Ciberseguridad y desarrollo de habilidades digitales: propuesta de alfabetización digital en edades tempranas

Olda Bustillos Ortega
obustillos@uia.ac.cr
https://orcid.org/0000-0003-2822-3428
Escuela de Ingeniería Informática de la Universidad Internacional de las Américas, Costa Rica

Javier Rojas Segura
jrojass@uia.ac.cr
https://orcid.org/0000-0002-0488-4056
Escuela de Ingeniería Informática de la Universidad Internacional de las Américas, Costa Rica

Jorge Murillo Gamboa
jorgemurillo2011@gmail.com
ttps://orcid.org/0000-0001-5548-8283
Docente Investigador de la Escuela de Ingeniería Informática de la Universidad Internacional de las Américas, San José Costa Rica

Recibido: 29 de agosto del 2023 / Aceptado: 18 de octubre del 2023
doi: https://doi.org/10.26439/interfases2023.n018.6626

RESUMEN. Los niños son el segmento más vulnerable de esta sociedad ciberfísica, pudiendo ser fácilmente explotados por su bajo nivel de percepción del riesgo cibernético. Iniciar la educación y el desarrollo de habilidades digitales en edades tempranas incentiva a esta población a seguir en el futuro carreras profesionales como ciberseguridad, aportando de manera sostenible a cerrar la brecha de la fuerza laboral en este campo. Mediante un enfoque cualitativo, se realizó una revisión documental, una revisión de la literatura y una consulta a expertos académicos, para proponer un programa de alfabetización digital en edades tempranas. A manera de caso de estudio se presenta el Programa de Alfabetización Digital de la Universidad Internacional de las Américas de Costa Rica y las experiencias con el Taller de Ciberseguridad para Niños, dirigido hacia el desarrollo de habilidades digitales, el bienestar cibernético en edades tempranas y el interés de los niños en seguir nuevas carreras profesionales. Se propone reducir la brecha de la fuerza laboral en puestos sobre ciberseguridad a través de programas de formación en edades tempranas, que concienticen sobre los riesgos en seguridad

cibernética, su evolución, su impacto en la sociedad y destaquen su importancia en un mundo cada vez más dominado por la tecnología.

PALABRAS CLAVE: ciberseguridad / niñez / alfabetización / academia / cibernética

CYBERSECURITY AND DIGITAL SKILLS DEVELOPMENT: A PROPOSAL FOR DIGITAL LITERACY AT EARLY AGES

ABSTRACT. Children are the most vulnerable segment of this cyberphysical society and can be easily exploited due to their level of perception of cyber risk. Starting education and the development of digital skills at an early age encourages this population to pursue professional careers such as cybersecurity in the future and contribute in a sustainable way to closing the gap in the workforce. Using a qualitative approach, a documentary review, a literature review, and consultation with academic experts are carried out to propose a digital literacy program at an early age. As a case study, the Digital Literacy Program of the International University of the Americas of Costa Rica and the experiences with the Cybersecurity Workshop for Children are presented. Workshop aimed at the development of digital skills, cyber well-being at an early age and children's interest in following new professional careers. It aims to reduce the gap in the workforce in cybersecurity positions with training programs at an early age, raising awareness about cybersecurity risks, their evolution, their impact on society and highlighting their importance in a world increasingly driven by technology.

KEYWORDS: cybersecurity / childhood / literacy / academy / cybernetics

1. INTRODUCCIÓN

Ya hace más de una década, Zhuge (2010) proponía que los seres humanos vivirían y se desarrollarían en un nuevo mundo que él denominó "sociedad ciberfísica", la cual concierne no solo al ciberespacio y al espacio físico, sino también al espacio socioemocional y mental. Sin embargo, la vida cotidiana de las personas se vio afectada considerablemente por la propagación global del COVID-19, pandemia que trajo consigo una mayor dependencia a las plataformas en línea, y dio paso a una mayor vulnerabilidad en la seguridad. A esta situación, AlShabibi y Al-Suqri (2021) la denominaron "ciberpandemia".

Los niños debieron trasladar su escolarización al ciberespacio, incrementando el tiempo que pasaban *online*, lo cual es asociado a un incremento en el riesgo en ciberseguridad (Martínez-Pastor et al., 2019). Siddiqui y Zeeshan (2020) consideran que los niños son una presa fácil de muchas amenazas cibernéticas, debido a la falta de conciencia de tales amenazas. Las familias y los maestros pueden desempeñar un papel importante en lograr una mejor conciencia sobre las amenazas de las plataformas cibernéticas para los niños (Aldawood & Skinner, 2018). Por otro lado, Herkanaidu et al. (2021) indican que un área poco explorada de la educación para la concientización sobre seguridad en línea es el papel de la cultura y, específicamente, las diferencias culturales que pueden conducir a resultados de aprendizaje muy diferentes.

El uso de internet está generalizado en la vida cotidiana de los escolares, quienes empiezan a utilizarlo a una edad cada vez más temprana (Gómez et al., 2020). Martínez-Pastor et al. (2019) vinculan esto a la necesidad que sienten de conocer de forma casi inmediata las novedades de su círculo *online*. El uso de las Tecnologías de Información y Comunicaciones (TIC) y del internet sin duda beneficia en gran medida a niños y jóvenes, pero a la vez genera desafíos en relación a la seguridad cibernética (Waldock et al., 2022), especialmente en momentos en que la brecha en la fuerza laboral de seguridad cibernética aumenta en América del Norte, Europa y Latinoamérica, donde se menciona que será necesario que todas las partes del ecosistema trabajen juntas para proporcionar más recursos de preparación técnica en todos los niveles y roles del sector para cerrar la brecha de la fuerza laboral y garantizar la preparación cibernética (ISC2, 2023). Además de a la industria, esta brecha también afecta a la academia en su objetivo de atraer investigadores y profesores con conocimiento teórico y práctico (OEA & CISCO, 2023).

Acorde a Gómez et al. (2020), uno de los problemas es que una parte importante de los escolares no ha recibido ningún tipo de formación o información previa sobre ciberseguridad. Para Astorga-Aguilar et al. (2019), el que los menores de edad no tengan una adecuada educación en seguridad cibernética les hace más vulnerables. Los niños deben poder evaluar la información y tomar decisiones objetivas sobre la credibilidad del contenido (Sadaghiani-Tabrizi, 2018). Sin embargo, la sensibilización sobre la seguridad en línea sigue siendo un ámbito poco investigado (Herkanaidu et al., 2021).

