Tipo de artículo: Artículo original

Estrategia para el perfeccionamiento curricular de las asignaturas de informática en los planes de estudio de nivel superior en temáticas de ciberseguridad

Strategy for the curricular enhancement of computer science subjects in higher education curricula on cybersecurity issues

Antonio Hernández Dominguez [1*], https://orcid.org/0000-0001-8391-3064
Yunia Reyes González [2], https://orcid.org/0000-0001-7143-7080
Madelis Pérez Gil [3], https://orcid.org/0000-0002-4441-7102

[1] Departamento Docente de Ciberseguridad. Facultad de Ciberseguridad. Universidad de las Ciencias Informáticas. Cuba. ahdominguez@uci.cu
[2] Dirección de Ciencia, Tecnología e Innovación. Universidad de las Ciencias Informáticas. Cuba. yrglez@uci.cu
[3] Departamento Docente de Ciberseguridad. Facultad de Ciberseguridad. Universidad de las Ciencias Informáticas. Cuba. mgil@uci.cu

*** Autor para correspondencia: ahdominguez@uci.cu**

Resumen

La necesidad de actualizar continuamente los planes de estudio en informática, especialmente en ciberseguridad, es crucial en la era digital. La investigación aborda el desarrollo de una estrategia que permita actualizar los planes de estudio en las asignaturas de informática, enfocándose en carreras afines al campo de la ciberseguridad, debido a la creciente dependencia de la tecnología y la información digital. La falta de una actualización curricular sistemática en Programación e Ingeniería y Gestión de Software, limita la preparación de los estudiantes para enfrentar desafíos actuales en esta área del conocimiento. Se propone como principal misión desarrollar una propuesta de perfeccionamiento curricular que incluya fundamentos y prácticas innovadoras en estas áreas. Además, se destaca la importancia de la formación continua y la calidad educativa, alineándose con los Objetivos de Desarrollo Sostenible de la ONU. Se enfatiza la necesidad de una colaboración más estrecha entre la academia y la industria para asegurar que los egresados estén bien preparados y que se contribuya a un entorno digital más seguro en el país.

Palabras clave: informática; ciberseguridad; plan de estudios; perfeccionamiento

Abstract

Currently it is very important to update computer science curricula, especially in cybersecurity. This is crucial in the digital era. This research approaches the development of a curricular updating strategy in computer science subjects, focusing on careers related to the field of cybersecurity, due to the growing dependence on technology and digital information. The inexistence of a systematic curricular update in Programming and Software Engineering and Management, limits the preparation of students to face the current challenges in this area of knowledge. The main objective is to develop a proposal for curricular improvement that includes fundamentals and innovative practices in these areas. In addition, the importance of continuous training and educational quality is highlighted, aligning with the UN Sustainable Development Goals. It emphasizes the need for closer

collaboration between academia and industry to ensure that graduates are well prepared and contribute to a more secure digital environment in the country.

Keywords: *computer science; cybersecurity; educational curriculum; further education*

Recibido: 16/08/2024
Aceptado: 22/10/2024
En línea: 01/11/2024

Introducción

Paralelo al desarrollo y penetración de las Tecnologías de la Información y las Comunicaciones (TIC) crece la necesidad de la seguridad de la información que es generada, almacenada, intercambiada y procesada. Las tendencias mundiales revelan un crecimiento exponencial de acciones malignas encaminadas a poner en riesgo la seguridad de la información. Para el contexto descrito, inicialmente las comunidades científicas y las comunidades de desarrolladores de software, han desarrollado enfoques y paradigmas de Programación e Ingeniería y Gestión de Software, que hicieran posible el desarrollo de software. Estos enfoques han necesitado, y lo siguen necesitando, una transformación y actualización constante que atempere sus postulados a las necesidades cada vez más crecientes y complicadas en estas áreas del conocimiento.

En este mismo período de tiempo, se actualizaron los postulados teóricos y las prácticas profesionales relativas a la seguridad de los sistemas informáticos y sus soportes tecnológicos, principalmente en cuanto a sistemas operativos, arquitectura de computadoras y redes de computadoras. Esta actualización ha ofrecido cuerpo teórico y curricular a la especialización en Ciberseguridad tanto en el pregrado como en el postgrado.

