INVESTIGACIÓN

# Análisis del sistema educativo costarricense: Desafío crítico para la ciberseguridad del país

ANALYSIS OF THE COSTA RICAN EDUCATIONAL SYSTEM:
CRITICAL CHALLENGE FOR THE COUNTRY'S CYBERSECURITY

**M. Ed. Carolina Artavia Madrigal[1], M. Ed. Melissa Guevara García[2], Isaac Mora Zumbado[3], Lic. Tadeo Murillo Murillo[4], Msc. Mynor Ramírez González[5], Ing. Valeria Solano Ruiz[6]**

Fecha de recepción: 20-03-2023 | Fecha de aprobación: 19-04-2023

## Resumen

La presente investigación tiene como objetivo conocer la realidad nacional en la educación superior en el área de estudio de ciberseguridad. Se realizó un análisis de planes de estudio de carreras específicas en las universidades públicas y universidades privadas reconocidas, el cual evidenció la carencia de preparación en temas de ciberseguridad. También, se analizaron las consecuencias de la carencia de preparación que tiene nuestro país en temas de seguridad informática y se estableció las implicaciones que conllevaría introducir materias de ciberseguridad en planes de estudio universitario.

## Palabras clave:

Seguridad informática, educación universitaria, ciberataque, tecnología, vulnerabilidad.

## Abstract

The investigation study has the objective to know the national reality in higher education in cybersecurity study; an analysis of curricula of specific careers in public universities and recognized private universities was carried out, which evidenced the lack of preparation in cybersecurity issues. Also, were analyzed the consequences of the lack of preparation that our country has in computer security issues and established the implications of introducing cybersecurity subjects in university curricula.

1 M. Ed. Carolina Artavia Madrigal, aartaviam094@ulacit.ed.cr, ORCID: 0000-0001-8966-4222
2 M. Ed. Melissa Guevara García, mguevarag970@ulacit.ed.cr, ORCID: 0000-0002-8280-9959
3 Isaac Mora Zumbado, isaacmz2002@gmail.com, ORCID: 0000-0001-9180-7835
4 Lic. Tadeo Murillo Murillo, tmurillom038@ulacit.ed.cr, ORCID: 0000-0002-5676-0493
5 Msc. Mynor Ramírez González, mramirezg116@ulacit.ed.cr, ORCID: 0000-0002-3050-0773
6 Ing. Valeria Solano Ruiz, vsolanor892@ulacit.ed.cr, ORCID: 0000-0003-2046-3881

## Keywords:

Computer security, university education, cyberattack, technology, vulnerability.

## Introducción

La educación, sin lugar a duda, ha sido un pilar fundamental del desarrollo de la sociedad costarricense, la cual se ve cada día más inmersa en avances científicos y tecnológicos que sustentan la capacidad de mejorar bienes, servicios, la economía y hasta la calidad de vida de las personas. En Costa Rica la educación, según indica Cartín-Sánchez (2018), está dividida en los siguientes niveles Preescolar, Primaria, Secundaria y Educación para el Trabajo, con el desarrollo proceso en el cual se obtienen los conocimientos necesarios de la educación general básica.

En cualquiera de los ámbitos que se desempeñen las personas profesionales actualmente, requieren contar con un perfil curricular que contenga conocimientos tecnológicos, al menos en uso de herramientas ofimáticas, lo cual ha sido durante años un tema prioritario en el sistema educativo costarricense, el cual incluyó el uso de la tecnología desde el año 1988 con el Programa Nacional de Informática Educativa que se ha orientado hacia el empleo de tecnologías digitales como herramientas para el aprendizaje y el desarrollo intelectual de los estudiantes y así disminuir brechas sociales y que la integración a economías mundiales sea de mejores beneficios (Ministerio de Educación Pública de Costa Rica, 2020).

Lo anterior, conllevó a que las personas profesionales se hallan convertido en buenos usuarios de la tecnología, haciendo uso de programas para realizar cálculos, sistemas particulares de las empresas, navegando en Internet y desempeñarse de manera asertiva utilizando múltiples dispositivos electrónicos como computadoras, tabletas, teléfonos inteligentes e incluso los denominados objetos inteligentes. No obstante, la gran labor de enseñanza de la tecnología ha dejado de lado el tema de la ciberseguridad, la cual promueve el uso adecuado de la tecnología y los cuidados que se deben tener para prevenir ser víctima, como individuo o como empresa, de los delincuentes cibernéticos denominados hackers, quienes ante un ataque exitoso pueden causar mucho daño a la información de personas, empresas y gobiernos.

En los últimos años se ha visto que uno de los principales vectores de ataque que utilizan los hackers es el usuario final, quien en muchas ocasiones a falta de conocimiento abre un correo malicioso y sigue enlaces de acceso a sitios de estafas. Según indica Cordero- Pérez (2022), "para el año 2021, los ataques tipo Correo Electrónico Comercial Comprometido (*Business Email Compromise* -BEC-) son los más costosos ($2.396 millones)" (párr. 17). Es preciso que los programas de educación incluyan además del contenido técnico, el tema de la ciberseguridad, en consideración de que los nuevos

actores en el mundo laboral posean conocimientos suficientes para identificar un correo electrónico falso, una llamada telefónica de estafa y cómo verificar que su equipo tecnológico de trabajo se encuentre actualizado y con las protecciones necesarias para prevenir un incidente.

Un usuario bien preparado puede salvar a una empresa de pérdida de información sensible que le podría costar mucho dinero recuperarla o incluso la quiebra por no tener información para operar. Es por esto que la articulación entre la educación y la ciberseguridad debe estrecharse cada día más, para formar buenos usuarios de la tecnología que velen por el buen uso de los recursos y la ciberseguridad.

Considerando lo indicado, esta investigación intenta establecer el reto que representa para la educación superior, integrar el tema de ciberseguridad y las implicaciones de agregar su contenido en programas ya establecidos que se enfocan en tecnificar al usuario y controles de seguridad para el entorno, mas no así en el contenido. Así mismo, se pretende establecer mecanismos que ayuden a optimizar la gestión de los planes de estudio y abarcar contenido de ciberseguridad.