El contenido considerado para la educación en seguridad cibernética varía mucho entre las naciones; por lo tanto, es inconsistente y está lleno de vacíos (Sağlam et al., 2023). Por ello, Herkanaidu et al. (2021) consideran que en los programas de concientización se deben tomar en cuenta los contextos culturales y nacionales. Esto nos conduce a las preguntas: ¿Qué ha hecho Costa Rica por la protección de la niñez en línea y la concientización sobre los riesgos de seguridad cibernética? ¿Cómo puede ayudar la academia en la culturización y sensibilización de la niñez en temas de ciberseguridad?

Dado que las alianzas público-privadas-académicas juegan un papel importante en un plan de acción para la educación en ciberseguridad (OEA & AWS, 2020), y siguiendo la recomendación de la OEA y CISCO (2023) de acuerdo a la que los proveedores de educación terciaria deben garantizar que la ciberseguridad se considere una opción de estudio deseable para atraer a los mejores y más motivados estudiantes, el objetivo de este estudio es proponer un programa de alfabetización digital en edades tempranas. Esto se haría mediante la capacitación de temáticas relacionadas con seguridad informática, con el objetivo de reducir la brecha de la fuerza laboral en ciberseguridad.

2. METODOLOGÍA

Con el fin de concientizar y sensibilizar en ciberseguridad en las edades tempranas, se concibió el programa de alfabetización digital empleando un enfoque cualitativo y siguiendo las etapas que se describen a continuación:

2.1 Revisión documental (desk review)

Para investigar qué ha hecho Costa Rica por la protección de la niñez en línea y la concientización sobre los riesgos de seguridad cibernética, siguiendo a Waldock et al. (2022), se realizó una revisión documental. Se consultaron agencias gubernamentales tales como el MICITT[1] y la Asamblea Legislativa, así como agencias no gubernamentales, como la ONU y sus dependencias, la OEA, entre otras.

2.2 Revisión de literatura

La currícula de ciberseguridad sugerida por la Association for Computing Machinery (ACM, por su sigla en inglés) y la organización Computer Society del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE-CS) incluye un plan integral de ciberseguridad y el desarrollo de habilidades en los estudiantes, para prepararlos desde una edad temprana a enfrentar los retos de la ciberseguridad, para fomentar su interés en carreras profesionales en este campo y para contribuir a cerrar la brecha de la fuerza laboral en ciberseguridad (ACM & IEEE-CS, 2017).

1 Ministerio de Ciencia, Tecnología y Telecomunicaciones. Gobierno de Costa Rica.

Para responder a la pregunta de investigación "¿Cómo puede ayudar la academia en la culturización y sensibilización de la niñez en temas de ciberseguridad?", siguiendo a Bustillos Ortega y Rojas Segura (2022), se realizó una revisión de literatura consultando diversas bases de datos tales como Google Académica, ProQuest Digital Dissertation and Theses, IEEE Xplore, entre otros. Además, se examinaron diversos trabajos de investigación y tesis, así como buenas prácticas y tendencias en ciberseguridad para la niñez en línea, utilizando el término en inglés *child online protection*.

2.3 Consulta a expertos

Siguiendo lo propuesto por Sağlam et al. (2023), se utilizó el asesoramiento de expertos para valorar la información obtenida de los procesos metodológicos anteriores. Ello permitió proponer un programa de alfabetización digital en edades tempranas, en el cual las perspectivas de los estudiantes, los padres y las autoridades de seguridad cibernética están representadas, así como la consideración de la cultura local, según recomendación de Herkanaidu et al. (2021).

2.4 Taller sobre ciberseguridad para niños

Se llevó a cabo un taller denominado *CyberKids*, durante cinco sesiones de tres horas, cada una proporcionando lecciones valiosas sobre cómo educar y concienciar a la juventud en torno a la ciberseguridad, destacando la necesidad de abordar este desafío a nivel global (ver apartado 3.5 para más detalles sobre el taller llevado a cabo). El enfoque permitió abrir un espacio para brindar una educación sólida y bien fundamentada hacia los futuros profesionales en ciberseguridad, preparando a los participantes para hacerles frente a los desafíos de la sociedad ciberfísica y contribuyendo de manera significativa a la seguridad y bienestar en el mundo digital.

3. RESULTADOS

Aun cuando el Fondo de las Naciones Unidas para la Infancia - UNICEF (2020) ha propuesto que los formuladores de política pública, las organizaciones que trabajan con niños y jóvenes o cualquier otro ente interesado en crear oportunidades para este grupo promueva y apoye la alfabetización digital y el desarrollo de habilidades, la educación en seguridad en línea para niños y jóvenes aún necesita fortalecerse (Waldock et al., 2022).

3.1 Revisión de la literatura

A lo largo del tiempo, la tecnología ha generado cambios en nuestra sociedad, y, a pesar de las controversias que el tema suscita, ha forjado la evolución de la raza humana (Díaz, 2022). Las TIC, especialmente el internet, han reconfigurado nuestras vidas. Actualmente formamos parte de una sociedad interactiva, vivimos en hogares con múltiples pantallas y las opciones de ocio que nos envuelven son mayoritariamente digitales (Gómez et

al., 2020). Nuestra sociedad continúa evolucionando hacia una era digital, debido al uso extensivo de las TICs y sus mecanismos de interconexión, tales como redes sociales, almacenamiento en la nube, el internet de las cosas (Robles-Gómez et al., 2020), y es aplicable a todas las áreas de nuestra vida: trabajo, educación, salud, ocio y responsabilidades ciudadanas.

La pandemia del COVID-19 demostró mundialmente que los internautas no están bien preparados para hacer frente a los ciberataques (AlShabibi & Al-Suqri, 2021). El nivel actual de conciencia de ciberseguridad de los ciudadanos no es el deseado y se deben tomar medidas para mejorarlo (Stavrou, 2020). Esa conciencia de ciberseguridad significa comprender las posibles amenazas y tomar las medidas adecuadas para contrarrestarlas (Vanderhoven et al., 2014). Por el contrario, según indican AlShabibi y Al-Suqri (2021), la falta de esta conciencia aumenta drásticamente las violaciones de datos y los ataques cibernéticos. Mejorar la concientización pública en ciberseguridad podría elevar el nivel general de inmunidad a los ciberataques (Díaz, 2021).

La Unión Internacional de Telecomunicaciones (ITU, 2023), órgano especializado en telecomunicaciones de las Naciones Unidas, nos dice que los niños y jóvenes son cada vez más activos en línea: el 71 % de ellos, a nivel mundial, utiliza el internet. Sus vidas en línea y fuera de línea están inherentemente interrelacionadas y ambas se combinan para afectar sus resultados de bienestar y oportunidades de vida. Esto concuerda con lo expuesto por Zhuge (2010), quien indica que, con el rápido desarrollo de las TIC, el ciberespacio está conectando el espacio físico, el espacio social y el espacio mental para formar un nuevo mundo denominado la sociedad ciberfísica.

