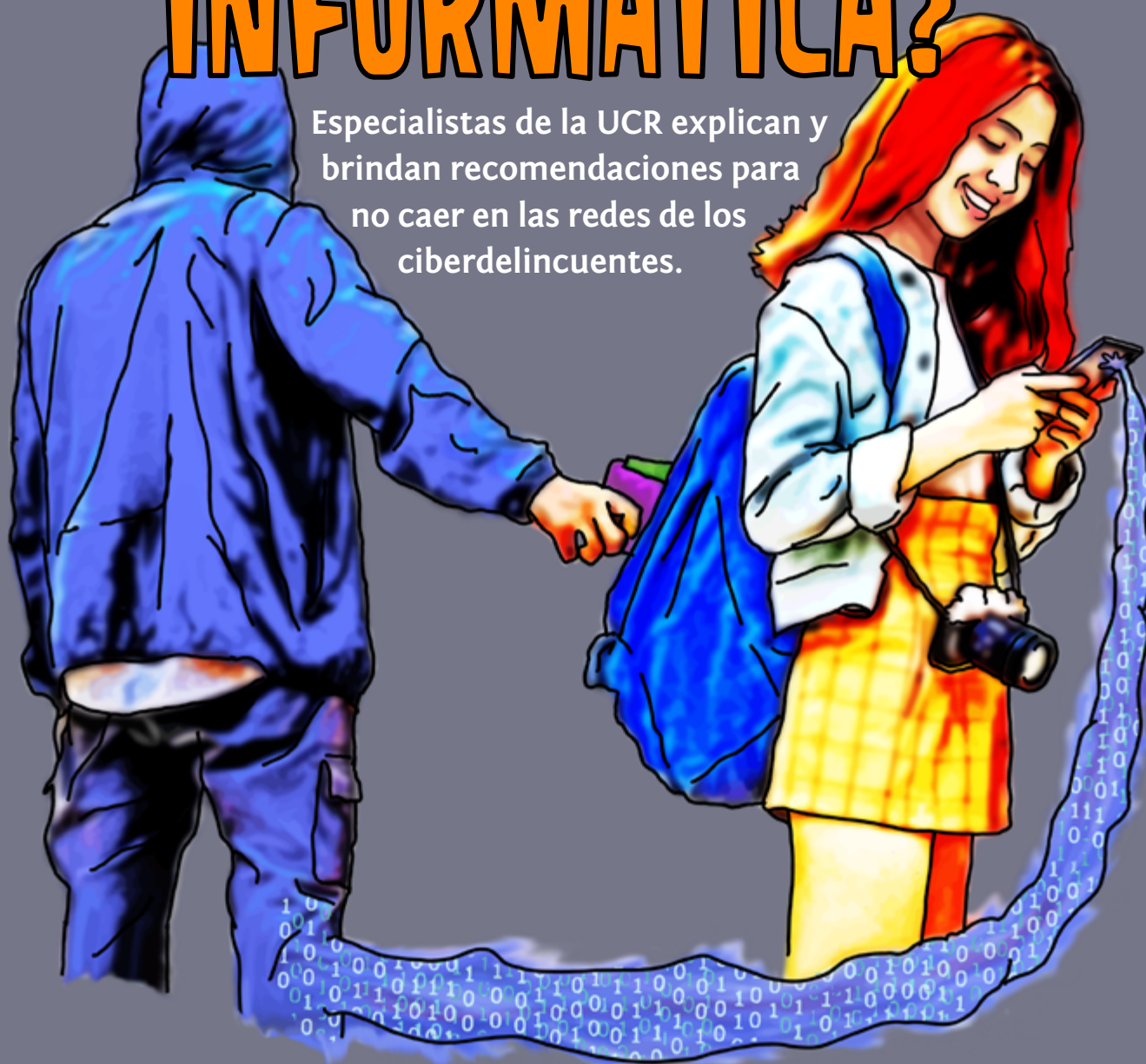


¿QUÉ HACER PARA EVITAR UNA ESTAFA INFORMÁTICA?

Especialistas de la UCR explican y brindan recomendaciones para no caer en las redes de los ciberdelincuentes.

