INNOVACIÓN UNIVERSITARIA

Revista Académica

2022

VOLUMEN4 | revistainnovacionu@uia.ac.cr

Editorial

Innovación Universitaria es la revista académica de la Universidad Internacional de las Américas (UIA), en Costa Rica. Esta nace en el Departamento de Investigación e Innovación de la Universidad, a partir del Programa de Capacitación y Actualización Docente en Didáctica Universitaria. Su objetivo es difundir distintos tipos de manuscritos donde se exponen actualidades académicas relacionadas con el arte de formar a los futuros profesionales. La Revista está dirigida a toda la comunidad educativa; las personas autoras son responsables de la educación integral de los distintos estudiantes que se preparan para su ejercicio profesional.

En esta oportunidad, se presentan trabajos de la carrera de la Escuela de Ingeniería Informática, así como dos Memorias de la experiencia vivida en las Jornadas de Reflexión en Investigación y Extensión Social organizadas por el Departamento de Investigación e Innovación y el Departamento de Extensión Social. Todos los manuscritos son inéditos y versan entorno a temáticas para la mejora de los procesos de enseñanza–aprendizaje y reflexiones sobre el modelo educativo de la Universidad.

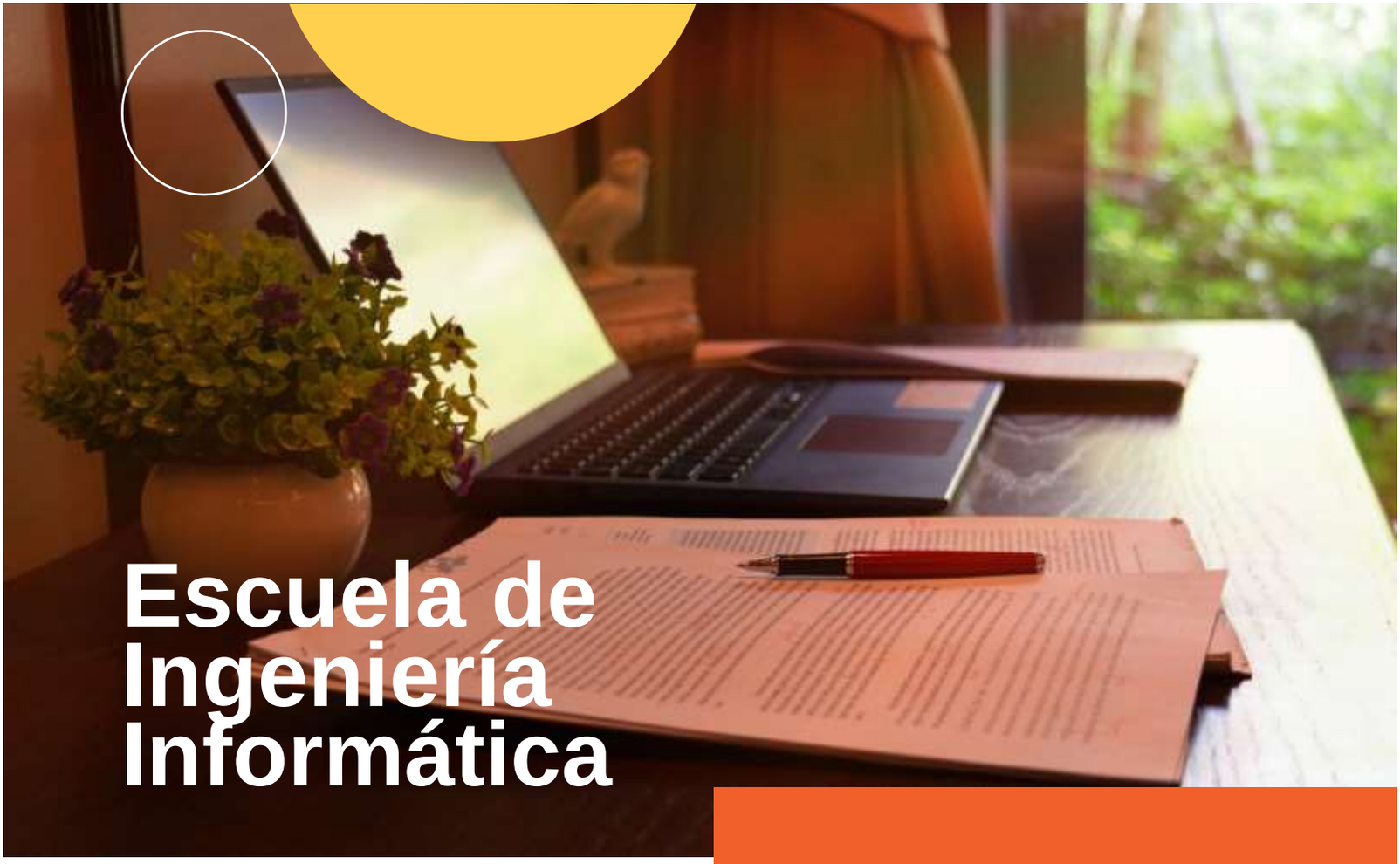
La Master Olda Bustillos Ortega, directora de la Escuela de Ingeniería Informática de la Universidad Internacional de las Américas, presenta su trabajo titulado: "*Memoria del Digital Time"*. La autora tiene propósito documentar y registrar la discusión acerca de la temática que está impactando actualmente a Costa Rica, como lo es la Ciberseguridad.