En el contexto socio-económico-político cubano en el presente siglo, se ha logrado una proyección estratégica del modelo económico-social para la nación con vista al 2030; que a su vez está alineada con los Objetivos de Desarrollo Sostenible (Agut & Del Pilar, 2015) de la Organización de Naciones Unidas (ONU) hacia el 2030. En el primero de los documentos se enfatiza en la necesidad de una mejor preparación de los especialistas y personal técnico que garantice el desarrollo científico-tecnológico de la nación; y que esta debe sostenerse en un perfeccionamiento y actualización continuos de los planes de formación, capacitación y superación del capital humano con que cuenta el país y en los que tanto ha invertido la nación en su período revolucionario.

Por su parte, el Ministerio de Educación Superior (MES), en la concepción de los planes de estudio (MES, 2022) en su generación E, enfatizó en la necesidad de elevar la preparación práctica de los egresados tanto en pregrado como en postgrado; así como diseñar programas y planes de estudio que potenciar la formación desde la industria de

software y los puestos de trabajos existentes alrededor de la misma. Similares reforzamientos en los diseños curriculares se indicaron para lograr una formación con énfasis en el uso de las TIC y el desarrollo de habilidades sociales y profesionales para la era digital.

A su vez, el Consejo de Ministros en sus documentos estratégicos (Ministros, 2021) para igual período; en especial las políticas trazadas para la informatización y la transformación digital en el país hacia el 2030, enfatiza tanto en la necesaria y constante preparación de los especialistas, como en la calidad de la formación, capacitación y superación que deben lograrse para mantener actualizado y con elevado nivel científico a los profesionales de este sector. Estos principios se priorizan en lo referente a los especialistas en Ciberseguridad por su impacto en la sostenibilidad de las comunicaciones, la soberanía digital y la transformación digital del país.

Cuba no ha estado ajena a este contexto descrito y en los últimos 20 años, en la Universidad de las Ciencias Informáticas (UCI), específicamente en la Facultad de Ciberseguridad, se creó la especialidad de postgrado en "Seguridad Informática"; y finalmente el programa de pregrado "Ingeniería en Ciberseguridad". En estos dos programas se ofrecen asignaturas en las temáticas de Programación, Ingeniería de Software, Bases de Datos, y Gestión de Software.

En el contexto descrito y en específico en la UCI, se ejecutan hoy los planes de estudio de estas dos especializaciones (1 en postgrado y 1 en pregrado) con programas en las asignaturas de Informática (Programación, Bases de Datos, Ingeniería de Software, y Gestión de Software) cuyos diseños curriculares tomaron un alto por ciento de aquellos procedentes de otras especializaciones afines como Ingeniería Informáticas, Ingeniería en Ciencias Informáticas e Ingeniería en Telecomunicaciones. Sin embargo, se percibe hoy por el claustro de profesores en estas especializaciones, que existen insuficiencias en la especificación y especialización de estos programas hacia la satisfacción de los problemas profesional que cumplen estos especialistas en sus esferas de actuación profesional.

Lo anterior se acrecienta (Martínez López, 2023), toda vez que se utilizan hoy iguales enfoques metodológicos y de diseño curricular para los ejercicios docente-metodológico y científico-metodológico que aquellos que sustentan el Proceso Docente-Educativo en las especializaciones de las que se nutrieron estos planes de estudio, sin haberse producido en la actualidad una transformación que favorezca tanto el diseño de los planes, como su implementación; así como la concepción y el desarrollo del claustro para servir de base al logro de los objetivos previstos en los planes de estudio. A pesar que hoy se logran positivos resultados en la promoción y retención de los estudiantes en ambos niveles de estudios, sí debe lograrse mayor nivel de interdisciplinariedad entre estas asignaturas y aquellas con las que

comparten en tiempo y espacio; así como mayor nivel de coherencia interna entre estas, toda vez que forman parte de un micro sistema altamente articulado en el ejercicio profesional de los egresados.