## Revisión de la literatura

Es bien conocido que la tecnología es un aliado fundamental para muchos sectores de la sociedad actual, pero también se ha convertido en una especie de arma si no se cuenta con los cuidados necesarios para evitar algún ataque. Así lo indica Rustici (2012), cuando menciona que "la complejidad y capacidades de estas amenazas [virtuales] aumentan en directa proporción al nivel de conectividad de la sociedad" (p. 25). Como continúa indicando Rustici (2012), durante los últimos veinte años se han formado grupos que utilizan la tecnología como medios para realizar ataques maliciosos en contra de muchos países.

Tal y como se menciona en párrafos anteriores, el proceso educativo como tal es un pilar fundamental de la sociedad, y sobre todo con lo cambiante que es el mundo actual, este sector debe estar siempre al pendiente de los giros que se dan, en especial en cuanto a tecnología se refiere. La constante evolución de la digitalización trae varios beneficios, específicamente en el sector de la educación. El acceso a la información y a la transferencia de conocimientos gracias a la interconexión en red agiliza el proceso de aprendizaje. Por tal motivo, no es de sorprenderse que cada vez más personas docentes y estudiantes, así como personal administrativo utilicen dispositivos tecnológicos para realizar sus labores.

Rohde y Schwarz Cybersecurity (2021), una empresa líder en seguridad informática lo describió perfectamente: "El acceso a wifi libre en los centros educativos, ya sean universidades, escuelas técnicas o bibliotecas, es hoy en día una parte integral del aprendizaje contemporáneo, los medios digitales aplicados a la docencia pueden mejorar los resultados del aprendizaje" (párr. 1).

La rápida incorporación de las nuevas tecnologías al proceso de enseñanza en los sistemas educativos es sin duda uno de los elementos que contribuye a la preparación de las personas estudiantes para los desafíos dentro del mundo profesional, así como también de los cambios a nivel económico y social. Sin embargo, esa integración, entre el proceso educativo y las tecnologías no es tan ágil como se creería, al contrario, se ha vuelto lento y difícil, y esto a pesar de que las metodologías actuales se han combinado con las tecnologías produciendo como resultados profesionales creativos y con múltiples habilidades (Renz y Hilbig, 2020). Según lo señala Poveda- Pineda y Cifuentes- Medina (2020):

> La incorporación de las tecnologías de información y comunicación (TIC) en la educación superior, hoy es una realidad, ahora el reto transciende a la combinación de metodologías de aprendizaje que fomente en el rol docente, la vinculación de estrategias pedagógicas apoyadas la gamificación, el aprovechamiento de herramientas digitales en línea y el uso adecuado de las TRIC para responder con las exigencias educativas actuales.(p. 96)

Entonces, desde la docencia, es necesario estar siempre al pendiente de la rapidez con que cambia la tecnología, lo que "hace necesario investigar nuevos modelos y estrategias de enseñanza-aprendizaje que faciliten al individuo la asimilación en el menor tiempo posible de los cambios tecnológicos y lo capaciten para las nuevas demandas del mercado laboral" (Prendes y Cerdán, 2021, p. 35).

La globalización ha traído a los países y sus poblaciones grandes ventajas tecnológicas, educativas y sociales, por mencionar solamente algunas. Así como la comunicación entre las naciones ha mejorado significativamente, junto con el intercambio de información en muchos ámbitos, ha surgido la necesidad también de proteger dichos datos de personas o entidades, de forma mal intencionada, se quieren aprovechar ilegalmente de la substracción de identidades, robo de información u otros delitos informáticos. De acuerdo con Vargas et al. (2017), la ciberseguridad se puede establecer desde dos acepciones. La primera de ellas, "desde un punto más estratégico, en el que se identifica la condición de un ciberespacio libre de amenazas, peligros y daños, así como el nivel de riesgo al que están expuestas sus organizaciones y ciudadanos" (Vargas et al., p. 34).

Por otra parte, siempre ha sido de gran interés para las personas y países conocer los planes o estrategias de sus vecinos y/o rivales. Eso son el fin de sacar provecho a distintas situaciones que se puedan presentar en el futuro y así beneficiar a sus poblaciones. Es por eso que Vargas et al. (2017), le da una segunda perspectiva al término de ciberseguridad al decir ésta "trata de preservar la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, entre otros atributos" (p. 35). Al mejorar el ambiente en el que cada país o población desarrolla el conjunto de sus acciones del día a día, se convierte en un

ambiente mucho más productivo y uno que permite continuar intercambiando información y mejoras tecnológicas.

Por ejemplo, sin la colaboración de sus ciudadanos, un país no es capaz de materializar por sí sólo el concepto de ciberseguridad. Se requiere de un esfuerzo muy amplio para defendernos, digitalmente, de los peligros que conlleva el camino de la era digital. De acuerdo con Cano (2008), son "necesarias una serie de prácticas prioritarias, con el fin de darle sentido real y dimensionado a la seguridad de un país, en el contexto digital en el que nos encontramos, en el cual la información es instantánea" (p. 6). A medida que exista una mayor y mejor puesta en práctica de formas de protegernos contra los ciberataques, mejor será el resultado del uso de las tecnologías que tanto beneficio traen a la población mundial.

Es por eso que cuando se trata de conceptualizar el término ciberseguridad, no es posible enfrascarlo únicamente en una sola institución, un solo organismo o una única persona. Es una responsabilidad de todas y todos. De acuerdo con Cano (2008), se trata de un trabajo en conjunto, coordinado y constante para que en el transcurrir del tiempo, cada institución, organismo y persona pueda transitar libremente por las increíbles vías de tecnología que la globalización ha dispuesto. Y puedan de esta forma aprovechar los enormes beneficios de estar conectados, en tiempo real, con el resto del mundo.