Por otra parte, la segunda publicación corresponde a la Memoria elaborada por el Departamento de Investigación e Innovación titulada: *"I Jornadas de Reflexión Universitaria: Resignificando la Investigación y Extensión Social".* Este manuscrito nace con el fin de conservar una sinopsis del primer evento académico reflexivo sobre procesos de investigación y extensión social organizado desde la Universidad Internacional de las Américas, en San José, Costa Rica.

Y, por último, la tercera propuesta que se encuentra en este volumen es la Memoria elaborada por la Coordinación Institucional de Extensión Social titulada: "*I Jornada de Reflexión Universitaria: Resignificando la Investigación y la Extensión Social".* El título busca recapitular las ideas principales generadas desde el área de Extensión Social, buscando reflejar así el exhaustivo proceso realizado en la UIA para llevar a cabo la tarea preliminar de colaborar con y para la sociedad.

Agradecemos los invaluables aportes de la licenciada Fernanda Segura Calderón colaboradora del Departamento de Investigación e Innovación por su mística y esmero para que este volumen fuese una realidad. Además, a los compañeros de Diseño Gráfico quienes aportaron de su talento para realizar el arte de la Revista Innovación Universitaria.

Bach. Carlos Ulate Lobo-Sociólogo
Editor colaborador del Departamento de Investigación e Innovación
Vicerrectoría de Gestión de Calidad UIA



Escuela de Ingeniería Informática

DIGITAL TIME

La Memoria del primer *Digital Time* de la Escuela de Ingeniería Informática de la Universidad Internacional de las Américas (UIA) se presenta con el propósito de documentar y registrar la discusión acerca de la temática que está impactando actualmente a Costa Rica, como lo es la Ciberseguridad.

El espacio del Digital Time tiene la intención de exponer con diversos especialistas sobre las tendencias tecnológicas que son vinculantes a las líneas de investigación de la Escuela de Ingeniería Informática.

Esta actividad se llevó a cabo el jueves 03 de marzo, donde los expertos compartieron con el público acerca de los esfuerzos, avances y prácticas de ciberseguridad que se han realizado en Costa Rica para afrontar los retos tecnológicos.

Objetivo

- **Conocer mediante un espacio académico con expertos en la materia acerca de las prácticas ytendencias de la Ciberseguridad en Costa Rica.**

Elaborado por: Master Olda Bustillos Ortega.

Descripción

Según la MSc. Olda Bustillos Ortega, Directora de la Escuela de Ingeniería Informática de la UIA (2022), el Digital Time tiene como referencia la Estrategia Nacional de Ciberseguridad de Costa Rica, elaborada por el Ministerio de Ciencia, Tecnología y Telecomunicaciones, MICITT 2017-2021, la cual representa un gran paso para Costa Rica en la creación de estrategias en materia de Ciberseguridad.

De acuerdo con el MICITT (2017), citado por Bustillos (2022) tal y como se describe en la estrategia “la seguridad cibernética requiere una visión holística y una atención multisectorial”, dado que el impacto de las Tecnologías de la Información y Comunicación (TICs) y la ciberseguridad están relacionadas con el desarrollo económico y social del país.