En esta sociedad ciberfísica, los niños son el segmento más vulnerable y pueden ser fácilmente explotados debido a su bajo nivel de discernimiento (AlShabibi & Al-Suqri, 2021). Los investigadores han observado que los niños se han visto impulsados a realizar compras indebidas, incluso aceptan mensajes emergentes no deseados e interactúan con personas extrañas en el ciberespacio (Mıhcı Türker & Kılıç Çakmak, 2019), colocando en riesgo no solamente su propio bienestar, sino también la seguridad de los datos almacenados en esos dispositivos y en la red. La amenaza del robo de datos personales a través de páginas web falsas se denomina *phishing* y, según Moncada Vargas (2020), es uno de los mayores riesgos en la actualidad. Por ese medio se han materializado la mayor cantidad de robos y estafas cibernéticas en los últimos años. Cuando un archivo malicioso implantado por el atacante es activado, nos dicen Bustillos Ortega y Rojas Segura (2022), este abre un sitio de *phishing* en el navegador web. Haciéndose pasar por una red social o bien el sitio de uno de los juegos preferidos por el usuario, solicita credenciales u otra información confidencial, que luego es enviada al atacante. Lamentablemente, en la mayoría de los casos, no solo los niños, sino también sus padres, desconocen estas amenazas de seguridad (Siddiqui & Zeeshan, 2020).

Los niños no pueden aumentar su conciencia cibernética solos, y los padres no son conscientes de estos riesgos o los subestiman, por lo que una de las soluciones

inmediatas que se pueden tomar para protegerlos es a través de programas efectivos de capacitación y educación (Aldawood & Skinner, 2018; AlShabibi & Al-Suqri, 2021), siendo esencial la cooperación entre la academia y los gobiernos, para promover la ciberseguridad (Bustillos Ortega, 2023).

Internet está totalmente integrado en la vida de los infantes y preadolescentes, quienes adquieren habilidades técnicas con bastante facilidad, pero carecen de habilidades digitales suficientes para navegar seguros en la red (Gómez et al., 2020). La UNICEF (2020) propone que las organizaciones que trabajan con niños y jóvenes fomenten y apoyen la alfabetización digital y el desarrollo de habilidades digitales. Por su parte, Venter et al. (2019) enfatizan la necesidad de tratar la ciberseguridad como una habilidad fundamental, junto con otras habilidades básicas en todo el sistema educativo. En la misma línea, AlShabibi y Al-Suqri (2021) concluyen que los programas integrales de concientización sobre ciberseguridad para niños pueden reducir significativamente la propagación y garantizar la seguridad de sus datos.

Por su parte Waldock et al. (2022) nos muestran otra ventaja de iniciar la educación cibernética en edades tempranas, ya que una exposición anticipada influiría a más niños y jóvenes a considerar una carrera profesional en ciberseguridad, ayudando a cerrar la brecha. Según el Information Security Consortium (ISC2, 2023) o, como también se le conoce, el Consorcio Internacional de Certificación de Seguridad del Sistema de Información, la brecha de la fuerza laboral de ciberseguridad es la cantidad de profesionales adicionales que las organizaciones necesitan para defender adecuadamente sus activos críticos. Según las estimaciones de su estudio realizado entre 3790 miembros de la organización, con sedes en Europa, las Américas y la región Asia Pacífico, para el 2021 había 4,19 millones de profesionales de ciberseguridad en todo el mundo (es decir, 20 % más de profesionales que en 2020). Aun cuando la brecha global disminuyó en 12,8 %, pasando de 3,12 millones en 2020 a 2,72 millones en 2021, en América del Norte, Europa y LATAM, la brecha está creciendo.

Después de un extenso proceso de dos años, un grupo de trabajo conjunto liderado por la Association for Computing Machinery (ACM) y el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) en su organización Computer Society (IEEE-CS) publicaron un primer conjunto de recomendaciones curriculares globales en educación en seguridad cibernética. Este nuevo conjunto de pautas, denominado *Cybersecurity Education Curriculum* (CSEC 2017) está diseñado para ser el principal recurso para elaborar contenidos curriculares integrales sobre seguridad cibernética en el nivel postsecundario y universitario. Más de 320 asesores e investigadores de 35 países diferentes contribuyeron a la publicación del CSEC 2017 (Ormond, 2018; ACM, 2017).

En la publicación mencionada anteriormente, CSEC 2017, se señala que el mundo enfrenta una escasez actual y creciente de mano de obra calificada en profesionales de ciberseguridad. Las fuentes gubernamentales y no gubernamentales proyectan casi 1,8

millones de puestos relacionados con la ciberseguridad sin cubrir para el año 2022, con una demanda de mano de obra aguda, inmediata y creciente. Con el fin de desarrollar el talento requerido, los departamentos académicos de todo el espectro de las disciplinas en informática, están lanzando iniciativas para elaborar nuevos contenidos o incluir cursos de ciberseguridad: ya sea desarrollando nuevos programas completos, definiendo nuevos temas dentro de las carreras, o aumentando el contenido de los cursos existentes. Estas instituciones necesitan orientación en su plan curricular, para que su formulación se base en una visión integral del campo de la ciberseguridad, considere las demandas específicas de la disciplina, y la relación entre el currículo y los marcos de trabajo en seguridad cibernética (ACM, 2017).

La situación sigue siendo crítica, ya que la demanda global de profesionales de ciberseguridad continúa superando la oferta. No solo la escasez de talento humano genera riesgos en las organizaciones, sino también la escasez de habilidades en la fuerza laboral (OEA & CISCO, 2023). Estas habilidades son la combinación de destrezas, conocimientos y experiencia que permiten a un individuo completar bien una tarea dentro de un rol de ciberseguridad en una organización (Stein et al., 2017).

Concientizar y sensibilizar a los estudiantes a temprana edad sobre los riesgos que enfrentan en línea es importante, pero también lo es ofrecerles la oportunidad de aprender sobre ciberseguridad a un nivel más profundo, permitiéndoles tener habilidades cibernéticas de por vida. Por ello, las entidades del sector público junto con la academia deben identificar y compartir prácticas efectivas para promover la conciencia de los niños y jóvenes y el descubrimiento de la carrera de ciberseguridad (OEA & CISCO, 2023).

Adicionalmente, fomentando su interés en carreras profesionales en este campo y contribuyendo a cerrar la brecha de la fuerza laboral en ciberseguridad con una educación sólida y bien fundamentada, los futuros profesionales en ciberseguridad estarán preparados para hacer frente a los desafíos de la sociedad ciberfísica y contribuir de manera significativa a la seguridad y bienestar en el mundo digital.