Así mismo, el rol de las universidades a lo largo de los años ha tenido un espacio característico e importante en el desarrollo y la evolución de las sociedades. Su misión desde el origen fue ocuparse de la conservación y la transmisión del conocimiento. Sin embargo, la evolución de la sociedad, el contexto y las necesidades relacionadas a estos ha generado una exigencia distinta al rol de dichas instituciones, no solo como entes que promueven el conocimiento, si no como el espacio de formación y transformación de la sociedad, y a su vez ser una plataforma que contribuye al crecimiento y evolución de la ciencia y la tecnología (Rodríguez et al., 2017).

Esta transformación es lo que ha generado que la investigación se convierta en un pilar esencial en las instituciones de formación superior, catalogándolas como uno de los puntos focales para la evolución y el mantenerse a la vanguardia de las transformaciones no solo tecnológicas si no sociales y culturales que vienen de la mano.

Las Tecnologías de la Información y la Comunicación (TIC) se han introducido en todo aspecto de la vida del ser humano, modificando la cultura, la interacción social, el entorno y hasta los sistemas educativos, transformando no solo los medios y las metodologías si no las temáticas y puntos de interés formativos. Lo que se traduce a una exigencia de la sociedad actual para hacer frente a la era tecnológica y las necesidades que estas conllevan (Mendivil et al., 2022).

En el 2017 la revista *The Economist* publicó un artículo en el que señalaba la sociedad actual como una en la que el recurso más valioso había dejado de ser el petróleo y se había convertido en los datos.

Dándole fuerza no solo a la necesidad de la integración de la tecnología en la educación si no a su vez en la seguridad del uso y de los datos generados por la misma, convirtiendo a la ciberseguridad en uno de los campos de estudio más relevantes en el ámbito de las TIC (Mendivil et al., 2022).

Desde el crecimiento del uso de la tecnología y de la generación de datos, los ciber ataques se han incrementado exponencialmente y esto ha generado golpes importantes en la confianza y en el uso de la misma tecnología. La realidad es que la seguridad no ha evolucionado con la misma velocidad con la que ha evolucionado el uso de la tecnología generando ataques constantes hacia la integridad de los datos no solo desde entes externos sino también a causa de la desinformación de las personas internas de las empresas o instituciones. Mas del 20% de los ciber ataques son incidentes o engaños realizados a los trabajadores de las empresas (Mendivil et al., 2022).

Debido a esto, se dice que los seres humanos siguen siendo el eslabón débil de los sistemas de seguridad, principalmente por su falta de educación al respecto, lo que a su vez es consecuencia de la falta de propuestas metodológicas que enseñen de forma actualizada y contextualizada y a la integración de estos programas en los sistemas formales e informales de educación (Mendivil et al., 2022).

Es necesario que las universidades adopten iniciativas y planes estratégicos para abordar la ciberseguridad desde la educación de la sociedad civil para hacer un frente y lograr evolucionar a la misma velocidad con la que evoluciona la tecnología. Se propone que las universidades elaboren programas de comunicación, servicio social, concientización y demás en temas de ciberseguridad para socializar los términos; que generen alianzas con instituciones públicas para hacer frente a las necesidades de seguridad y proporcionar personas preparadas e insumos para subsidiarlas y, sobre todo, que sea un elemento parte de esa formación integral buscada por las instituciones de educación superior (Rodríguez et al., 2017).

Como se ha expuesto anteriormente, una correcta educación y orientación en el área de ciberseguridad y tecnología en general es crucial para el desarrollo del país en la actualidad, puesto que se ha evidenciado la necesidad de mejora en estos ámbitos debido a la poca eficiente intervención estatal con el fin educar a la población de una manera adecuada y sustanciosa en estos tópicos.

En primer lugar, se debe analizar la escasez de profesionales en el área, es decir, hay muy pocas personas graduadas en este momento en materia de ciberseguridad, lo que provoca una clara ineficiencia en el engranaje necesario para poder generar un ambiente de seguridad cibernética en el país. Aunque varias universidades están incorporando en sus planes de estudio especialidades e ingenierías en ciberseguridad, no se está ni cerca de cumplir con la demanda laboral actual, puesto que hay que tomar en cuenta tanto el área privada como pública (Le-Lous, 2021).

Según Le-Lous (2021), la cantidad de graduados en carreras relacionadas a la tecnología y ciberseguridad cayó un 16% en 2020, comparando los graduandos del año anterior (tomando en cuenta datos actualizados

a octubre 2021 por Consejo Nacional de Rectores [CONARE]). Así mismo, se habla del alejamiento y desinterés que está mostrando el joven costarricense hacia las conocidas "carreras del futuro", esto provoca que el país no cumpla con la creciente demanda internacional en este ámbito, quedando rezagado en temas de ciberseguridad simplemente por no poseer con la planilla suficiente.

Debido a lo anteriormente expuesto, se puede deducir con facilidad que Costa Rica, como país en sí, es un vulnerable y fácil objetivo para distintos grupos criminales organizados que se dedican a realizar hackeos a entes públicos u organizaciones privadas con el fin de extraer información sensible, encriptarla, y extorsionar a la víctima para que realice un pago de una cantidad considerable de dinero a cambio de la liberación de dicha información.

Lo anterior se puede ejemplificar con el ciberataque que recibió el Ministerio de Hacienda el pasado 19 de abril, el cual afectó la plataforma de Administración Tributaria Virtual (ATV), por la cual se declaran y se pagan impuestos, asimismo el sistema de Tecnología de Información para el Control Aduanero (TICA). Por otro lado, se presentaron problemas con el pago a la planilla pública de este ente ya que el sistema se encontraba caído. Este ciberataque se la atribuyó al grupo organizado Conti, el cual hizo su enunciado colgando su autoría en el sitio oficial del Ministerio de Hacienda (Swissinfo, 2022).

El ataque al Ministerio Hacienda ha sido solamente el principio de la ola de ciberataques que está viviendo el país actualmente, lo cual genera una verdadera angustia y preocupación, ya que la deficiente respuesta ante dichos ataques ha sido lenta y se podría decir, "débil". Debido a esto, se debe estudiar detenidamente el actuar de estos grupos criminales para así poder entender de qué manera se puede mejorar la seguridad y respaldo de datos sensibles, con el fin de prevenir futuros desastres como el que se está viviendo. Tal y como lo reportó el periódico La República, el grupo de origen ruso llamado "Conti", solicitó un pago de $10 millones de dólares a cambio de devolver los datos sensibles que fueron sustraídos a esta institución, y con el fin de detener también los ataques a los otros entes estatales (Castro, 2022).