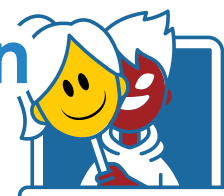




En las estafas informáticas median, por lo general, factores humanos. Por esto, debemos desarrollar mucha malicia digital para no caer en el engaño de las redes dedicadas a este negocio. Foto: Laura Rodríguez.



Con una mejor cultura digital disminuyen los riesgos de una estafa informática



La mayoría de los casos de los delitos informáticos ocurren por factores humanos mediante técnicas de ingeniería social.

Patricia Blanco Picado
patricia.blancopicado@ucr.ac.cr

Isabel se encontraba esa mañana en su casa atendiendo a unos trabajadores de la construcción cuando sonó su teléfono celular.

—Buenos días, señora. Le hablamos de parte del Banco Continental para informarle que hay un problema con su cuenta, el cual debe ser resuelto lo antes posible.

—¿Y cuál será el problema? Es que en este momento estoy ocupada y no puedo atenderlo.

—No le vamos a quitar mucho tiempo, es rápido y es muy importante para usted porque su cuenta corre peligro, en cualquier momento le podrían sustraer el dinero.

—Este... es que como le dije, en este momento estoy ocupada. ¿Podría llamarme más tarde?

—Es que esto es urgente, son solo un par de minutos. Usted no tiene que hacer nada, nada más le mandamos un enlace por WhatsApp y usted le da clic. Con solo eso nosotros corregimos de inmediato el problema técnico.

La historia de Isabel, aunque ficticia, no tuvo un final feliz. Todos los días se repite y es similar a la de muchas personas que son víctimas de los fraudes informáticos por medio de una llamada telefónica, un correo electrónico, el hackeo de su perfil

de Facebook o de su información personal por medio de una red no segura de wifi.

Este fenómeno está presente en todo el país. Aunque las provincias del Área Metropolitana son las que reportan más casos, ya se presentan denuncias en Guanacaste, Puntarenas y Limón.

Todo esto ocurre en un abrir y cerrar de ojos, sin que nos percatemos de que estamos siendo estafados. Es, posteriormente, cuando nos damos cuenta de que caímos en las estratagemas de los grupos de ciberdelincuentes dedicados a dicho negocio.

El *vishing* es un tipo de fraude por medio de llamadas telefónicas, en las cuales el atacante suplanta la identidad de una institución, empresa o persona con el propósito de obtener información personal de la víctima. Es lo que le ocurrió a Isabel,

quien creyó que realmente la contactaban del banco en donde ella guardaba su dinero.

Al hacer ella clic en un enlace, instalan un *software* de gestión remota para ver el contenido de una cuenta bancaria y luego capturar la información.

El artículo 217 bis del Código Penal costarricense establece una pena de tres a seis años de prisión por el delito de estafa informática. La sanción será de cinco a diez años de prisión si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras o si el autor del fraude es una persona encargada de administrar o dar soporte a un sistema o red informática.

De acuerdo con el Foro Económico Mundial, el 95 % de los delitos e incidentes



Las personas son el blanco principal de las técnicas de manipulación (conocidas como ingeniería social) que los atacantes usan para engañar a las personas y obtener información confidencial. Foto: Laura Rodríguez.

informáticos ocurren por factores humanos; es decir, “el ser humano es el punto donde se focaliza toda la energía del ataque”, explica el Ing. Abel Brenes Arce, oficial de seguridad de la información (CISO, por sus siglas en inglés) de la Universidad de Costa Rica (UCR).

Las diferentes técnicas de manipulación que usan los ciberdelincuentes para engañar a los usuarios y obtener información confidencial es lo que se conoce como ingeniería social.

¿Por qué este acercamiento hacia el usuario? Brenes considera que los ciudadanos no son conscientes de la cantidad de información que manejan y de la importancia de resguardarla. Nos referimos a claves, acceso a sistemas informáticos, datos confidenciales personales o de su lugar de trabajo, por ejemplo.

Se busca atacar a las personas que usan los sistemas informáticos para obtener información valiosa de ellos. Por tanto, no hay en primera instancia un ataque directo a las máquinas, sino que este se efectúa de forma indirecta.

En palabras del ingeniero informático y abogado especialista en ciberseguridad Roberto Lemaitre Picado, profesor de la Escuela de Ciencias de la Computación e Informática de la UCR, “nuestro sistema operativo humano es muy vulnerable”.

