.1973526.

[8] Verizon, «2021 Data Breach Investigations Report», Verizon, 2021. [En línea]. Disponible en: http://http://enterprise.verizon.com/DBIR2021

[9] Check_Point, «Check Point Research: Education sector sees 29% increase in attacks against organizations globally», Check Point Blog. [En línea]. Disponible en: https://blog.checkpoint.com/2021/08/18/check-point-research-education-sector-sees-29-increase-in-attacks-against-organizations-globally/

[10] A. Aliyu *et al.*, «A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom», *Applied Sciences*, vol. 10, n.º 10, p. 3660, 2020.

[11] D. E. Imbaquingo Esparza, F. J. Díaz, T. K. Saltos Echeverría, S. R. Arciniega Hidrobo, D. A. León Villavicencio, y A. Robayo Ordoñez, «Information security issues in educational institutions», presentado en 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), jun. 2020, pp. 1-7. doi: 10.23919/CISTI49556.2020.9141014.

[12] A. Alexei, «Network Security Threats to Higher Education Institutions», presentado en Central and Eastern European eDem and eGov Days, 2021, pp. 323-333.

[13] S. Roberts, «Learning lessons from data breaches», *Network Security*, vol. 2018, n.º 11, pp. 8-11, nov. 2018, doi: 10.1016/S1353-4858(18)30111-9.

[14] M. E. Armstrong, K. S. Jones, A. S. Namin, y D. C. Newton, «Knowledge, Skills, and Abilities for Specialized Curricula in Cyber Defense: Results from Interviews with Cyber Professionals», *ACM Transactions on Computing Education*, vol. 20, n.º 4, p. Article 29, 2020, doi: 10.1145/3421254.

[15] P. Chapman, «Defending against insider threats with network security's eighth layer», *Computer Fraud & Security*, vol. 2021, n.º 3, pp. 8-13, mar. 2021, doi: 10.1016/S1361-3723(21)00029-4.

[16] O. Paterson, «Training is the foundation of security», *Computer Fraud & Security*, vol. 2021, n.º 8, pp. 10-13, ago. 2021, doi: 10.1016/S1361-3723(21)00085-3.

[17] A. Alonso-Becerra, M. A. Baños-Martínez, y M. Columbié-Santana, «Los objetivos de desarrollo sostenible desde la proyección estratégica de la educación superior», *Ingeniería Industrial*, vol. 42, pp. 62-77, 2021.

[18] B. R. G. Jesús, D. M. T. Díaz, y Z. S. L. Collazo, *La superación del profesional: mover ideas y avanzar más. La Habana: Editorial Universitaria. Córdoba: El Cid Editor. 146 páginas*. 2018.

[19] Consejo_de_Estado, «DECRETO LEY No. 350 "DE LA CAPACITACIÓN DE LOS TRABAJADORES"». 2017.

[20] M. del Llano Meléndez y V. Arencibia Sosa, «Formación inicial y permanente de los profesores en los Institutos Superiores Pedagógicos», en *Presentado en el Congreso Pedagogía*, 1999.

[21] Z. S. López Collazo, «Enfoques teóricos acerca de la superación profesional, una mirada en las áreas técnicas», *Varona. Revista Científico Metodológica*, 2019, [En línea]. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1992-82382019000100004&nrm=iso

[22] J. P. Anderson, «Information Security in a Multi-User Computer Environment», en *Advances in Computers*, vol. 12, M. Rubtnoff, Ed., Elsevier, 1972, pp. 1-36. doi: 10.1016/S0065-2458(08)60506-9.

[23] P. Charles P y P. Shari Lawrence, *Security in Computing*, Fifth edition. Pearson Education, Inc., 2015.

[24] J. P. Titus, «Security and privacy», *Commun. ACM*, vol. 10, n.º 6, pp. 379-381, jun. 1967, doi: 10.1145/363332.363421.

[25] R. Slayton, «Framing computer security and privacy: the 1960s and 1970s», *SIGCAS Comput. Soc.*, vol. 46, n.º 3, pp. 45-54, dic. 2016, doi: 10.1145/3024949.3024954.