## Metodología

El enfoque de investigación del presente artículo se desarrolla desde la perspectiva de un modelo cualitativo; a través de la descripción de la problemática existente e indagando de manera dinámica entre los hechos y su interpretación (Hernández-Sampieri et al., 2014).

Acerca de la caracterización del estudio se establece que sea de tipo exploratorio, el cual se basa en conocer una problemática de la cual no se evidencia amplio estudio previo. Tal como indican Hernández-Sampieri et al. (2014), este estudio permitirá obtener información para una investigación posterior más completa, estableciendo prioridades para investigación posteriores.

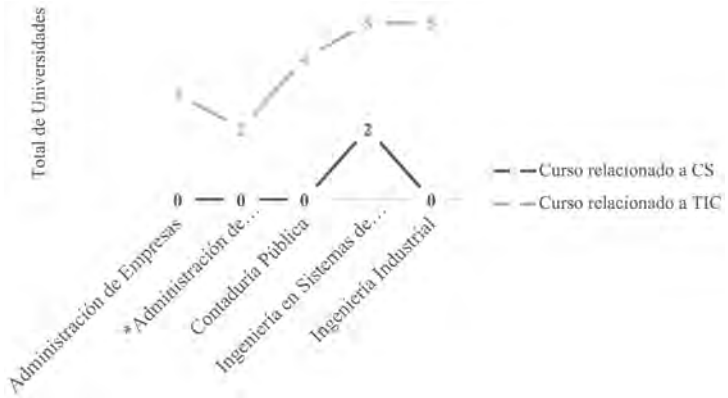
## Resultados

El análisis de se ha denominado *un vistazo básico de la realidad nacional*. Con el fin de conocer la realidad actual en la educación superior universitaria a nivel nacional, se procede a realizar un análisis de carreras específicas tanto a nivel privado como público con el fin de conocer existencia o inexistencia de temas de ciberseguridad en los planes de estudio.

Se efectuó un estudio de los planes universitarios de 5 Universidades privadas que se ubican en el Gran Área Metropolitana (GAM) y que se encuentran entre las más conocidas, y de cada Universidad se evaluó de 5 de las 10 carreras (en el grado de bachillerato universitario) que se encuentran en el ranking de carreras de mayor demanda laboral según la Agencia Costarricense de Promoción de Inversiones (CINDE) (Revista Summa, 2020). Parte de importante del porqué se eligieron esas 5 carreras es debido a la relación estrecha con la TIC y su relación con información confidencial y sensible.

En la Tabla 1, que a continuación se presenta, se refleja la cantidad total de cursos que imparte cada universidad en temas de Tecnología de la Información (TI) y de ciberseguridad tomando en cuenta las carreras seleccionadas. Las carreras tomadas por universidad son: Universidad Latina: Ingeniería de Sistemas de Computación, Administración de Negocios, Administración de Negocios con énfasis en Recursos Humanos, Contaduría Pública, Ingeniería Industrial; Universidad Latinoamérica de Ciencia y Tecnología: Ingeniería Informática, Administración de Negocios, Comportamiento Organizacional, Contaduría, Ingeniería Industrial; Universidad Americana: Ingeniería de Sistemas, Administración de Negocios, Administración con Énfasis en Recursos Humanos, Contaduría, Ingeniería Industrial; Universidad Internacional de las Américas: Ingeniería en Informática, Administración de Empresas, Administración de Empresas con Énfasis en Recursos Humanos, Contaduría Pública, Ingeniería Industrial; Universidad Fidélitas: Ingeniería en Sistemas de Computación, Administración de Negocios, Gestión de Recursos Humanos, Contaduría, Ingeniería Industrial.

**Tabla 1. Comparativa entre carreras universitarias a nivel de bachillerato**




Fuente: Elaboración propia.

Según el gráfico anterior, se puede evidenciar que, de las 5 universidades, 3 de las mismas tienen algún curso relacionado con TIC incluido en el plan de estudio de la carrera de Administración de Empresas; en la carrera de Administración de Recursos Humanos únicamente 2 tienen algún curso relacionado con TIC en su Plan de Estudio, en el caso de Contaduría 4 de las 5 universidades si contemplan un curso relacionado con TIC en su Plan de Estudio, y para las carreas de Ingeniería en Sistemas e Ingeniería Industrial todas las carreras contemplan el conocimiento sobre TIC.

Ahora bien, también se realizó un estudio sobre si estas carreras contemplaban algún curso relacionado con la ciberseguridad dentro de su plan de estudio, y tal como se esperaba, únicamente 2 universidades en la carrera de Ingeniería en Sistemas contemplan este curso como parte del plan de estudio, siendo bastante interesante ya que se esperaría que en la carrera de Ingeniería en Sistemas todos los planes contemplen este tema tan importante, pero queda evidenciado de que no. Las demás carreras que no están directamente relacionadas a TIC no contemplan nada relacionado a ciberseguridad en sus Planes de Estudio, siendo hoy uso de las mismas esencial para ejercer labores en estas carreras laborales.

Como parte de esa investigación, se evidenció si estas Universidades contemplaban en su oferta académica el tema de Ciberseguridad, con lo cual se encontró la siguiente información, como lo indica la Tabla 2:

**Tabla 2. Grado académico que las universidades ofrecen en Ciberseguridad**

| | **Universidad 1** | **Universidad 2** | **Universidad 3** | **Universidad 4** | **Universidad 5** |
|---|---|---|---|---|---|
| ¿Cuenta la Universidad con algún técnico, diplomado, especialización, etc. en Ciberseguridad? | Licenciatura en Seguridad Informática | Especialización en *Cybersecurity* | No cuenta | No cuenta | Bachillerato Ingeniería en Seguridad Informática<br><br>Micro Máster en Ciberseguridad |

Fuente: Elaboración propia.