En resumen, la situación actual de estas especializaciones en cuanto a las asignaturas de Informática se puede caracterizar de la siguiente forma:

1. Programas de las asignaturas con necesidad de actualización y especificación científico-técnica.
2. Procederes metodológicos para la enseñanza y el aprendizaje de las asignaturas que no favorecen de forma eficiente y eficaz el desarrollo de competencias de la era digital.
3. Concepciones de la preparación docente para los claustros de estas asignaturas que no promueven eficientemente el uso de enfoques y práctica pedagógicas y didácticas acorde con la era digital y el tipo de egresado en estos programas.

Teniendo en cuenta la situación expuesta se identifica el siguiente problema: ¿Cómo lograr la actualización curricular sistemática de las materias de Programación e Ingeniería y Gestión de Software en los planes de estudio de nivel superior asociados a la ciberseguridad, a partir de la mejora continua del diseño curricular y del trabajo docente y científico-metodológico?

Para lograr resolver el problema planteado, se ha definido como Objetivo general el de "Desarrollar una propuesta de perfeccionamiento curricular de las asignaturas de Informática a partir de los fundamentos y prácticas más novedosas en Programación e Ingeniería y Gestión de Software, para dotar a las comisiones nacionales de carrera y comités académicos de postgrado de una actualización del currículo y su implementación en los programas universitarios de pregrado y postgrado en las temáticas de ciberseguridad.

Materiales y métodos

Actualmente la carrera de Ingeniería en Ciberseguridad en la UCI se dirige desde el Departamento Docente de Ciberseguridad en la Facultad de Ciberseguridad. Esta carrera forma profesionales integrales, comprometidos con la patria y con el desarrollo del modelo socialista cubano, cuya función está asociada al empleo seguro de las TIC para la informatización de la sociedad cubana y a la defensa del ciberespacio nacional.

El Ingeniero en Ciberseguridad tiene como objeto de la profesión (MES, 2020) la gestión de la ciberseguridad de las organizaciones, a partir del diseño, implementación, operación, monitorización, revisión, mantenimiento y mejora continua de las medidas necesarias para la preservación de la confidencialidad, integridad y disponibilidad de la información; así como la protección de las tecnologías mediante las cuales esta información es creada, procesada,

almacenada y transmitida. En este sentido las asignaturas de informática se encuentran dentro de la disciplina Diseño y Programación de Software, de ahí que la siguiente propuesta incida directamente en la actualización del programa de las asignaturas de dicha disciplina y tribute directamente a la superación del claustro y por consiguiente a la preparación de los estudiantes y futuros egresados.

En este sentido y como solución al problema se concibió una estrategia, la cual se basa en los pilares fundamentales de la concepción de un proyecto institucional propio del departamento. La estrategia plantea las siguientes etapas:

- Propuestas teórico-metodológicas con impacto no solo en la UCI, sino en las instituciones con programas de pregrado y postgrado asociados a la ciberseguridad.
- Vínculos con las entidades empleadoras de los especialistas en ciberseguridad y redes de computadoras.
- Dominio curricular y metodológico de los docentes asociados al programa de pregrado de ICS y de postgrado en la ESI en la UCI que imparten asignaturas de Programación e Ingeniería y Gestión de Software.

Plan de acciones de la estrategia:

- Aplicar un diagnóstico a los futuros empleadores y entidades donde hoy día los estudiantes realizan sus prácticas laborales acerca de las necesidades profesionales desde la producción y la industria.
- Aplicar un diagnóstico de la formación de los docentes involucrados en la carrera Ingeniería en Ciberseguridad que permita establecer las necesidades de capación que necesitan los docentes para asumir las asignaturas del perfil informático en la carrera.
- Diseñar un Modelo de perfeccionamiento curricular continuo de las asignaturas de Informática a partir de los fundamentos y prácticas más novedosas en Programación e Ingeniería y Gestión de Software para los programas universitarios en temáticas de ciberseguridad y redes de computadoras.
- Diseñar un sistema de capacitación y trabajo metodológico para los colectivos docentes de las materias asociadas a la Programación e Ingeniería y Gestión de Software en el programa de ICS en la UCI.
- Realizar una propuesta de programa analítico de las asignaturas de Programación, Ingeniería y Gestión de Software para ciberseguridad y en planes de estudio de pregrado y postgrado.

Desarrollar de Trabajos de Diplomas relacionados con aplicaciones web para la gestión de competencias de los roles programador y analista de software de aplicaciones informáticas para la ciberseguridad.