[26] B. Peters, «Security considerations in a multi-programmed computer system», en *Proceedings of the April 18-20, 1967, spring joint computer conference on - AFIPS '67 (Spring)*, Atlantic City, New Jersey: ACM Press, 1967, p. 283. doi: 10.1145/1465482.1465524.

[27] W. H. Ware, *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security*. Santa Monica, CA: RAND Corporation, 1979. doi: 10.7249/R609-1.

[28] R. R. Linde, «Operating system penetration», en *Proceedings of the May 19-22, 1975, national computer conference and exposition on - AFIPS '75*, Anaheim, California: ACM Press, 1975, p. 361. doi: 10.1145/1499949.1500018.

[29] J. P. Anderson, «Computer security technology planning study», ESD-TR-73-51, 1972. Accedido: 16 de marzo de 2024. [En línea]. Disponible en: https://apps.dtic.mil/sti/citations/AD0758206

[30] T. J. Knapp, «Selling Data Security to Upper Management», *Data Management*, pp. 22-25, 1983.

[31] T. J. Misa, «Framing Computer Security and Privacy, 1967–1992», en *Communities of Computing: Computer Science and Society in the ACM*, Association for Computing Machinery and Morgan & Claypool, 2018. Accedido: 16 de marzo de 2024. [En línea]. Disponible en: https://doi.org/10.1145/2973856.2973869

[32] D. E. Denning, «The United States vs. Craig Neidorf: A debate on electronic publishing, Constitutional rights and hacking», *Commun. ACM*, vol. 34, n.º 3, pp. 22-43, mar. 1991, doi: 10.1145/102868.102869.

[33] J. A. Lee, G. Segal, y R. Steier, «Positive alternatives: a report on an ACM panel on hacking», *Commun. ACM*, vol. 29, n.º 4, pp. 297-299, abr. 1986, doi: 10.1145/5684.6377.

[34] R. C. Summers, «An overview of computer security», *IBM Systems Journal*, vol. 23, n.º 4, pp. 309-325, 1984, doi: 10.1147/sj.234.0309.

[35] Walsh, «Protecting information assets through effective computer security training», en *1994 Proceedings of IEEE International Carnahan*

Conference on Security Technology, oct. 1994, pp. 126-127. doi: 10.1109/CCST.1994.363782.

[36] K. A. Forcht, «The need for including data security topics in the college business curriculum», *SIGSAC Rev.*, vol. 4, n.º 3, pp. 9-11, jul. 1986, doi: 10.1145/1058414.1058416.

[37] S. F. Barnett, «Computer security training and education: a needs analysis», en *Proceedings 1996 IEEE Symposium on Security and Privacy*, may 1996, pp. 26-27. doi: 10.1109/SECPRI.1996.502666.

[38] O. O. T. U. S. O. DEFENSE (ACQUISITION y T. W. DC, «Report of the Defense Science Board Task Force On Information Warfare-Defense (IW-D)», 1996, Accedido: 17 de marzo de 2024. [En línea]. Disponible en: https://apps.dtic.mil/sti/citations/tr/ADA432539

[39] D. F. Poindexter, «A Reassessment of Computer Security Training Needs», en *Proceedings of the 13th National Computer Security Conference: «Information Systems Security: Standards--the Key to the Future»*, National Institute of Standards and Technology, 1990, pp. 865-865. doi: 10/01/proceedings-13th-national-computer-security-confer/final.

[40] G. O'Regan, «Computer Crime», en *Ethical and Legal Aspects of Computing: A Professional Perspective from Software Engineering*, G. O'Regan, Ed., Cham: Springer Nature Switzerland, 2024, pp. 237-252. doi: 10.1007/978-3-031-52664-0_12.