Los cibercriminales se aprovechan de la condición humana, desde quienes quieren ayudar a otros o creen mediante

engaño que ganaron un premio sin haber participado en ninguna actividad, hasta las personas que dan por cierta una herencia que no esperaban.

“Los atacantes son depredadores del comportamiento y de las emociones humanas”, complementa Brenes.

Métodos sofisticados

Lemaitre confirma que el cibercrimen no ha dejado de avanzar. La pandemia por el COVID-19 marcó un antes y un después en este tipo de acciones, ya que muchos criminales tradicionales evolucionaron hacia actividades más sofisticadas.

De hecho, durante ese período de emergencia sanitaria disminuyeron los asaltos físicos a las personas y aumentaron los ataques por medios informáticos.

Con la inteligencia artificial, los ciberataques han aumentado y las capacidades de los delincuentes también se han fortalecido para acceder a dichos recursos tecnológicos.

Este campo de la informática permite mejorar los mensajes para que parezcan más reales y cada vez es más difícil identificar las fuentes de la estafa, puntualizan los expertos.

“El *phishing* —indica Lemaitre—, que se usa mucho para estafas informáticas, inicialmente era muy difundido, mal redactado y con temas poco precisos. Ahora ha

mejorado y se ha venido especializando”.

Esta técnica de ingeniería social se dirige a ciertos segmentos de la población, entre estos los adultos mayores, pues se aprovechan del desconocimiento del uso de la tecnología debido a la brecha digital.

También buscan información en las redes sociales y en internet de ciertas personas de su interés, ya sea por las características de su perfil, su trabajo o su condición económica.

Brenes detalla que existen tres fases en la estrategia de los fraudes informáticos. La primera fase es la recolección de la información de la víctima.

“Los ciberdelincuentes hacen previamente una investigación de la persona, principalmente en las redes sociales, y empiezan así a planificar el ataque. Entonces disponen de mucha información, lo que lleva a pensar que el mensaje es legítimo”, afirma.

Luego viene la fase de adquirir confianza con la persona a través de llamadas telefónicas, mensajes por las redes sociales y correos electrónicos, con el fin de construir una relación armoniosa.

En la tercera fase empieza la manipulación que al ciberdelincuente le interesa para obtener cierta información más específica y así llegar al dinero.

“La salida consiste en irse sin dejar pruebas y con el objetivo satisfecho. Es tratar de que no les den seguimiento”, finaliza.

Más cultura digital

El director del Organismo de Investigación Judicial (OIJ), Randall Zúñiga López, reveló al periódico *La República* que, del 2017 al año en curso, el monto de las estafas informáticas se triplicó en el país, al pasar de 4 000 millones de colones a 12 000 millones de colones.

Los expertos de la UCR enfatizan en la necesidad de que haya mayor responsabilidad y cultura digital por parte de la ciudadanía, para que esta adquiera conciencia sobre el valor de la información que maneja y cómo protegerse de los cibercriminales.

Brenes recuerda que uno como ciudadano digital debe ser responsable y cuidar la huella. “Todo lo que hacemos en internet no es privado, la información sobre nuestros movimientos en la red es recolectada por los sistemas de trazabilidad”, aclara.

Para Lemaitre, se debe apostar a una formación sobre cultura digital muy fuerte en todos los niveles etarios, desde la niñez, para que los usuarios estén mejor preparados sobre el uso y funcionamiento de la tecnología y el accionar de estos grupos criminales.

Las estrategias nacionales de ciberseguridad deben incluir la creación de

[Continúa en la página 4](#)



Como usuaria de la tecnología, la ciudadanía debe ser más responsable y consciente del valor de la información que maneja y cómo protegerse de los ciberdelincuentes. Foto: Laura Rodríguez.

programas de formación con énfasis en las poblaciones más vulnerables, manifiesta. En este momento, Costa Rica tiene dicha estrategia en período de consulta.

Las instituciones también deben tener mecanismos de seguridad tecnológica y toda una infraestructura que dé garantía de protección de sus sistemas informáticos y de la información que resguardan.

De acuerdo con Brenes, son muy importantes las campañas de educación y sensibilización en este sentido, para que las personas aprendan que la información es estratégica y tiene un gran valor institucional. “Es un proceso de recordación permanente”, recalca.