Resultados y discusión

Como parte del "Diagnóstico de las necesidades profesionales desde la producción y la industria" se concibió un primer resultado denominado "Estado de las necesidades profesionales desde la producción y la industria para el perfeccionamiento continuo de las asignaturas de Informática para los programas universitarios en temáticas de ciberseguridad". A partir de la valoración de la percepción del diseño curricular de las asignaturas de informática en el programa de Ingeniería en Ciberseguridad (ICS), se arrojó que los especialistas en Ciberseguridad deben realizar las siguientes actividades: detectar y solucionar contagios por malware; supervisar el uso de sistemas de protección de datos; planificar e implementar estrategias para asegurar la información; implementar protocolos criptográficos y herramientas de seguridad basadas en estos protocolos; detectar y analizar amenazas de seguridad; conocer y desarrollar técnicas de prevención y detección de intrusos; dominar las normativas reguladoras de la Ciberseguridad; conocer los procedimientos estándares de centros de respuesta a incidentes de seguridad y crear proyectos de seguridad informática.

Desde el punto de vista de los conocimientos ordenados de mayor a menor importancia, se recogieron las siguientes temáticas para los especialistas en ciberseguridad: sistemas informáticos, redes, hardware y software; conocimientos especializados en informática; protección de datos; seguridad en las redes de datos; programas malignos; seguridad de base de datos; seguridad de aplicaciones y códigos, herramientas y lenguajes de programación. En el caso de las habilidades transversales predefinidas se determinan que son muy importantes el trabajo en equipo, presentación de información, recuperación/revisión de literatura científica, redacción técnica, trabajo con las TIC, discusión y argumentación científica.

De ahí que se concibieron anteproyectos de mejoras en una primera etapa para los programas analíticos de las siguientes asignaturas pertenecientes a la disciplina Diseño y programación de software:

1. Seguridad en el Desarrollo de Software
2. Elementos de diseño de sistemas web
3. Inteligencia artificial

En la asignatura de Seguridad en el Desarrollo de Software (SDSW):

Pocos modelos de ciclo de vida de desarrollo de software (SDLC) abordan explícitamente la seguridad del software en detalle, por lo que las prácticas seguras de desarrollo de software generalmente deben agregarse a cada modelo SDLC para garantizar que el software que se desarrolla esté bien protegido.

En el curso 2019/2020 se elaboró y aprobó, la primera versión del Programa Analítico de la asignatura Seguridad en el Desarrollo de Software a impartirse en el 3er año de la Carrera de Ingeniería en Ciberseguridad. Tres años después cuando se impartiría por primera vez la misma, el colectivo de profesores decidió hacer varias modificaciones a este documento, a raíz de la evolución que ha tenido el desarrollo de software seguro del año 2020 a la fecha. Uno de los documentos incluidos, es el "*Marco de desarrollo de software seguro (SSDF)*" que propone el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés).

En este documento (Souppaya et al., 2022) emitido en febrero de 2022 se recomienda un conjunto básico de buenas prácticas de desarrollo de software seguro de alto nivel que se pueden integrar en cada implementación de SDLC. Seguir tales prácticas debería ayudar a los productores de software a reducir la cantidad de vulnerabilidades en el software publicado, reducir el impacto potencial de la explotación de software no detectado o no abordado.

Es por tal motivo, unido a varias regulaciones, normas, estándares y avances que han existido en Cuba, es que se decide realizar un anteproyecto de mejora del programa analítico de la asignatura, en función de impartir contenido más actualizado y acorde a las tendencias internacionales y nacionales.

En la asignatura de Elementos de Diseño de Sistemas Web (EDSW):

En la actualidad, el desarrollo seguro de aplicaciones consiste en aplicar ciertas consideraciones y elementos durante el periodo de tiempo que dura la creación de la aplicación hasta lanzarla a producción (Varela Gutiérrez, 2021). Inclusive, una vez distribuida al público, también se deben seguir un conjunto de buenas prácticas para proteger al software de posibles amenazas. Los sistemas web tienen una alta probabilidad de enfrentarse a amenazas desencadenadas por diversos factores: fallos del sistema debidos a una codificación incorrecta, servidores mal configurados y problemas de diseño de la propia aplicación (Carmona Salazar & Rivas Maldonado, 2020).