[41] «ISC2». Accedido: 30 de marzo de 2024. [En línea]. Disponible en: https://www.isc2.org/about

[42] J. McConnell, «National training standard for information systems security (INFOSEC) professionals», *National Security Agency/Central Security Service Fort George G Meade Md*, 1994, Accedido: 30 de marzo de 2024. [En línea]. Disponible en: https://apps.dtic.mil/sti/pdfs/ADA404113.pdf

[43] C. E. Irvine, P. C. Clark, y D. F. Warren, «The NPS CISR Graduate Program in INFOSEC Education: Six Years of Experience», 1997. [En línea]. Disponible en: https://api.semanticscholar.org/CorpusID:70702587

[44] C. E. Irvine, «The first ACM Workshop on Education in Computer Security», *SIGSAC Rev.*, vol. 15, n.º 2, pp. 3-5, abr. 1997, doi: 10.1145/254594.254595.

[45] C. E. Irvine, S.-K. Chin, y D. Frincke, «Integrating Security into the Curriculum», *Computer*, vol. 31, n.º 12, pp. 25-30, dic. 1998, doi: 10.1109/2.735847.

[46] «Information system security curricula development | Proceedings of the 4th conference on Information technology curriculum». Accedido: 30 de marzo de 2024. [En línea]. Disponible en: https://dl.acm.org/doi/10.1145/947121.947178

[47] M. A. Wright, «Assessing the Impact of Security Education Initiatives on Critical Infrastructure Protection», *Computer Fraud & Security*, vol. 2001, n.º 8, pp. 8-10, ago. 2001, doi: 10.1016/S1361-3723(01)00814-4.

[48] D. Manson y S. S. Curl, «A comparison of academic and government information security curriculum standards», *Proceedings ISECON 2003*, pp. 1-6, 2003.

[49] M. Wilson, D. Zafra, S. Pitcher, J. Tressler, y J. Ippolito, «NIST Special Publication 800-16. Information Technology Security Training Requirements: A Role-and Performance-Based Model», *Gaithersburg, MD: US Department of Commerce*, pp. 800-16, 1998.

[50] J. Ferdous, R. Islam, A. Mahboubi, y Md. Z. Islam, «A Review of State-of-the-Art Malware Attack Trends and Defense Mechanisms», *IEEE Access*, vol. 11, pp. 121118-121141, 2023, doi: 10.1109/ACCESS.2023.3328351.

[51] M. Mirtsch, J. Kinne, y K. Blind, «Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis», *IEEE Transactions on Engineering Management*, vol. 68, n.º 1, pp. 87-100, feb. 2021, doi: 10.1109/TEM.2020.2977815.

[52] M. Gorge, «Security for third level education organizations and other educational bodies», *Computer Fraud & Security*, vol. 2007, n.º 7, pp. 6-9, jul. 2007, doi: 10.1016/S1361-3723(07)70089-1.

[53] A. Yasinsac y M. Burmester, «Centers of academic excellence: a case study», *IEEE Security & Privacy*, vol. 3, n.º 1, pp. 62-65, ene. 2005, doi: 10.1109/MSP.2005.8.

[54] C. Paulsen, E. McDuffie, W. Newhouse, y P. Toth, «NICE: Creating a Cybersecurity Workforce and Aware Public», *IEEE Security & Privacy*, vol. 10, n.º 3, pp. 76-79, 2012, doi: 10.1109/MSP.2012.73.

[55] CSEC2017, *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. Association for Computing Machinery Joint Task Force on Cybersecurity Education, 2018.

[56] I. Ashby y M. Exter, «Designing for Interdisciplinarity in Higher Education: Considerations for Instructional Designers», *TechTrends*, vol. 63, n.º 2, pp. 202-208, mar. 2019, doi: 10.1007/s11528-018-0352-z.

[57] S. von Solms y L. Futcher, «Identifying the Cybersecurity Body of Knowledge for a Postgraduate Module in Systems Engineering», presentado en Information Security Education – Towards a Cybersecure Society, L. Drevin y M. Theocharidou, Eds., Cham: Springer International Publishing, 2018, pp. 121-132.