Asimismo, Bustillos (2022) hace referencia acerca de la situación del país en materia de Ciberseguridad

Costa Rica, es un país que confía en una fuerte promoción del uso de las tecnologías de la información y las telecomunicaciones como un eje para impulsar el desarrollo nacional y de manera que pueda fortalecer el marco normativo vigente en aras de favorecer el desarrollo y el uso de los servicios de telecomunicaciones dentro del marco de la sociedad de información del conocimiento y también con el apoyo de sectores como la salud, la educación, cultura, el comercio y gobierno.

Sin duda cada paso que se logra en el avance tecnológico, con lleva un gran reto a trabajar en estrategias para la protección de datos, el robo y uso no ético de la información.

La expositora inicia el diálogo a partir de una reflexión sobre la concepción y las implicaciones de la Ciberseguridad en las personas, y de cómo el tema se percibe con un alto grado de complejidad y alejado de la realidad individual. Las personas en su mayoría no toman en consideración algunas medidas de seguridad de la información personal, y en un momento donde el uso del internet ha crecido aceleradamente, las personas tienen una mayor exposición a este tipo de escenarios.

A partir de esta reflexión, es necesario definir ¿qué es un ciberataque? De acuerdo con Alejandro Andrade Mafla (2022) experto en ciberseguridad en el sector financiero, un ciberataque es:

Una acción que puede llevar a cabo un agente de amenaza en contra de un activo conectado al Internet. Se puede ejemplificar con algo sencillo, el tema de las suplantaciones de la identidad, si se conecta un dispositivo móvil al Internet en el quese utilizan las redes sociales, podría suceder que en algún momento alguien coloca nuestro nombre en el Internet, resultando así la suplantación de identidad intentando robar los datos personales y tratando de explotar nuestro perfil.

El Sr. Andrade menciona que un protocolo para afrontar un ciberataque debe considerar lo siguiente:

1. **La concientización de la sociedad acerca de la exposición de la información**
2. **Conocimiento acerca de la información con la que se cuenta.**
3. **Clasificación de la información. Se debe identificar la información sensible y crítica, para luego generar un respaldo en la nube u otro servidor.**
4. **En el caso de la parte empresarial, las organizaciones deben contar con políticas y procedimientos acerca de cómo gestionar la información**
5. **Contar con un equipo interdisciplinar. Es decir, las organizaciones requieren de un equipo de respuesta en diferentes áreas para afrontar un ciberataque.**

A partir de la comprensión de la importancia de tener un protocolo acerca de la gestión de la información y ante una situación de ciberataque, Roberto Lemaitre Picado (2022), experto en derecho informático y coordinador de incidentes

Informáticos del MICITT aporta al concepto de ciberataque, partiendo desde la diferencia conceptual que existe entre un ataque y un incidente:

Un incidente no implica un ataque, normalmente cualquier ataque es un incidente, pero no implica un ataque. Las organizaciones, empresas e instituciones siempre van a tener incidentes, pero no todo es un ataque. Un ataque

va a implicar que todo es una acción dirigida contra el individuo contra su empresa, contra sus plataformas, para afectarlos directamente o alguna situación que afecte los principios de continuidad, disponibilidad e integridad de los servicios.

Desde el punto de vista del sector privado Edwin Meza Sánchez (2022), experto en Ciberseguridad menciona que "la ciberseguridad responde al sin número de amenazas que están presentes en múltiples industrias, las cuales representan una amenaza latente y concreta.

Además, agrega la consigna de "como mitigar el riesgo y como hacer la mayor cantidad de esfuerzo en diferentes aristas para manejarlo ya que este nunca se va a ir por completo, el riesgo siempre existe"

Por otro lado, aunando a la materia de Ciberseguridad en Costa Rica, Lemaitre (2022) hace referencia acerca de los avances que ha tenido en materia de Ciberseguridad en los últimos años a partir de la elaboración de la primera Estrategia Nacional de Ciberseguridad, elaborada con cooperación internacional de la Organización de Estados Americanos (OEA), sector privado, sector público, la académica y la sociedad civil.