3.2 Costa Rica y la protección de la infancia en línea

Como Estado miembro de la Organización de las Naciones Unidas (ONU), en noviembre de 1989 Costa Rica se adhirió a la Convención sobre los Derechos del Niño, considerada la primera ley internacional sobre los derechos de los niños y las niñas (UNICEF, 2006). Posteriormente se aprobó en la Asamblea Legislativa la Ley 7739, Código de la Niñez y la Adolescencia (1998), la cual da derecho a los niños de obtener información, sin importar su fuente o modo de expresión.

Patrocinado por Costa Rica, en noviembre de 2008 y como un esfuerzo de múltiples partes interesadas en el marco de la Agenda Mundial de Ciberseguridad, la Unión Internacional de Telecomunicaciones de la ONU puso en marcha la Iniciativa para la

Protección de la Infancia en Línea (COP por su sigla en inglés). La iniciativa reunió a socios de todos los sectores de la comunidad mundial para crear una experiencia en línea segura y empoderadora para los niños de todo el mundo (COP, 2008). En el decreto ejecutivo que hizo posible la creación de la Comisión Nacional de Seguridad en Línea (2010) se definió que uno de sus objetivos era crear proyectos dirigidos a la sensibilización y formación de niños y adolescentes.

Posteriormente, a nivel nacional y en un mismo año, se aprobaron dos legislaciones importantes para la protección de la niñez: la Ley de Protección de Datos (2011) y la Ley de Protección de la Niñez y la Adolescencia frente al Contenido Nocivo de Internet y otros Medios Electrónicos (2011). Al año siguiente, mediante el Decreto Ejecutivo 37052 del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), en 2012 se creó un Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR), uno de cuyos objetivos fue crear proyectos dirigidos a la sensibilización y formación de niños, adolescentes y sus familias en el uso adecuado de internet y las tecnologías digitales.

El MICITT (2017), bajo una visión holística con atención multisectorial, instauró la Estrategia Nacional de Ciberseguridad de Costa Rica. Colocó a las personas como el eje central, procuró que cualquier acción tuviera como prioridad la atención y mitigación de los riesgos que impactan a población vulnerable, como la niñez. Con esta estrategia se buscó promover el uso de las TIC como instrumento para el mejoramiento de la calidad de vida de manera segura, generando conciencia por medio de la educación desde edades tempranas sobre los efectos del uso responsable de estas tecnologías. Cuatro años después, en el año 2021, el MICITT, con el apoyo de la Organización de Estados Americanos (OEA) realizó una revisión de la Estrategia Nacional de Ciberseguridad, a fin de evaluar su nivel de implementación. Uno de sus hallazgos fue que las campañas de concientización dirigidas a la población en condición vulnerable fueron limitadas, habiendo sido el Centro de Respuesta de Incidentes de Seguridad Informática el único que impulsó capacitaciones de ciberseguridad para menores. En esta revisión, el MICITT recomendó una campaña nacional de mensajería centralizada dirigida a la niñez y a cada uno de estos grupos vulnerables (niños y jóvenes con problemas de salud mental, personas sin hogar y ancianos entre otros). Para visualizar estos hechos en una línea de tiempo, véase la Tabla 1.

Al momento de elaborar este artículo, un proyecto de ley de ciberseguridad se encuentra en discusión en la Asamblea Legislativa de Costa Rica (2022). Allí se indica que el estado de madurez en cuanto a normativas sobre ciberseguridad, a nivel país, es apenas formativo, ubicándolo en una fase incipiente, con una madurez embrionaria. Además, se tiene un balance negativo de personal capacitado en ciberseguridad, según el cual el 55 % de las instituciones del Estado no cuentan con personal dedicado a esta labor.

Tabla 1

Costa Rica y la protección de la infancia en línea

Año	Hecho relevante en Costa Rica	Tipo
1990	Convención sobre los Derechos del Niño	Convención
1993	WWW World Wide Web, código fuente liberado y se abre al público	WWW liberado
1998	Código de la Niñez y la Adolescencia. Ley 7739	Ley 7739
2001	Convenio de Budapest. Creado por Consejo de Europa sobre Ciberdelincuencia, aprobado por la Unión Europea y muchos países	Convenio
2005	Ley de Certificados, Firmas Digitales y Documentos Electrónicos. Ley 8454	Ley 8454
2008	Rectoría del MICITT, creación de iniciativa Children Online Protection (COP) con el patrocinio de Costa Rica	Ley 8454
2010	Comisión Nacional de Seguridad en Línea y Adhesión al COP	
2011	Legislación importante: Ley de Protección de la Niñez y la Adolescencia frente al Contenido Nocivo de Internet y otros Medios Electrónicos, Ley 7739	Ley 7739
2012	Ministerio Ciencia, Tecnología y Telecomunicaciones MICITT, Decreto Ejecutivo 37052. Centro de Respuesta de Incidentes de Seguridad Informática CSIRT-CR	Decreto 37052
2017	Estrategia Nacional de Ciberseguridad. Adhesión al Convenio de Budapest mediante Ley 9452	Ley 9452
2021	Revisión Estrategia Nacional de Ciberseguridad (2017). MICITT – Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (OEA)	Programa OEA
2022	Ciberataques fuertes al Estado. Proyecto de Ley de Ciberseguridad Abril 2022 – Grupo Cibercriminal "Conti" atacó fuertemente Octubre 2022 – Se presenta el Proyecto de Ley de Ciberseguridad	Proyecto de Ley

Fuente: Tomado del proyecto de Ley de Ciberseguridad de Costa Rica, (MICITT, 2017).

3.3 Desde la academia

En un caso similar al de Costa Rica (MICITT, 2017, 2021), la estrategia de seguridad cibernética de Singapur se definió por primera vez en 2016 y se actualizó en 2021. Waldock et al. (2022) nos indican que Singapur, en su nueva estrategia del 2021, abordó explícitamente la educación en ciberseguridad como un proceso robusto de atracción de talentos cibernéticos, fomentando el desarrollo, desde la niñez y adolescencia, de interés y habilidades cibernéticas, para alentar a más jóvenes a seguir una carrera en ciberseguridad, así como el apoyo de la academia para guiar a los jóvenes en su formación.

La OEA y Twitter (2021) consideraron la alfabetización digital como un proceso dinámico de experiencias vividas, que se completa cuando incluye conocimientos, habilidades y actitudes; cuando abarca el acceso, la evaluación, el uso, la producción y la comunicación de información, de contenido mediático y tecnológico. Además, para fortalecer las habilidades esenciales, lograr la alfabetización digital, combatir la desinformación y otros fenómenos que atentan contra una navegación digital segura, recomiendan a la academia expandir la investigación empírica.