En el curso 2019/2020 se elaboró y aprobó, la primera versión del Programa Analítico de la asignatura EDSW a impartirse en el 3er año de la Carrera de Ingeniería en Ciberseguridad. Tres años después cuando se impartiría por primera vez la misma, el colectivo de profesores decidió hacer varias modificaciones a este documento, a raíz de la evolución que ha tenido el desarrollo de software seguro del año 2020 a la fecha.

A partir de las experiencias obtenidas producto a la integración de SDSW con la asignatura EDSW se propusieron un conjunto de cambios siguiendo las buenas prácticas de los modelos de ciclo de vida de desarrollo de software (SDLC) y el "Marco de desarrollo de software seguro (SSDF)".

Se reajustaron las horas de conferencias y laboratorios inicialmente concebidas, potenciando en los estudiantes que tuvieran más horas de práctica guiada por los profesores de ambas asignaturas. Además, tras la valoración realizada al programa analítico de la asignatura se proponen añadir contenidos asociados a:

1. La implementación de patrones de diseño seguro como por ejemplo Validador Interceptor, Escape de las salidas, Proxy confiable, Canal seguro e Identificador de autenticidad de transacciones, entre otros que se correspondan a los mecanismos de seguridad seleccionados.
2. Mecanismos para evitar o reducir las posibilidades de ataque de las principales vulnerabilidades.
3. Buenas prácticas en el desarrollo seguro de sistemas web bajo la metodología DevSecOps.

En la asignatura de Inteligencia Artificial:

A partir de las necesidades identificadas en entrevistas con organismos potenciales empleadores de los futuros egresados de la carrera de Ciberseguridad y del perfil del ingeniero en Ciberseguridad, en correspondencia con las prácticas y tendencias actuales relacionadas fundamentalmente con:

- La detección de amenazas con precisión
- La automatización de respuestas
- Optimización de los esfuerzos de los administradores.
- El análisis de datos relacionados con incidentes de ciberseguridad
- La detección temprano de comportamientos anómalos en redes de datos
- La importancia de la video vigilancia a partir del reconocimiento de patrones

Basado en estos preceptos y a partir del actual programa aprobado de Inteligencia Artificial según se muestra en la tabla 1 y se detalla en el anexo 1 se proponen cambios en el actual programa docente de la asignatura Inteligencia Artificial en la carrera ICS. Además, se tiene como un antecedente importante que ya se impartió por primera vez esta asignatura el periodo anterior, obteniendo buenos resultados docentes.

Tabla 1: Propuesta de distribución de horas por temas de la asignatura IA.

Temas	C	CP	S	L	Eval	Total
Tema 1: Métodos de solución de problemas de IA	10	12			2	**24**
Tema 2: Conocimiento e incertidumbre	10	10				**20**
Tema 3: Aprendizaje	6	8		4	2	**20**
Totales	**26**	**30**		**4**	**4**	**64**

Por tal motivo se proponen modificaciones (Tabla 2) dirigidas a:

- Fortalecer la orientación de las actividades docentes hacia la resolución de problemas relacionados con la ciberseguridad.
- Incrementar la cantidad de horas en el tema 3 de la asignatura dedicada al aprendizaje automático.
- Incrementar la cantidad de horas en actividades de prácticas de laboratorio.

Tabla 2: Propuesta de distribución de horas por temas de la asignatura IA.

Temas	C	CP	S	L	Eval	Total
Tema 1: Métodos de solución de problemas de IA	10	10				**20**
Tema 2: Conocimiento e incertidumbre	8	10			2	**20**
Tema 3: Aprendizaje	10	2	2	8	2	**24**
Totales	**28**	**22**	**2**	**8**	**4**	**64**

La descripción detallada de las actividades puede apreciarse en las evidencias del proyecto para esta etapa. Por otra parte, se propone el programa docente de una nueva asignatura optativa titulada "*Aprendizaje Automático*", dada la importancia de reforzar y profundizar en estas técnicas que resultan muy útiles en la resolución de problemas de ciberseguridad con Inteligencia Artificial.