[58] M. Hudnall, «Educational and Workforce Cybersecurity Frameworks: Comparing, Contrasting, and Mapping», *Computer*, vol. 52, n.º 3, pp. 18-28, 2019, doi: 10.1109/MC.2018.2883334.

[59] A. Parrish, R. K. Raj, y L. Jones, «Academic Cybersecurity Disciplinary Foundations and Accreditation», presentado en Proceedings of the 50th ACM Technical Symposium on Computer Science Education, Minneapolis, MN, USA: Association for Computing Machinery, 2019, p. 1248. doi: 10.1145/3287324.3293728.

[60] D. Shoemaker, A. Kohnke, y K. Sigler, «What the profession of cybersecurity needs to know and do», *EDPACS*, vol. 59, n.º 2, pp. 6-18, feb. 2019, doi: 10.1080/07366981.2019.1565106.

[61] S. Elder, N. Zahan, V. Kozarev, R. Shu, T. Menzies, y L. Williams, «Structuring a Comprehensive Software Security Course Around the OWASP Application Security Verification Standard», presentado en 2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering Education and Training (ICSE-SEET), may 2021, pp. 95-104. doi: 10.1109/ICSE-SEET52601.2021.00019.

[62] S. Furnell, «The cybersecurity workforce and skills», *Computers & Security*, vol. 100, p. 102080, ene. 2021, doi: 10.1016/j.cose.2020.102080.

[63] J. Hajny, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta, y R. D. Nicola, «Framework, Tools and Good Practices for Cybersecurity Curricula», *IEEE Access*, vol. 9, pp. 94723-94747, 2021, doi: 10.1109/ACCESS.2021.3093952.

[64] I. Ngambeki, S. McBride, y J. Slay, «Knowledge Gaps in Curricular Guidance for ICS Security», presentado en Journal of The Colloquium for Information Systems Security Education, 2022, pp. 6-6.

[65] R. K. Raj, V. Anand, D. Gibson, S. Kaza, y A. Phillips, «Cybersecurity Program Accreditation: Benefits and Challenges», presentado en Proceedings of the 50th ACM Technical Symposium on Computer Science Education, Minneapolis, MN, USA: Association for Computing Machinery, 2019, pp. 173-174. doi: 10.1145/3287324.3287325.

[66] A. Rashid, H. Chivers, E. Lupu, A. Martin, y S. Schneider, «The Cyber Security Body of Knowledge», University of Bristol, 2021. [En línea]. Disponible en: https://www.cybok.org/

[67] W. Newhouse, S. Keith, B. Scribner, y G. Witte, «National initiative for cybersecurity education (NICE) cybersecurity workforce framework», 2020.

[68] V. Nestler, T. Coulson, y J. D. Ashley, «The NICE Challenge Project: Providing Workforce Experience Before the Workforce», *IEEE Security & Privacy*, vol. 17, n.º 2, pp. 73-78, 2019, doi: 10.1109/MSEC.2018.2888784.

[69] H. R. González Brito, «Diseño de un curso de posgrado de pruebas de penetración en aplicaciones web», presentado en VI Simposio Nacional INFODISK 2020, Santiago de Cuba. Cuba.: Universidad de Oriente, 2020.

[70] A. F. M. Giraldoni, E. H. Barrio, J. M. Torres, y A. S. Echevarría, «Problemas éticos y de seguridad asociados al uso de las tecnologías de la información y el conocimiento en Salud», *Medisur: Revista Electrónica de las Ciencias Médicas en Cienfuegos*, vol. 6, n.º 1, pp. 84-88, 2008.

[71] A. Morejón Alfonso y H. C. Domínguez Arocha, «La seguridad informática es un componente esencial de la Seguridad Nacional», *Mendive. Revista Científico Pedagógica.*, vol. 10, n.º 3, pp. 213-218, 2012.

[72] E. R. Regalado Miranda y E. M. Regalado Miranda, «Nuevos retos en informatización y ciberseguridad para la Universidad de Ciencias Médicas de La Habana», *Revista Habanera de Ciencias Médicas*, vol. 14, n.º 4, pp. 376-379, 2015.