A partir de la creación en de la Estrategia 2018-2021 en el 2017 por parte del Viceministerio de Telecomunicaciones de Costa Rica, se ha impulsado, desde el área de Ciencia y Tecnología, a trabajar en la creación y cumplimientos de los objetivos planteados, por lo que se han generado diversos trabajos de concientización, capacitación y formación (Lemaitre, Digital Time 2022)

Agrega que a partir de ese trabajo colaborativo entre los diferentes sectores se ha creado una red de colaboración en materia de Ciberseguridad con más de 330 instituciones del país, y se ha logrado fortalecer la relación con diferentes sectores. Además, citó que Costa Rica en el Security Índex mejoró 39 lugares con respecto del año 2021, siendo el octavo país de América Latina y el número 76 a nivel mundial.

Respecto al avance marco jurídico, el expositor menciona que Costa Rica cuenta con uno de los más desarrollados en el área de tecnología y qué es de suma importancia conocer, para lo cual cita la siguiente lista de leyes, marcos y normas vinculados a la Ciberseguridad:

- El marco de delitos informáticos
- Las leyes acerca de la Protección de Datos
- La ley de firma digital donde se regula el tema de firma digital certificada y el efecto legal que tiene ese medio tecnológico frente este a temas legales
- Marcos legales de protección de menores en Internet
- Derechos de autor y propiedad intelectual, derechos de autor.
- Marco Normativo de leyes de telecomunicaciones,
- Las normas técnicas en materia de

tecnologías de la información

De acuerdo con lo anterior, se puede concluir que Costa Rica tiene un Marco Jurídico actualizado respecto a las tecnologías de la información, el cual debe ser conocido y tratado en el sector tecnológico, ya que es un tema trasversal en cual ámbito de la sociedad.

A pesar de los retos y aspectos por mejorar de acuerdo con estándares a nivel nacional y las mediciones internacionales, según Lemaitre (2022) Costa Rica "un país más ciberseguro atrae más inversión, y esta atrae más puestos de trabajo para las áreas de tecnología, y a su vez más pymes, más inversiones y proyectos que se requiera generar en materia de tecnología".

Otros retos mencionados por Lemaitre (2022), fue acerca de la necesidad de mejorar la investigación del cibercrimen, el cual ha sido fundamentado en el Convenio de Ciberdelincuencia, conocida como Convención de Vida ratificado por Costa Rica, debido a que se considera que se debe optimizar sus implementaciones porque permite la cooperación internacional y la eficacia al compartir información entre países.

Añadiendo, a las mejoras que se deben realizar Meza (2022) hace referencia a los mecanismos para la identificación y protección de infraestructuras críticas a nivel país, por lo que comenta acerca del concepto de *ransomware,* como "un dispositivo malicioso que viene y se encripta en los discos duros o dispositivos de almacenamiento", los cuales puedengenerar incidentes en las funcionalidad de las empresas, por lo tanto, indica que se debe identificar y mejorar las infraestructuras críticas del país.

De igual manera, Lemaitre (2022) añade que dentro de los esfuerzos realizados desde el MICITT se han reforzado y mejorado las infraestructuras críticas a partir de las mediciones internacionales.

También hace referencia acerca de los avances y crecimientos de las diferentes industrias, aunque hay gran necesidad profesional en diferentes áreas de la ciberseguridad, tales como la ciberseguridad tradicional y la ciberseguridad industrial. El expositor conceptualiza de la siguiente manera:

Respecto de la ciberseguridad tradicional, esta se relaciona directamente con los equipos, computadoras, equipos de servicios relacionados, es decir con la infraestructura de tecnología de una empresa tradicional. Mientras que la ciberseguridad industrial se vincula a las diferentes infraestructuras críticas, infraestructura de sistemas, sistemas de controladores de sistemas eléctricos que permiten el monitoreo, registro, atención en línea de todos estos sistemas controladores, apertura de equipos, represas, puertas, entre otras. (Lemaitre, 2022)

Además, el expositor indica que la ciberseguridad compete a todas las personas de las organizaciones, no únicamente al departamento de Tecnología, citó el informe del *Global Risk del World Economic Forum,* que indica que el 95% de los incidentes en el mundo ocurren

por un factor humano, y la importancia de hacer cultura digital.

En cuanto a principales ataques e incidentes, Meza (2022) propone que estos van a dependerdel tipo de objetivo desde el punto de vista del atacante, a partir de ahí se implementan las diversas técnicas que se usan para generar vulnerabilidad y atacar. Por lo tanto, es prioritarioidentificar el sistema al que se está atacando, ya que los atacantes suelen usar estrategias predatorias. Asimismo, menciona que el concepto de Ingeniería Social dentro del campo de la ciberseguridad consiste en:

Una serie de técnicas y trampas para lograr que una persona entregue o divulgue información que no está autorizada a brindar, siendo el primer paso en la cadena de acciones que terminando lleva a un incidente de vulnerabilidad, es decir ataques de ingeniería social que buscan vulnerar a las personas para obtener una afectación de manera inmediata.