Conclusiones

El perfeccionamiento curricular de las asignaturas de informática en los planes de estudio de nivel superior, con un enfoque en ciberseguridad, es una necesidad imperante en la era digital actual. La creciente dependencia de la tecnología y la información digital ha puesto de manifiesto la importancia de formar profesionales capacitados para enfrentar los desafíos de la ciberseguridad.

La inclusión de temáticas de ciberseguridad en los planes de estudio asegura que los estudiantes estén al tanto de las últimas amenazas y técnicas de defensa. Esto no solo mejora su aplicabilidad, sino que también contribuye a la creación de un entorno digital más seguro en las organizaciones del país. Un currículo actualizado en ciberseguridad fomenta el desarrollo de competencias técnicas y analíticas esenciales. Los estudiantes adquieren habilidades prácticas que les permiten identificar, prevenir y mitigar riesgos cibernéticos de manera efectiva.

La demanda de profesionales en ciberseguridad está en constante crecimiento. Al adaptar los planes de estudio a estas necesidades, la universidad y el departamento no solo responden a las exigencias del mercado laboral, sino que también contribuyen al fortalecimiento de la seguridad nacional e internacional. Además de las habilidades técnicas, es crucial inculcar una conciencia ética en los futuros profesionales. La educación en ciberseguridad debe enfatizar la

importancia de la ética y la responsabilidad en el manejo de la información y la protección de la privacidad. El perfeccionamiento curricular debe ser un proceso continuo y colaborativo, involucrando a expertos de la industria, académicos y reguladores. Solo a través de un esfuerzo conjunto se puede garantizar que los programas educativos se mantengan relevantes y efectivos.

Finalmente, la integración de la ciberseguridad en los planes de estudio de informática es esencial para preparar a los estudiantes para los desafíos del mundo digital. Este enfoque no solo mejora la calidad de la educación, sino que también fortalece la seguridad y la resiliencia de nuestras infraestructuras digitales.

Conflictos de intereses

Los autores no poseen conflictos de intereses.

Contribución de los autores

1. Conceptualización: Antonio Hernández Dominguez
2. Curación de datos: Yunia Reyes González
3. Análisis formal: Madelis Pérez Gil
4. Investigación: Antonio Hernández Dominguez, Yunia Reyes González, Madelis Pérez Gil
5. Metodología: Madelis Pérez Gil
6. Administración del proyecto: Antonio Hernández Dominguez
7. Supervisión: Yunia Reyes González
8. Validación: Antonio Hernández Dominguez
9. Visualización: Yunia Reyes González
10. Redacción – borrador original: Antonio Hernández Dominguez, Yunia Reyes González, Madelis Pérez Gil
11. Redacción – revisión y edición: Antonio Hernández Dominguez, Yunia Reyes González, Madelis Pérez Gil

Financiamiento

La investigación no requirió fuente de financiamiento externa.

Referencias

Agut, M., & Del Pilar, M. (2015). Objetivos de Desarrollo Sostenible (ODS, 2015-2030) y Agenda de Desarrollo post 2015 a partir de los objetivos de desarrollo del milenio (2015-2030). *Organización de Naciones Unidas*.

Carmona Salazar, A. J., & Rivas Maldonado, H. (2020). Mejores prácticas en el desarrollo seguro de aplicaciones.

Martínez López, J. (2023). *Desarrollo de situación de aprendizaje aplicado a la enseñanza de la programación y ciberseguridad* Universidad Internacional de Andalucía].

MES. (2020). Plan de Estudios E de la Carrera en Ingeniería en Ciberseguridad. In UCI (Ed.).

Reglamento organizativo del proceso docente y de dirección del trabajo docente y metodológico para las carreras universitarias. Resolución 47/2022, (2022). https://www.gacetaoficial.gob.cu/es/gaceta-oficial-no-129-ordinaria-de-2022

Decreto 42-2021. Reglamento General Telecomunicaciones, Tecnología de la Información y la Comunicación, (2021). https://www.gacetaoficial.gob.cu/es/gaceta-oficial-no-92-ordinaria-de-2021

Souppaya, M., Scarfone, K., & Dodson, D. (2022). Secure software development framework (ssdf) version 1.1. *NIST Special Publication*, *800*, 218.

Varela Gutiérrez, B. (2021). Desarrollo seguro de software bajo la metodología DevSecOps.