Según recopilado, se puede evidenciar una gran carencia nivel de Planes de Estudio en las universidades privadas, no sólo de temas relacionados a las TIC, sino y como eje central del estudio, la carencia de enseñanza relacionada a Ciberseguridad.

Así mismo, se realizó una comparación entre las 4 universidades públicas con mayor relevancia en temas de tecnología como lo son: la Universidad de Costa Rica (UCR), el Instituto Tecnológico de Costa Rica (ITCR), la Universidad Nacional (UNA) y la Universidad Técnica Nacional (UTN).

Se realizó un análisis de los 5 planes de estudios de las carreras con mayor demanda laboral, y en los casos de las universidades que no las impartían, se seleccionaron las carreras con mayor corte y

popularidad dentro de cada universidad para determinar la cantidad de cursos relacionados a TI que poseen las carreras y si poseen cursos relacionados a la ciberseguridad. Es importante mencionar que este análisis se dio juzgando por los títulos otorgados a cada uno de los cursos, esto quiere decir que si el título no refleja la temática no fueron tomados en cuenta.

La Tabla 3, que a continuación se presenta, refleja la cantidad total de cursos que imparte cada universidad en temas de TI y de ciberseguridad tomando en cuenta las 5 carreras seleccionadas; de igual manera se señala la cantidad de carreras cuantas de estas cuentan con dichos cursos. Las carreras tomadas por universidad son: UCR: Ingeniería en Software, Ingeniería en Computadoras, Dirección de Empresas, Contaduría Pública, Ingeniería Industrial, Ingeniería Eléctrica; TEC: Ingeniería en computación, Administración de Empresas, Ingeniería en Producción Industrial, Ingeniería Física, Ingeniería Ambiental; UNA: Ingeniería en Sistemas de Información, Relaciones internacionales, Ingeniería en Gestión Ambiental, Administración, Economía y UTN: Ingeniería en tecnologías de información, Ingeniería en Gestión Ambiental, Gestión y Administración empresarial, Contabilidad y Finanzas, Producción Industrial.

**Tabla 3. Análisis del nivel de inclusión del tema de TI en las carreras universitarias**

| Universidad | Cantidad total materias de TI | Cantidad de carreras con materias de TI | Cantidad total materias de ciberseguridad | Cantidad de carreras con materias de ciberseguridad |
|---|---|---|---|---|
| UCR | 18+ | 5/5 | 1 | 1/5 |
| ITCR | 9+ | 5/5 | 0 | 0/5 |
| UNA | 2+ | 3/5 | 1 | 1/5 |
| UTN | 6+ | 4/5 | 2 | 1/5 |

Fuente: Elaboración propia.

En el caso de la cantidad total de materias de TI se coloca el símbolo de '+' debido a que, en las carreras relacionadas a la ingeniería de sistemas, o afines, el 90% de los cursos eran de temáticas de TI por lo tanto contabilizarlas era contabilizar el plan completo de estudios.

Este resumen de datos demuestra que en las universidades públicas existe la incorporación de materias de TI en su gran mayoría, ya sea de elementos básicos o de funcionalidades genéricas que pueden apoyar en el desarrollo profesional sin importar si al área está directamente relacionada con la temática. Sin embargo, y con relación al tema de estudio, los cursos enfocados a la ciber seguridad no son tan comunes ni implementadas en las carreras, en su mayoría, los cursos encontrados fueron dentro de las carreras de ingeniería en sistemas y similares.

No obstante, las universidades públicas cuentan con una serie de programas libres o alternativos de distintas modalidades en las cuales se abarca el tema de la ciberseguridad. La Tabla 4 pretende ser un resumen de la oferta encontrada por cada universidad:

**Tabla 4. Grados académicos en Ciberseguridad en las universidades públicas**

| UCR | ITCR | UNA | UTN |
|---|---|---|---|
| Curso OEA en Ciberseguridad 2022 | Técnico en ciberseguridad empresarial | No | Ciberseguridad curso virtual |
| Introduction to Cybersecurity | Maestría en ciberseguridad | | Introduction to cibersecurity |
| Cibersecurity Essentials | Curso de Gestión de la ciberseguridad para profesionales asociados a la informática | | Cibersecurity essentials |
| Ciberseguridad Informática | Técnico en seguridad de redes de cómputo | | Fundamentos de ciberseguridad |
| | Programas de ed. continua: principios de ciberseguridad y privacidad | | |

Fuente: Elaboración propia.

Permitiendo concluir, que, a pesar de la gran demanda del conocimiento sobre ciberseguridad, y la necesidad de mantenerse a la vanguardia en dichos temas, las universidades no hay entrado a darle un frente significativo a la formación y expansión de conocimiento, a pesar de que debería ser un eje obligatorio como profesionales.

Después de realizar la investigación sobre las carreras, tanto en universidades públicas como privadas, sobre la incorporación de temas relacionados a tecnología o ciberseguridad, surge la consulta, ¿qué tan fácil o complicado es incorporar estos contenidos a las carreras? ¿Es viable esta opción? O bien implicaría un trabajo extra para las instituciones de educación. Por lo anterior se realizó un estudio de lo que implica incorporar contenidos sobre el tema en las carreras.

La inclusión de contenidos en los programas de los cursos de una carrera ya diseñada no solo requiere de un estudio completo por parte de las autoridades de esta, sino que, además, es necesario realizar un estudio de mercado, en dónde diferentes actores valoren las posibles implicaciones tanto para el sector comercial, industrial, social y académico, pues implicaría realizar cambios en el cambio de perfil

profesional o de salida, en los objetivos de la carrera, en los contenidos y otros. A parte de esto, el cambio debe ir de la mano con lo estipulado tanto en el Consejo Nacional de Rectores (CONARE) para las universidades públicas como para el Consejo Nacional de Enseñanza Superior Universitaria (CONESUP) para las universidades privadas, en cuanto a nomenclatura y créditos se refiere.