Sumando al concepto de ingeniería social, Andrade (2022) propone que esta busca vulnerar una parte del proceso del algún producto de alguna organización, ya que el ciber delincuente es capaz de estudiar cuál es el funcionamiento específico de una aplicación móvil para hallar la vulnerabilidad y eso lo aprovecha utilizando mecanismos técnicos.

Añade que, uno de los ataques mencionados es acerca del *Fishing.* Este es el acto mismo de un ciber atacante, tratando de impresionar algún tipo de canal legítimo con el fin de engañar. Consiste en que la víctima entregue la información de carácter confidencial y privada, siendouno de los ataques más usados durante la pandemia.

Por lo tanto, hace las siguientes recomendaciones respecto a las principales prácticas que sedeben considerar en materia de ciberseguridad en los dispositivos personales para evitar algún tipo de ataque o engaño:

- **Utilizar un antivirus especializado en dispositivos móviles**
- **Vigilar la interacción de los dispositives**
- **Tener métodos para la gestión de contraseñas**
- **No utilizar los datos personales con los dispositivos y cuentas de los equipos empresariales**
- **Hacer uso de la nube para respaldar información y datos**
- **Tener diferentes formas de respaldar la información**
- **Leer cuidadosamente los términos y condiciones de las aplicaciones**

La ciberseguridad es una práctica tecnológica que tiene incidencia en el uso de otras tecnologías 4.0, una de ella es acerca del Internet de las Cosas, lo que implica un enorme retodebido a la cantidad de información y dispositivos conectados dado al gran crecimiento del uso de esta en diferentes sectores económicos y sociales.

Ante lo expuesto, se deja en manifiesto la necesidad de fomentar una cultura del uso correcto de las tecnologías de la información tanto a nivel personal como en las empresas a pesar de las limitaciones de los recursos con los que cuentan. Respecto a esto, Meza (2022) hace referencia que el uso de los recursos va a depender de la disposición de la empresa para prevenir, corregir y mitigar los riesgos en los posibles ataques.

Por su parte, Andrade (2022) menciona que, es vital capacitar y sensibilizar a las personas sobre la importancia del manejo de la información y la protección de los datos, y realizar acciones de concientización al colaborador dentro de una empresa sobre la responsabilidad legal y económica, así mismo, las políticas y procedimiento deben estar claros para los empleados.

Igualmente, Lemaitre (2022) menciona que, Costa Rica debe considerar los modelos de protección de ciberseguridad que se apliquen, tanto en las industrias, como en el sector público, señalando que los principales retos son oportunidades para la implementación de un modelo de gestión de riesgos que vayan de acuerdo con las necesidades específicas.

El expositor hace énfasis a tres grandes retos, que son, generar una cultura desde el área de ingeniería, la clasificación de datos, y establecer las políticas de gestión en materia de datospersonales y datos en general, así como la identificación de los riesgos reales. Respecto de las oportunidades, menciona que, "la información es poder y la información y el conocimiento es garantía y es un seguro", por lo tanto, es necesario compartir con otras personas, prácticas y acciones de cómo mejorar y gestionar la seguridad de la información personal.

Acerca del escenario actual, Bustillos (2022) menciona que en Costa Rica ha aumentado la necesidad de contratar a especialistas en ciberseguridad, y la dificultad de encontrar perfilesespecíficos que apoyen esta área.

Añadiendo, Andrade (2022) hace un acercamiento acerca del perfil de cuáles serían algunoshabilidades y competencias que se debe considerar para un ingeniero en ciberseguridad con los siguientes puntos:

- **Conocimiento en la parte técnica**
- **Capacidad de desarrollo de software**
- **Contar con certificaciones de los diferentes estándares**
- **Que cuente con un título académico**
- **Ética y buena moral**
- **Capacidad resiliente**

Bustillos (2022) menciona que, de acuerdo con los datos proporcionados por Fortinet, líder mundial en soluciones de ciberseguridad, Costa Rica sufrió más de 2500 millones de intentos de ciberataques en el 2021, y menciona que el escenario actual exige que una de una persona graduada en el área de tecnología ya debe cambiar por lo que la academia tiene un papel protagónico para apoyar y proponer soluciones que permitan el desarrollo de Costa Rica.