Para la OEA y AWS (2020), por su labor en investigación y extensión, es esencial la participación de universidades, centros de investigación y otras instituciones académicas en la educación de la próxima generación de la fuerza laboral en ciberseguridad. Con el fin de concientizar y sensibilizar en ciberseguridad durante la edad temprana, las entidades del sector público relacionadas, junto con la academia, deben identificar y compartir prácticas efectivas para promover la conciencia de los niños y jóvenes y el descubrimiento de la carrera de ciberseguridad (OEA & CISCO, 2023).

3.4 Programa de alfabetización digital

El Programa de Alfabetización Digital de la Escuela de Ingeniería Informática se lanzó en 2016, con el propósito de ofrecer a la sociedad costarricense diversas actividades de acción social desde las carreras de la Escuela. Ha sido un componente integral de la acción social de la institución, brindando a jóvenes y adultos costarricenses la oportunidad de adquirir habilidades digitales cruciales para su desarrollo social y económico. A pesar de los desafíos presentados por la virtualidad, el programa ha continuado prosperando, ofreciendo capacitación gratuita en tres categorías principales: *Digital kids*, *Digital youth* y *Digital adults*.

Uno de los pilares fundamentales del programa es *Digital kids*, diseñado específicamente para la niñez costarricense. Se enfoca en inspirar a los niños a explorar y comprender el mundo de la tecnología de una manera lúdica y educativa. Los talleres y actividades promueven la creatividad, la resolución de problemas y la alfabetización digital en edades tempranas.

Al cultivar el interés de los niños en la alfabetización digital, el programa está sentando las bases para una futura generación de innovadores y líderes en tecnología, incluyendo la formación en temáticas relacionadas con seguridad informática, para alentar a más jóvenes a seguir una carrera en ciberseguridad y ayudar a reducir la brecha de la fuerza laboral en esta materia.

El programa se subdivide en siete áreas temáticas: conciencia tecnológica, conciencia procedimental, protección de datos, identidad en línea, conciencia socio/cultural, sensibilización comercial y redes sociales. Estas temáticas fueron desarrolladas durante cinco sesiones, según se muestra en la Tabla 2.

Tabla 2

Programa de alfabetización en ciberseguridad en edades tempranas

Sesión	Área temática	Contenido
1	Conciencia tecnológica	Qué es y para que se utiliza internet
		Tipos de ataques y amenazas
		Salvaguardas contra ataques
	Conciencia procedimental	Administración de contraseñas
		Actualizaciones de software y antivirus
		Evitar enlaces desconocidos y phishing
		Reportar contenido y actividades ilegales
2	Protección de datos	Concientización de la privacidad
		Qué son datos y datos personales
		Valor comercial de los datos personales, piratería
		Consecuencia de compartir los datos
	Identidad en línea	Comprender cómo se construye la identidad, la imagen, la representación y la reputación en línea
		Cómo protegerse uno mismo y la imagen propia
		Comprender el significado de robo de identidad
		Reputación e integración online/offline
3	Conciencia socio cultural	Comprensión del comportamiento ético en línea
		Prevención de la intimidación, racismo y discurso de odio en línea
		Evaluación crítica de la información falsa
		Denuncia de actos delictivos
		Conocer qué es y cómo evitar el contenido ilegal
		Peligro de extraños
		Fomentar el uso responsable de las tecnologías
4	Sensibilización comercial	Comprender el carácter comercial de internet
		Sensibilización y gestión responsable de costos, compras y facturación en línea
		Conocimiento del fraude
		Conciencia del potencial de adicción (juegos, apuestas, entre otros)
	Redes sociales	Cuáles son las redes sociales
		Cómo usarlas responsablemente
		Riesgos y beneficios
		Socialización offline

(continúa)

(continuación)

Sesión	Área temática	Contenido
5	Presentación de proyectos	El niño desarrollará una propuesta creativa (video, caricaturas, cuentos, entre otros), donde se visualice el uso de internet sin limitaciones.
	Encuesta	Consulta a los niños sobre el tipo de contenido sobre el que desean ser capacitados, para ser implementado en futuras iteraciones.

Tanto la Universidad, la Dirección de la Escuela de Ingeniería Informática, así como estudiantes y docentes participan en estas actividades y, de esta forma, generan un cambio en nuestra sociedad. Para conocer algunos proyectos de este programa de alfabetización, véase el Anexo 1.

3.5 Taller *CiberKids*

El taller *CiberKids* se propuso como objetivo principal la educación y concienciación de un grupo demográfico crítico (niños y adolescentes con edades comprendidas entre 10 y 15 años), en relación con los riesgos y desafíos que conlleva el uso del ciberespacio. A lo largo de cinco sesiones de tres horas cada una, cada semana, y con el apoyo de sus padres, se buscó prepararlos para un manejo responsable y seguro de las tecnologías de la información, promoviendo así la ciberseguridad, la privacidad en línea y la promoción de relaciones interpersonales virtuales saludables y respetuosas. El contenido del taller y sus objetivos se muestran en la Tabla 3.

Tabla 3

Taller de CiberKids *(alfabetización en ciberseguridad en edades tempranas)*

Sesión		Objetivos
1.	Introducción al internet y la ciberseguridad	Conocer el uso del internet, identificar logotipos en línea y aprender medidas de ciberseguridad en redes sociales, relaciones en línea y juegos en línea.
2.	Ciberacoso y contenidos inadecuados	Sensibilizar a los participantes sobre el ciberacoso y contenidos inadecuados en internet, así como enseñarles cómo actuar ante estos problemas y la importancia de la privacidad.
3.	Relaciones en línea y uso excesivo de internet	Fomentar una comunicación respetuosa, reflexionar sobre el tiempo en línea y promover el equilibrio entre actividades en línea y fuera de línea.
4.	Comunicación online y seguridad en dispositivos	Enseñar a configurar la seguridad en los dispositivos personales y del hogar, usar contraseñas seguras, descargar aplicaciones de manera segura y utilizar herramientas como Kiddle, que busca evitar o minimizar la vulnerabilidad en línea.

(continúa)

(continuación)

Sesión	Objetivos
5. Presentación de proyectos	Los participantes presentarán proyectos basados en lo aprendido en las sesiones anteriores, demostrando su comprensión de la ciberseguridad y cómo aplicarla en su vida en línea.

En síntesis, el taller *CyberKids*, una vez aplicado, se ha revelado como una iniciativa educativa valiosa y efectiva para empoderar a la niñez y juventud digital, ofreciendo herramientas necesarias para navegar de manera segura y responsable en el entorno virtual, preparándose adecuadamente para enfrentar los desafíos inherentes y contribuyendo así a la formación de ciudadanos digitales responsables en la era de la información. De forma proactiva, la academia va asumiendo su responsabilidad de ser un actor fundamental en la sociedad.