En cuanto a nomenclatura y créditos se refiere, ambos entes utilizan el Convenio para crear nomenclatura de grados (o niveles, hablando de diplomado, profesora, bachillerato, maestría o doctorado) y títulos de la Educación Superior Universitaria Estatal del CONARE (2004), qué, entre otras cosas, menciona la nomenclatura de grados y títulos aprobados para ser utilizados por las instituciones de educación superior universitaria estatal y privada. En este se indica, en su artículo 3 lo siguiente:

> Los tres grados o niveles para ofertar, se determinan de la siguiente:
>
> Pregrado: comprende el Diplomado y profesorado.
>
> Grado: Bachillerato y Licenciatura
>
> Posgrado: que serían la: Especialidad profesional, maestría y doctorado académico.

En el caso del Diplomado, el convenio CONARE (2004) indica que debe poseer cómo mínimo un total de 60 créditos y un máximo de 90. Esto estaría divido en 4 ciclos lectivos de 15 semanas (a excepción de la UTN que se distribuye en 14 semanas). Por otro lado, el pregrado de profesorado tiene un mínimo de 98 créditos y un máximo de 110, de igual manera con una duración de 6 ciclos y 15 o 14 semanas.

En el caso del grado de Bachillerato, CONARE (2004) menciona que el minino de créditos es 120 y un máximo de 144, con una duración de 8 ciclos lectivos y 15 semanas. Dado lo anterior, las instituciones de educación superior pública y privada deben regirse bajo este parámetro para incorporar los contenidos necesarios en los cursos para cubrir los tramos de la carrera.

En conversación con la señora Cynthia Gardela Berrocal, jefa del Departamento de Gestión y Evaluación Curricular de la Universidad Técnica Nacional, sobre la posibilidad de incluir en los programas de contenidos de ciberseguridad, y analizando junto a ella algunas estructuras y programas de cursos se determina que incorporar uno o varios contenidos o cursos sobre ciberseguridad, requiere un cambio en la estructura de cursos, esto implicaría un cambio en el perfil profesional o de salida, llevando a realizar un rediseño a la carrera, además, para incorporar contenidos se necesita realizar un análisis profundo el que debe incluir consultas como ¿Cuáles contenidos debe quitar o variar para introducir los de ciberseguridad y que no se altere el perfil profesional de la carrera?, también las carreras deben considerar si será mejor agregar cursos, en lugar de contenidos, para cumplir con lo mínimo del tema de ciberseguridad, esto implicaría analizar dos detalles. El primero de ellos sería que si al incorporar estos cursos se pasa de los créditos estipulados por CONARE (2004) ¿cuáles cursos se deberán eliminar para cumplir con los créditos?, y si elimino algún curso ¿cómo afectaría al objetivo de la carrera? Y en

segunda instancia si eliminar o incorporar algunos cursos, además de generar un cambio en la estructura de cursos, afectaría el perfil profesional, esto llevaría a un rediseño de carrera.

Dentro de la conversación con la señora Gardela, se llegó algunas otras ideas que podrían ser de mayor beneficio para las carreras, entre ellos los cursos de ciberseguridad podrían incorporarse como requisito de graduación, más no estar contabilizados en la estructura de curso (es decir no ser parte de los créditos). Generar esto dejaría la duda: ¿hacer uno o dos cursos cubriría lo necesario? Otra idea sería, generar un técnico, que sea complementario para las carreras, pero que se ofrezca como una opción que la carrera ofrece, la tercera opción, es realizar cursos desde la parte de extensión y se pueda ofrecerse a la comunidad en general, dando un espacio a las personas estudiantes de todas las carreras que así lo desean.

## Consecuencias

Según Freire (2017), en su investigación realizada, la región latinoamericana se encuentra años atrasada con respecto a regulación de ciberseguridad de parte de su marco jurídico. Datos de su investigación ubican a Costa Rica como el octavo país latinoamericano con mayores índices de ataques cibernéticos por medio de *malware*, lo que refleja la insuficiente e ineficiente seguridad que posee el país para este tipo de ataques. Como se ha expuesto anteriormente, es crucial para el desarrollo del país el legislar acertadamente en este tópico, puesto que hoy en día hay grandes brechas de seguridad y notables falencias en el sistema que colocan a Costa Rica en una situación de mayor vulnerabilidad.

Según lo expuesto anteriormente, se infiere con facilidad que Costa Rica posee sistemas de ciberseguridad muy pobres y frágiles, esto en todo el esquema estatal. Sin embargo, esta no es la única razón por la cual fue un objetivo tan claro del grupo criminal denominado Conti; sino que Costa Rica ha venido presentando un incremento considerable en conectividad a nivel país, es decir ha avanzado con pasos firmes en temas de digitalización y virtualización en distintos entes y procesos, no obstante, este crecimiento no ha sido proporcional al de seguridad y respaldo de dichos sistemas. (Amerise, 2022).

Lo anterior facilita el ingreso de *hackers* a los diversos sistemas para así implementar su *ransomware* que secuestra y encripta toda la información ahí almacenada. Cómo se ha documentado anteriormente el Ministerio de Hacienda fue el ente más afectado ante estos ataques, cuya pérdida monetaria se estima en decenas de millones de dólares; además del atraso de miles de procedimientos quirúrgicos que se han tenido que postergar puesto que la Caja Costarricense de Seguro Social (CCSS) también se vio vulnerada, la cual a la fecha sigue con su sistema caído. (Amerise, 2022).

Adicionalmente, se han contabilizado al menos 30 instituciones públicas que han sido afectadas por dichos ataques. Se aproxima que solo por el ataque a Hacienda el país pierde alrededor de $30 millones, eso sin contar la pérdida de control de la cantidad de ingresos recaudados por medio de impuestos y la

cantidad de dinero utilizada por las instituciones públicas, lo cual expone aún más al país a distintas situaciones perjudiciales. Por desgracia para los costarricenses, estos ataques no cesan y se proyecta un incremento en ellos y potencialmente a nivel regional se habla de un posible caos latinoamericano (Rosch, 2022).