[73] M. de los Á. Sesé Montalvo, M. Agustina Morales Laborí, y M. Yulexis Villa Hernández, «La seguridad Informática en el Contexto Educacional Cubano», 2015.

[74] G. G. G. Pierrat y M. J. V. Ledo, «La informática y la seguridad. Un tema de importancia para el directivo», *Revista de Información científica para la Dirección en Salud. INFODIR*, n.º 22, pp. 47-58, 2016.

[75] O. Almaguer Aguilera, E. de J. Osmán Pérez Alí, y R. Cuesta Rivero, «La protección de la información. una visión desde las entidades educativas cubanas», *Ciencias de la Información*, vol. 48, n.º 3, pp. 41-47, 2018.

[76] N. C. González Cadalso, J. R. Beltrán Barrizonte, y R. L. Paz Companioni, «El gobierno electrónico, su impacto en la seguridad de la información», *Observatorio de la Economía Latinoamericana*, n.º marzo, 2019.

[77] M. Borjas Aguilera, O. Almaguer Aguilera, y E. de J. Osmán Pérez Alí, «Aproximación a la ética informática en la Educación Superior», *Espergesia*, vol. 7, n.º 2, pp. 33-45, 2020.
[78] D. F. Roca-Castro y M. F. Roca-Castro, «Las TIC en la educación superior. Retos para la innovación académica», *Dominio de las Ciencias*, vol. 6, n.º 4, pp. 1221-1235, 2020.
[79] L. López Leiva, «Sistema de acciones de superación en seguridad informática para docentes de economía del ISP Félix Varela», Universidad Central "Marta Abreu" de Las Villas. Centro de Estudio, Santa Clara, Cuba, 2009.
[80] Y. Tamayo Noa, «Sitio Web "Seguridad Informática" para profesores y estudiantes de Secundaria Básica», Universidad de Ciencias Pedagógicas José de la Luz y Caballero, Holguín, Cuba, 2010.
[81] W. Betancourt Falcón, H. M. Barrera Pérez, y Y. Blanco Gallardo, «Sitio Web acerca del sistema normativo del Ministerio de Educación para la preparación jurídica de los cuadros en la Universidad Pedagógica de Pinar del Río», *Mendive. Revista de Educación*, vol. 11, n.º 4, pp. 379-387, 2013.
[82] E. Durán-Rodríguez, «Seguridad informática: un reto para los usuarios de los sistemas informáticos», *Educación y sociedad*, vol. 12, n.º 2, pp. 146-162, 2014.
[83] R. Font-Hernández, «La dimensión seguridad y sus elementos esenciales para la Competencia Básica en Infocomunicaciones y su inserción en el currículo de las carreras pedagógicas», *Maestro y Sociedad*, vol. 12, n.º 2, pp. 75-82, 2015.
[84] I. E. Conde, S. S. Millán, y Y. M. Martín, «Sistema para la Gestión de Información de Seguridad Informática en la Universidad Máximo Gómez Báez de Ciego de Ávila.», *Universidad&Ciencia*, vol. 3, n.º 3, pp. 96-106, 2014.
[85] Y. Díaz-Ricardo, Y. Pérez-del Cerro, y D. Proenza-Pupo, «Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín», *Ciencias Holguín*, vol. 20, n.º 2, pp. 1-14, 2014.
[86] J. M. Castellanos, E. Toledo, y L. Castellanos, «Automatización de Controles de Seguridad Informática en la UCF», *Infometric@-Serie Ingeniería, Básicas y Agrícolas*, vol. 2, n.º 1, 2019.
[87] M. Arias Lescay, L. A. Acosta Montoya, L. Ladoy Estrada, G. de la Vega Torre, y L. G. Yero Barrera, «Estrategia de superación para la utilización de proxmox y pfSense en las instituciones de salud», *Revista Cubana de Informática Médica*, vol. 11, n.º 2, pp. 100-114, 2019.