4. DISCUSIÓN DE LOS RESULTADOS. CÓMO ALFABETIZAR

Con la intención de acercar a los jóvenes desde edades tempranas a las universidades, para fomentar el deleite por carreras con formación en ciberseguridad, este programa de alfabetización digital se diseñó para ser impartido en los laboratorios de ciberseguridad del campus universitario, por docentes universitarios expertos en el tema y adecuados para ser impartido a niños y adolescentes entre los 11 y los 14 años.

En el caso específico del taller *CiberKids*, las actividades formativas utilizan recursos tales como juegos, dibujos animados, vídeos, simulación de casos reales en entornos virtuales, entre otros.

Al elaborar el contenido de los distintos cursos y talleres, los docentes buscaron mejorar la imaginación moral[2] (Hyry-Beihammer, 2022) en línea, a través de historias y narraciones, en vez de seguir enfoques tradicionales. Se tomaron en cuenta los factores culturales que afectaron a la población, hacia un comportamiento seguro en línea, utilizando específicamente áreas STEM[3] apostando por la enseñanza conjunta de las ciencias, las matemáticas y la tecnología, apoyadas por la ingeniería (Aneas et al., 2023).

Para proponer en Costa Rica un programa de alfabetización digital en edades tempranas con la visión de reducir la brecha de la fuerza laboral en ciberseguridad, tal como lo recomiendan Waldock et al. (2022), la OEA y CISCO (2023), se debe hacer una exposición anticipada que promueva la concientización de niños, adolescentes y jóvenes al descubrimiento de carreras profesionales en ciberseguridad.

2 La imaginación moral se refiere a la capacidad de considerar una situación desde la distancia y comprender diferentes perspectivas a través de la imaginación.

3 Ciencia, tecnología, ingeniería y matemáticas por su sigla en inglés

La concientización en ciberseguridad tiene un importante papel en la reducción del impacto de los ciberataques contra los niños (AlShabibi & Al-Suqri, 2021) y Costa Rica ha demostrado sus acciones en este campo (ver Tabla 1).

A nivel nacional, desde una etapa incipiente en el uso del ciberespacio, el gobierno de Costa Rica aprobó el Código de la Niñez y la Adolescencia (1998) donde se garantiza a los menores de edad el derecho a obtener información sin importar su fuente ni modo de expresión. Ante la comunidad internacional, esta decisión sirvió de base para promover la puesta en marcha de la iniciativa COP (2008). Posteriormente se presentó ante la Asamblea General de las Naciones Unidas (ONU, 2013) como mensaje de los jóvenes al mundo, quienes solicitaban a las autoridades mundiales, entre varios puntos relevantes, la preparación técnica para la protección en línea. Siendo que el éxito económico de una nación depende de un acceso sin trabas al conocimiento que las TIC pueden contribuir haciéndolas llegar a todos. La difusión de información entre los niños y jóvenes puede fomentar directamente la autonomía y la innovación a escala mundial (ITU, 2013).

Los delitos cibernéticos se incrementaron durante la transformación digital de la educación, a partir del momento en que se facilitó a los niños acceder al ciberespacio incondicionalmente (AlShabibi & Al-Suqri, 2021), abriendo más espacio a los ciberdelincuentes para manipular a los niños (Robles-Gómez et al., 2020).

Existe una necesidad urgente de capacitar a los estudiantes en el tema de la ciberseguridad, para que adquieran habilidades prácticas (Robles-Gómez et al., 2020). La OEA y CISCO (2023), que indican que la academia debe identificar y compartir prácticas efectivas para promover la conciencia de los niños y jóvenes. Para Siddiqui y Zeeshan (2020) esta falta de conciencia es la principal amenaza que los lleva a ser presa fácil. Desde otra perspectiva, al ser la academia el actor más representativo y que genera impacto en la oferta laboral (OEA & CISCO, 2023), es el ente indicado para acompañar a los futuros profesionales en su viaje de seguridad cibernética desde edades tempranas, colaborando así a reducir la brecha existente en la fuerza laboral en ciberseguridad.

Aun cuando en la literatura se encontraron varias investigaciones sobre la protección de la niñez en línea, mayoritariamente se dirigían a la educación primaria y secundaria en sus respectivas escuelas, como es el caso de Gómez et al. (2020), o bien refiriéndose a la educación preuniversitaria (Waldock et al., 2022), pero con mayor énfasis en la capacitación a los educadores de escuelas. Esto es considerado una limitación en la investigación. Sin embargo, para futuras investigaciones sobre ciberseguridad, tal como lo consideran la OEA y CISCO (2023) la academia tendrá dificultades para atraer investigadores con conocimiento, experiencia práctica y antecedentes en investigación, ya que el sector industrial absorberá a estos profesionales.

Es fundamental crear un ciberespacio más seguro en Latinoamérica y el Caribe (Cudjoe et al., 2022), ya que los jóvenes han demostrado que las TIC son la fuerza motriz para alcanzar los objetivos de desarrollo sostenible (Touré, 2013).

5. CONCLUSIONES

En un mundo cada vez más interconectado y digitalizado, la creación de un ciberespacio seguro se ha convertido en una prioridad ineludible para la sociedad moderna. El taller *CyberKids* proporciona lecciones valiosas sobre cómo educar y concientizar a la juventud en torno a la ciberseguridad, destacando la necesidad de abordar este desafío a nivel global. Esta iniciativa también abre una vía alternativa desde la academia para cerrar la brecha de la fuerza laboral en ciberseguridad, al combinar la educación temprana en ciberseguridad y el desarrollo de habilidades digitales en edades tempranas.

Además del enfoque más tradicional de una estrategia educativa de arriba hacia abajo que se basa en consejos generados por la industria, gobierno y academia, este programa contó con la perspectiva de la niñez; es decir, tuvo un enfoque de abajo hacia arriba. Se aplicaron encuestas a los niños participantes y se les consultó en qué tipo de contenido requerían ser capacitados. Se previó incluso, para futuras iteraciones de este programa, aplicar a los estudiantes una encuesta en la última sesión sobre las necesidades desde su punto de vista, con el objetivo de utilizarlo como insumo para mantener actualizado el currículo del programa.

Algunos de los temas a considerar en futuros trabajos de investigación subrayan la importancia de educar y fomentar la creación de un ciberespacio más seguro donde se incorporen temas como: la protección de la infancia, prevenir el cibercrimen, proteger la infraestructura crítica (seguridad nacional), preservación de la privacidad, fomento de la confianza digital, educación y empoderamiento, y cierre de la brecha de la fuerza laboral en ciberseguridad.