Una mala orientación y gestión de la legislación en temas de ciberseguridad podría conducir a una especie de carrera armamentista y militar por parte de las grandes potencias mundiales, lo que desembocaría un gran conflicto con consecuencias mortales para todo el globo. Para evitar esto, se requiere una implementación a escala en todo el sistema educativo en temas de ciberseguridad para instruir a la población joven sobre estos temas que son vitales en la actualidad; además de firmar acuerdos internacionales que tengan como principal objetivo la resiliencia cibernética que busquen espacios seguros en la red (Cartini, 2016).

Los avances tecnológicos demandan cada día de mayores conocimientos y habilidades de parte de los usuarios, sean estos usuarios finales o profesionales que requieren utilizar equipos y herramientas tecnológicas para llevar a cabo sus tareas. Esto ha motivado a que la comunidad internacional realice acuerdos y brinde apoyo a países, empresas y personas para que su adaptación y conocimiento en cuanto al uso de tecnologías sea más amigable.

Según apunta el Ministerio de Educación Pública de Costa Rica (MEP, 2020), en el campo internacional, Costa Rica firmó su adhesión a la Declaración de Incheon, que resume la visión de la educación de aquí al 2030 de la UNESCO (Agenda 2030), que fue aprobada en el Foro Mundial de Educación el 21 de mayo de 2015. Su principal objetivo es conseguir una educación inclusiva, a, equitativa y de calidad y un aprendizaje a lo largo de la vida para todos. El MEP (2021) indica lo siguiente:

> Nos comprometemos también a fortalecer la ciencia, la tecnología y la innovación. Es preciso aprovechar las tecnologías de la información y la comunicación (TIC) para reforzar los sistemas educativos, la difusión de conocimientos, el acceso a la información, el aprendizaje efectivo y de calidad, y una prestación más eficaz de servicios. (p. 21)

El creciente entorno tecnológico, ha traído consigo la magnificación de las superficies de ataque hacia elementos cotidianos como dispositivos de Internet de las cosas (IoT), cámaras, teléfonos, micrófonos. Esto trae consigo la necesidad de necesidad de "educar desde temprana edad a los jóvenes sobre el buen uso del Internet y a su vez incentivar a la adquisición de conocimientos para la prevención de ciberataques" (Tamayo y Cuervo, 2022, p. 4).

Actualmente existen herramientas para fortalecer los conocimientos en ciberseguridad de toda la familia, tal como el Internet segura para niños del Instituto Nacional de Ciberseguridad de España (INCIBE) la

cual ofrece recursos como guías de control parental para reducir riesgos según los menores aprenden el uso de Internet, *Guía infancia para un uso seguro y responsable del Internet para profesionales relacionados con la protección de la infancia* y *Guía de Seguridad en Redes Sociales para Familias* (Guía RRSS) que brinda guías de seguridad en redes sociales y elementos para comprender porque le gustan a los jóvenes (INCIBE, 2019; INCIBE, 2020).

En consideración del alto nivel de tecnificación que se ha venido dando, es necesario que Costa Rica aborde con prontitud la integración de temas de ciberseguridad a los planes de estudio desde los primeros niveles y facilitar de herramientas que puedan ayudar a los ciudadanos (niños, jóvenes, adultos) y empresas a minimizar el riesgo que representa siempre el eslabón más débil de la cadena, como lo son quienes menos saben de ciberseguridad en este contexto.

## Conclusiones

Dentro de la larga lista de carreras universitarias que podemos encontrar en las instituciones tanto públicas como privadas de Costa Rica, el estudio de la ciberseguridad no tiene representación significativa. Es mínima la presencia de esta importante área de estudio, a pesar de lo actual y relevante de este tema en nuestra sociedad y a nivel global.

A pesar de ser un tópico altamente conversado en plataformas tanto nacionales como internacionales, se sigue haciendo caso omiso a la necesidad cada vez mayor de una mejor preparación en temas de ciberseguridad para protección personal, empresarial y nacional.

Finalmente, aunque existe amplia literatura sobre la relevancia que tiene la protección de la identidad virtual y todo lo que cubre la ciberseguridad, las universidades del país siguen sin actualizar sus planes de estudio o crear nuevas carreras que preparen a los estudiantes a enfrentarse y adaptarse a los requerimientos globales en cuanto a este tema.

## Recomendaciones

Aunque la Ciberseguridad es un tema que cada día toma más auge la investigación realizada para esta articulo dejo entrever que hoy falta todavía para poder incorporarla dentro de los planes de estudios, entre otras cosas las instituciones de educación superior podrían, entre otras cosas analizar los planes de estudios de las carreras para comprobar la posibilidad de incorporación de cursos de ciberseguridad, verificar la pertinencia de estos cursos para cada carrera.

De ser posible la incorporación de cursos de ciberseguridad solicitar el rediseño de las carreras correspondientes para la incorporación de los cursos al departamento indicado. También, de ser cursos

de extensión, verificar la población meta, si es una empresa, personas graduadas o bien para público en general, esto llevaría a analizar la metodología, procesos de evaluación y mediación a utilizar en los cursos. Finalmente, comprobar las plataformas tecnológicas que se utilizarán durante el proceso y de no tener las necesarias, hacer un análisis presupuestario para la incorporación de las mismas.

## Futuras líneas de investigación

Este artículo ha presentado argumentos relevantes en cuanto a la importancia de abordar la ciberseguridad en la educación con un alcance más amplio, no obstante, para futuras investigaciones se plantea investigar acerca de la necesidad de incluir en los planes de estudio de educación secundaria costarricense temas de ciberseguridad, esto a fin de indagar cuan permeado está el uso seguro de equipos electrónicos inteligentes.

También se recomienda investigar sobre programas de educación técnica en materia de tecnología y la importancia de que se incluya en éstos la ciberseguridad, en consideración evaluar si estos centros educativos enfatizan sus programas de estudio en sus especialidades, o bien, integran temas de utilidad para la vida cotidiana como lo es la seguridad de la información que se genera, comparte y guarda en medios electrónicos.

Otro tema que se recomienda estudiar es acerca de las incidencias cibernéticas a causa de los usuarios internos de las organizaciones, ya sea por desconocimiento de buenas prácticas de ciberseguridad o por falta de malicia ante atacantes.