Andrade (2022) agrega que la Academia debe desarrollar habilidades, tanto técnicas como blandas que respondan a las necesidades de la industria como lo son la resolución de conflictos, análisis e investigación, e incluir dentro de los contenidos de los cursos las nuevastendencias tecnológicas y metodologías prácticas.

Respecto a esto, Lemaitre (2022) indica que "indiscutiblemente la universidad tiene un enorme reto de responsabilidad de formar profesionales que respondan a las necesidades delpaís" y debe hacerse una revisión constante de a la malla curricular, pero que también los docentes estén actualizados.

Por último, Meza (2022) agrega que la academia debe desarrollar sus contenidos en función de que el estudiante pueda tener contacto y práctica con la realidad y las últimas tendencias, ya que la actualización hace la diferencia.

La ciberseguridad es un área transversal que compete a diversos sectores de la sociedad, porlo tanto, es necesario que desde la Academia se desarrollen espacios para dialogar y reflexionar acerca de la importancia de este tema, ya que esto aporta a la formación en los estudiantes, y a la actualización de los docentes, porque son quienes están guiando los procesos educativos dentro de las aulas; esto con el fin de entender el contexto nacional e internacional en cuanto a las necesidades de la industria y el impacto que ha tenido la aceleración tecnológica en los últimos años.

CONCLUSIONES

El Digital Time reunió a expertos en la disciplina para dialogar, reflexionar y exponer, a través de las diferentes prácticas aplicadas hasta el momento, sobre un tema trascendental como es la Ciberseguridad en Costa Rica

Costa Rica ha avanzado en diversos aspectos tanto a nivel público y privado, mediante la adopción de una serie de acciones que han permitido que las instituciones y organizaciones puedan apoyarse para minimizar el impacto de un incidente informático o un ciberataque.

Desde el Gobierno de Costa Rica, se ha buscado mejorar los mecanismos y procedimientos para afrontar los nuevos delitos, el uso de la información y las consecuencias del aumento de la navegación del internet en la sociedad, a través de la construcción de un marco jurídico actualizado y robusto que ha fortalecido las prácticas a nivel institucional.

Asimismo, se indicaron una serie de protocolos y medidas para enfrentar un ataque, tanto a nivel personal, empresarial e institucional que deben ser considerados, ya que ha existido un aumento de la exposición de los datos personales y organizacionales en las diferentes transacciones de las dinámicas sociales, económicas y culturales en los últimos años.

A nivel país, se han implementado una serie de acciones a través de la Estrategia Nacional de Ciberseguridad establecidos por el MICITT. Esto permite direccionar en una misma línea los diferentes mecanismos, procesos y protocolos que las empresas e instituciones deben

implementar para responder a las necesidades de caracter tecnológico.

En el escenario actual, ha aumentado la necesidad de contratar a especialistas en Ciberseguridad debido a la transformación digital y al uso exponencial del internet, por lo tanto, las universidades tienen un papel protagónico en la formación de nuevos perfiles profesionales que estén preparados, no solamente con habilidades técnicas, sino también conlas habilidades blandas necesarias para responder al entorno económico, cultural y social queestá en constante cambio.

A partir de la creación de estos espacios por parte de la Escuela de Ingeniería Informática de la UIA, se pretende informar, actualizar y apoyar la formación de los estudiantes en su carrera profesional, brindándoles un acercamiento con las últimas tendencias tecnológicas.

BIBLIOGRAFÍA

Ministerio de Ciencia, Tecnología y Telecomunicaciones (2017). *Estrategia Nacional de Ciberseguridad de Costa Rica.* https://www.micitt.go.cr/sites/default/files/estrategia- nacional-de-ciberseguridad-costa-rica-19-10-17.pdf.

Equipo editorial de la revista Innovación Universitaria:

Bach. Carlos Ulate Lobo-Editor
Colaborador del Departamento de Investigación e Innovación UIA

Licda. Fernanda Segura Calderón
Colaboradora del Departamento de Investigación e Innovación UIA

Correo: revistainnovacionu@uia.ac.cr