REFERENCIAS

ACM, IEEE-CS (2017). Cybersecurity Education Curriculum 2017. A Report in the Computing Curricula Series. Joint Task Force on Cybersecurity Education. Version 1.0 Report. 31 December 2017. Association for Computing Machinery ACM & Institute of Electrical and Electronics Engineer IEEE Computer Society publication. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Aldawood, H., & Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), 62-68. https://doi.org/10.1109/TALE.2018.8615162

AlShabibi, A., & Al-Suqri, M. (2021). Cybersecurity Awareness and Its Impact on Protecting Children in Cyberspace. 22nd International Arab Conference on Information Technology (ACIT), 1-6. https://doi.org/10.1109/ACIT53391.2021.9677117

Aneas, A. B., Domingo, J. A. M., Ortiz, B. B., & Navas-Parejo, M. R. (2023). Análisis de la metodología STEM en el aula de educación infantil. Una revisión sistemática. *Hachetetepé. Revista Científica de Educación y Comunicación*, 26. https://doi.org/10.25267/Hachetetepe.2023.i26.1101

Astorga-Aguilar, C., Schmidt-Fonseca, I., Astorga-Aguilar, C., & Schmidt-Fonseca, I. (2019). Peligros de las redes sociales: cómo educar a nuestros hijos e hijas en ciberseguridad. *Revista Electrónica Educare*, *23*(3), 339-362. https://doi.org/10.15359/ree.23-3.17

Bustillos Ortega, O., & Rojas Segura, J. (2022). Protocolo básico de ciberseguridad para pymes. *Interfases*, 016. https://doi.org/10.26439/interfases2022.n016.6021

Bustillos Ortega, O., & Rojas Segura, J. (2023). Cómo promueven los estados la ciberseguridad de las PYMEs. *Interfases*, 016.

Child Online Protection. (2008). ITU. https://www.itu.int:443/en/cop/Pages/about_cop.aspx

Cudjoe, B., Lagakali, C., Name, V., Lykoura, G., & Noij, A. (2022, octubre 31). *Iniciativas regionales sobre concienciación sobre ciberseguridad – Foro mundial sobre ciberconocimientos especializados*. GFCE. https://thegfce.org/regional-initiatives-on-cyber-security-awareness/

Díaz, R. M. (2021). Estado de la ciberseguridad en la logística de América Latina y el Caribe (serie Desarrollo Productivo, 228). *Comisión Económica para América Latina y el Caribe (CEPAL)*. https://repositorio.cepal.org/handle/11362/47240

Díaz, R. M. (2022). Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe. *Comisión Económica para América Latina y el Caribe (CEPAL)*. https://repositorio.cepal.org/handle/11362/48065

Gómez, R. G., Llorente, P. A., Morales, M. T. V., & Hernández, I. L. (2020). Seguridad y protección digital de la infancia: retos de la escuela del siglo xxi. *Educar*, *56*(1). https://doi.org/10.5565/rev/educar.1113

Herkanaidu, R., Furnell, S. M., & Papadaki, M. (2021). Towards a cross-cultural education framework for online safety awareness. *Information & Computer Security*, *29*(4), 664-679. https://doi.org/10.1108/ICS-11-2020-0183

Hyry-Beihammer, E. K., Lassila, E. T., Estola, E., & Uitto, M. (2022). Moral imagination in student teachers' written stories on an ethical dilemma. *European Journal of Teacher Education*, 45(3). https://doi.org/10.1080/02619768.2020.1860013

ISC2. (2023, 20 de noviembre). *Cybersecurity on The Hill: The Future of the Cybersecurity Workforce*. International Information System Security Certification Consortium. https://www.isc2.org/Insights/2023/11/Cybersecurity-on-The-Hill-The-Future-of-the-Cybersecurity-Workforce?queryID=bf6b78c06c85f7eca1d1d923d9baa0c0

ITU. (2013). *BYND2015 Global Youth Declaration*. International Telecomunication Union. https://www.itu.int:443/en/bynd2015/Pages/global-youth-declaration.aspx

ITU. (2023). *POP: Protection through online participation*. https://www.itu.int:443/en/ITU-D/Cybersecurity/Pages/COP/POP.aspx

Ley 7739. Código de la Niñez y la Adolescencia, Asamblea Legislativa de Costa Rica (1998). http://www.pgrweb.go.cr/scij/busqueda/normativa/normas/nrm_texto_completo.aspx?param2=1&nValor1=1&nValor2=43077&lResultado=4&strSelect=sel

Ley 8968. Ley de Protección de la persona frente al tratamiento de sus datos personales. Asamblea Legislativa de Costa Rica (2011). http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC

Ley 8934. Ley de Protección de la Niñez y la Adolescencia frente al contenido nocivo de Internet y otros medios electrónicos. Asamblea Legislativa de Costa Rica (2011). http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=71024&nValor3=0

Martínez-Pastor, E., Catalina-García, B., & López-de-Ayala-López, M.-C. (2019). Smartphone, menores y vulnerabilidades. Revisión de la literatura. *Revista Mediterránea de Comunicación*, *10*(2). https://doi.org/10.14198/MEDCOM2019.10.2.5

MICITT. (2017). Estrategia Nacional de Ciberseguridad de Costa Rica 2017 (ISBN: 978-9968-732-52-9; p. 59). Ministerio de Ciencia, Tecnología y Telecomunicaciones. https://www.micitt.go.cr/wp-content/uploads/2022/05/Estrategia-Nacional-de-Ciberseguridad-Costa-Rica-Oficial.pdf

MICITT. (2021). Revisión de la Estrategia Nacional de Ciberseguridad de Costa Rica (2017) (p. 52). Ministerio de Ciencia, Tecnología y Telecomunicaciones. https://www.micitt.go.cr/wp-content/uploads/2022/05/Revision-de-la-Estrategia-Nacional-de-Ciberseguridad-de-Costa-Rica-2017.pdf

Mıhcı Türker, P., & Kılıç Çakmak, E. (2019). An investigation of cyber wellness awareness: Turkey secondary school students, teachers, and parents. *Computers in the Schools*, *36*(4), 293-318. https://doi.org/10.1080/07380569.2019.1677433

Moncada Vargas, A. E. (2020). Comparación de técnicas de machine learning para detección de sitios web de phishing. *Revista Interfases*, (013), 77-103. https://doi.org/10.26439/interfases2020.n013.4886

OEA, & AWS. (2020). Alfabetización y seguridad digital: la importancia de mantenerse seguro e informado. *Programa de Ciberseguridad del Comité Interamericano*

contra el Terrorismo. https://www.oas.org/es/sms/cicte/docs/20200925-ESP-White-Paper-Educacion-en-Ciberseguridad.pdf