## Referencias

Amerise, A. (20 de mayo de 2022). "Estamos en guerra": 5 claves para entender el ciberataque que tiene a Costa Rica en estado de emergencia. *BBC News Mundo*. https://www.bbc.com/mundo/noticias-america-latina-61516874

Cano, J. (2008). *Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global*. Asociación Colombia a de Ingenieros de Sistemas. https://acis.org.co/archivos/Revista/119/Editorial.pdf

Castro, J. (18 de abril de 2022). Hackers piden $10 millones al Gobierno de Costa Rica por información del Ministerio de Hacienda. *La República*. https://www.larepublica.net/noticia/hackers-piden-10-millones-al-gobierno-de-costa-rica-por-informacion-del-ministerio-de-hacienda

Cartín-Sánchez, D. (2018). *Datos de la Educación en Costa Rica*. Ministerio de Educación Pública de Costa Rica. https://www.mep.go.cr/indicadores_edu/BOLETINES/05_18.pdf

Cartini, A. (2016). Ciberseguridad: un nuevo desafío para la comunidad Internacional. *Bie3: Boletín IEEE,* (2), 950-966. https://dialnet.unirioja.es/servlet/articulo?codigo=5998287

Cordero-Pérez, C. (24 de abril de 2022). 13 estadísticas sobre la gravedad de los ataques de 'hackers'. *El Financiero*. https://www.elfinancierocr.com/blogs/la-ley-de-murphy/13-estadisticas-sobre-la-gravedad-de-los-ataques/FG5IJRWGKVEI3HUH2VRT3J74YU/story/

Consejo Nacional de Rectores. (2004). *Convenio para crear nomenclatura de grados y títulos de la Educación Superior Universitaria Estatal*. UCR. https://www.cu.ucr.ac.cr/normativ/nomenclatura_grados_titulos.pdf

Freire, K. (2017). *Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad* [Trabajo de grado, Universidad Católica de Santiago de Guayaquil, Ecuador]. Repositorio digital UCSG. http://201.159.223.180/handle/3317/9203

Hernández-Sampieri, R., Fernández-Collado, C., y Baptista-Lucio, P. (2014). *Metodología de la investigación* (6ta ed.). McGRAW-HILL.

Instituto Nacional de Ciberseguridad de España. (2019). *Guía de seguridad en redes sociales para familias*. https://www.incibe.es/menores/materiales/guia-de-seguridad-en-redes-sociales-para-familias

Instituto Nacional de Ciberseguridad de España. (2020). *Guía para profesionales de servicios de protección a la infancia*. https://www.incibe.es/menores/materiales/profesionales-infancia

Le Lous, F. (19 de diciembre de 2021). Graduados universitarios se alejan de carreras del futuro. *La Nación*. https://www.nacion.com/el-pais/educacion/numero-de-graduados-universitarios-en-carreras-del/5LB5YIECNBAGBMNZXWD5CBQLVA/story/

Mendivil, J., Sanz, B. y Gutiérrez, M. (2022). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. *Pixel-Bit, Revista de Medios y Educación, 63*, 197-225.

Poveda-Pineda, F., y Cifuentes-Medina, E. (2020). Incorporación de las tecnologías de información y comunicación (TIC) durante el proceso de aprendizaje en la educación superior. *Formación universitaria, 13*(6), 95-104. https://dx.doi.org/10.4067/S0718-50062020000600095

Prendes, P., y Cerdán, F. (2021). Tecnologías avanzadas para afrontar el reto de la innovación educativa RIED. *Revista Iberoamericana de Educación a Distancia, 24*(1). https://www.redalyc.org/articulo.oa?id=331464460002

Renz, A., y Hilbig, R. (2020). Prerequisites for artificial intelligence in further education: identification of drivers, barriers, and business models of educational technology companies. *International Journal of Educational Technology in Higher Education, 17*, 1-21. https://doi.org/10.1186/s41239-020-00193-3

Revista Summa. (29 de diciembre de 2020). *Costa Rica: Las carreras que tendrán mayor demanda laboral en 2021, según CINDE*. Recuperado el 10 de mayo de 2023 de https://revistasumma.com/costa-rica-las-carreras-que-tendran-mayor-demanda-laboral-en-2021-segun-cinde/

Rodríguez, C. H., Flores, M. C., y López, T. G. (2017). La universidad y su relación con la ciberseguridad. En *10 Temas de Ciberseguridad* (pp. 109). Editorial Universidad de Xalapa.

Rosch, C. (2 de junio de 2022). *Un ciberataque masivo en Costa Rica aflige a la ciudadanía*. Rest of Worlds. Recuperado el 10 de mayo de 2023 de https://restofworld.org/2022/ciberataque-costa-rica-ciudadania/

Rustici, R. (2012). Armas Cibernéticas: La igualdad de condiciones a nivel internacional. *Military Review, 25*. https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/MilitaryReview_20120831_art006SPA.pdf

Ministerio de Educación Pública de Costa Rica. (2020). *Política en tecnologías de la información del Ministerio de Educación Pública*. https://www.mep.go.cr/sites/default/files/documentos/politica-tic-mep.pdf

Swissinfo. (19 de abril de 2022). *El Ministerio de Hacienda de Costa Rica enfrenta un cibertaque*. Recuperado el 10 de mayo de 2023 de https://www.swissinfo.ch/spa/costa-rica-ciberataque_el-ministerio-de-hacienda-de-costa-rica-enfrenta-un-cibertaque/47528790

Tamayo V. y Cuervo C (2022). *Conocimientos sobre ciberseguridad en jóvenes y su impacto durante la virtualidad* [Trabajo de grado, Universidad Cooperativa de Colombia, Colombia]. Repositorio institucional. http://repository.ucc.edu.co/bitstream/20.500.12494/44928/1/2022-Conocimientos_Sobre_Ciberseguridad.pdf

Vargas, R., Recalde, L., y Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *Revista Latinoamericana de Estudios de Seguridad, 20,* 31-45. https://www.redalyc.org/journal/5526/552656641013/552656641013.pdf