OEA, & CISCO. (2023). Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades. *Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo*. https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf

OEA & Twitter. (2021). Alfabetización y seguridad digital: la importancia de mantenerse seguro e informado. *Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo*. https://www.oas.org/es/sms/cicte/docs/alfabetizacion-y-seguridad-digital.pdf

ONU. (2013). *BYND2015 Global Youth Declaration. Organización de las Naciones Unidas*. https://www.un.org/youthenvoy/2013/09/bynd2015-the-worlds-youth-send-message-from-costa-rica-to-the-united-nations-general-assembly/

Ormond, Jim (2018). Well-Trained Cybersecurity Pros Needed to Fill 1.8 Million Open Jobs. First-Ever Global Curriculum Guidelines Reflect Worldwide Demand for Qualified Professionals and Urgent Industry Needs. *ACM Association for Computing Machinery publication in Advancing Computing as a Science & Profession*. https://www.acm.org/binaries/content/assets/press-releases/2018/february/cybersecurity-curricula-17.pdf

Proyecto de Ley de Ciberseguridad de Costa Rica, Expediente 23292, Asamblea Legislativa, Gaceta 172 Alcance 189 (2022). http://www.asamblea.go.cr/Centro_de_informacion/Consultas_SIL/SitePages/ConsultaProyectos.aspx

Robles-Gómez, A., Tobarra, L., Pastor-Vargas, R., Hernández, R., & Cano, J. (2020). Emulating and evaluating virtual remote laboratories for cybersecurity. *Sensors*, *20*(11). https://doi.org/10.3390/s20113011

Sadaghiani-Tabrizi, A. (2018). *Integrating Cybersecurity Education in K-6 Curriculum: Schoolteachers, IT Experts, and Parents' Perceptions [DM/IST]*. https://www.proquest.com/docview/2029241565/abstract/7334F06BB5114751PQ/1

Sağlam, R. B., Miller, V., & Franqueira, V. N. L. (2023). A Systematic Literature Review on Cyber Security Education for Children. *IEEE Transactions on Education*, 66(3), 274-286. https://doi.org/10.1109/TE.2022.3231019

Siddiqui, Z., & Zeeshan, N. (2020). A Survey on Cybersecurity Challenges and Awareness for Children of all Ages. *International Conference on Computing, Electronics & Communications Engineering (ICCECE*), 131-136. https://doi.org/10.1109/iCCECE49321.2020.9231229

Stavrou, E. (2020). Back to Basics: Towards Building Societal Resilience Against a Cyber Pandemic. *Journal on Systemics, Cybernetics and Informatics (JSCI)*, *18*(7).

Stein, D., Scribner, B., Kyle, N., Newhouse, W., Williams, C., & Yakin, B. (2017). National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators: Indicators for Performing Work Roles (NIST Internal or Interagency Report (NISTIR) 8193 (Draft); p. 98). National Institute of Standards and Technology. https://csrc.nist.gov/CSRC/media/Publications/nistir/8193/draft/documents/nistir8193-draft.pdf

Touré, H. (2013). Global Youth Summit BYND2015. https://www.un.org/youthenvoy/2013/09/bynd2015-the-worlds-youth-send-message-from-costa-rica-to-the-united-nations-general-assembly/

UNICEF. (2006). Convención sobre los Derechos del Niño. https://www.un.org/es/events/childrenday/pdf/derechos.pdf

UNICEF. (2020, marzo 11). Digital civic engagement by young people. https://www.unicef.org/globalinsight/reports/digital-civic-engagement-young-people

Vanderhoven, E., Schellens, T., & Valcke, M. (2014). Educational Packages about the Risks on Social Network Sites: State of the Art. *Procedia - Social and Behavioral Sciences*, 112, 603-612. https://doi.org/10.1016/j.sbspro.2014.01.1207

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as "the three R's". *Heliyon*, *5*(12). https://doi.org/10.1016/j.heliyon.2019.e02855

Waldock, K., Miller, V., Li, S., & Franqueira, V. (2022). Pre-University Cyber Security Education: A report on developing cyber skills amongst children and young people (p. 159). Institute of Cyber Security for Society, University of Kent. https://cybilportal.org/wp-content/uploads/2022/08/GFCE-report-20220731.pdf

Zhuge, H. (2010). Cyber Physical Society. 2010 Sixth International Conference on Semantics, Knowledge and Grids, 1-8. https://doi.org/10.1109/SKG.2010.7

ANEXO

Universidad Internacional de las Américas de Costa Rica – Escuela de Ingeniería Informática

Programa de Alfabetización Digital – Proyectos realizados de extensión universitaria

Nombre del proyecto	Población meta
Taller de herramientas ***Office***	Todo público
Capacitación en soporte técnico para jóvenes	Jóvenes entre 15 a 18 años
Aplicación de escritorio para el aprendizaje de operaciones básicas	Niños entre 9 y 10 años
Capacitación en soporte técnico y redes	Jóvenes entre 17 y 24 años
Software para el manejo del servicio de comedor del Liceo Napoleón Quesada en Guadalupe	Jóvenes de educación media del Liceo
Taller para el uso del computador e internet	Todo público
Capacitación para el aprendizaje del lenguaje de programación Java	Jóvenes entre 15 y 24 años
Taller de herramientas ***Office*** para Aldeas SOS	Niños y jóvenes de la organización
Taller de herramientas ***Office*** para la Fuerza Pública	Adultos miembros de la institución policial
Taller de Herramientas ***Office*** AGECO	Adultos mayores miembros de la Asociación Gerontológica de Costa Rica
Capacitación en soporte técnico y redes	Jóvenes entre 16 y 19 años
Taller de herramientas ***Office*** para IFEMSI	Adultos miembros de la organización
Capacitación para el aprendizaje del lenguaje de programación Java	Jóvenes entre 15 y 24 años
Capacitación sobre el desarrollo de páginas web	Jóvenes entre 17 y 24 años
Taller de soporte técnico	Todo público
Capacitación en desarrollo para aplicaciones de escritorio	Todo público
Taller para uso de redes para adultos mayores	Adultos mayores
Taller de ciberseguridad para niños	Niños
Taller de ciberseguridad para pymes	Miembros de emprendimientos de pequeñas y medianas empresas (pymes)

Olda Bustillos Ortega, Javier Rojas Segura,
Jorge Murillo Gamboa

Ciberseguridad y desarrollo de habilidades digitales: propuesta de alfabetización digital en edades tempranas
Cybersecurity and digital skills development: a proposal for digital literacy at early ages

Interfases
núm. 18, p. 185 - 205, 2023
Universidad de Lima,
ISSN: 1993-4912

DOI: https://doi.org/10.26439/interfases2023.n018.6626