Reto global

Los grupos de cibercriminales actúan globalmente, como lo hace el crimen organizado en otros campos.

El internet no tiene límites, razón por la cual los países se enfrentan al reto de definir cuál debe ser la respuesta jurídica y técnica ante los fraudes informáticos.

En Latinoamérica, algunas naciones han venido avanzando en la atención de los delitos informáticos y en la creación de grupos especializados de atención de esta materia en los órganos de investigación judicial y policial.

El Convenio sobre Ciberdelincuencia, conocido como el Convenio de Budapest, fue firmado en 2001 y tiene como objetivo proteger a la sociedad contra el cibercrimen. Costa Rica es uno de los países firmantes de tal documento.

Lemaitre destaca la importancia de este instrumento para que los países miembros puedan colaborar en la investigación y persecución de estas faltas, los incorporen a sus marcos jurídicos y dispongan de equipos especializados que atiendan esta problemática.

Al ser un tema que trasciende las fronteras, se necesita mucha colaboración para poder investigar y conseguir en otro territorio la información que se requiere para entender cómo se cometió un delito y buscar a las personas responsables.

Sin embargo, aunque las normativas jurídicas son importantes, se deben

tener establecidas las buenas prácticas y estándares para el buen funcionamiento de la parte operativa. En esta materia, señala Lemaitre, nuestro país tiene una calificación baja.

“Esto implica que los marcos de seguridad nos permitan tener buenas prácticas en las organizaciones e instituciones, con protocolos adecuados y con formación para que los funcionarios tengan claro qué hacer. Esto baja el riesgo”, concluye el especialista. ■

Denuncias de estafas informáticas en el Organismo de Investigación Judicial (OIJ)

A octubre del 2023: **3 846 denuncias**

2022: **5 318 denuncias**

Patrones que se repiten en las denuncias sobre la forma en que los delincuentes abordan a las personas para estafarlas:

- Falso funcionario o funcionaria bancaria
- Falso funcionario gubernamental
- Falso funcionario municipal
- Falso empleador
- Página falsa en los buscadores de internet
- Phishing* (envío de correos electrónicos que suplantan la identidad de instituciones o empresas y solicitan información personal y bancaria al usuario)
- Venta o alquiler falso

Fuente: Organismo de Investigación Judicial (OIJ).

Consejos de ciberseguridad

- Desarrollar la malicia y la alerta digital para no caer en engaños.
 - Nunca atender una llamada telefónica cuando le dicen que procede de un banco. Cuelgue y llame usted al banco.
 - No brindar datos personales a desconocidos.
 - Evitar conectarse a una red desconocida. Y si lo hace, se recomienda tener en el teléfono o en la computadora un *software* antivirus y anti *malware* que le permita crear una red privada virtual (VPN).
 - No abrir correos de usuarios desconocidos y revisar la procedencia del mensaje.
 - Verificar la seguridad de los sitios web.
 - No compartir contraseñas.
 - Verificar la identidad de la persona con quien se está hablando.
 - Mantener el equipo informático actualizado.
 - Tener doble autenticación en las cuentas personales.
 - Conectarse desde la casa por medio de una VPN.
 - No apresurarse a darle clic a los enlaces. Tener precaución y revisar primero el enlace. Se debe copiar a mano para validar el mensaje.
 - Capacitarse para entender cómo funciona la tecnología, por ejemplo, un teléfono celular o una computadora y sobre cuáles medidas de seguridad debo tomar.
- Fuentes: Roberto Lemaitre y Abel Brenes, expertos en ciberseguridad de la UCR.



La propuesta de la Sede del Pacífico de la UCR pretende contribuir a dinamizar la actividad económica de Puntarenas. Foto: cortesía de María Teresa Jiménez.



Con códigos QR se impulsarán los negocios del cantón central de Puntarenas



La investigación es liderada por la Sede del Pacífico de la UCR.

Fabrizio Rosales López
fabrizio.rosaleslopez@ucr.ac.cr

Con el propósito de potenciar la tecnología y la economía de la ciudad de Puntarenas, nació el proyecto Códigos QR para promover la interacción entre empresas y consumidores, promocionar productos y generar oportunidades de negocio.

La investigación también busca fomentar la identidad y el sentido de pertenencia con la comunidad puntarenense.

El 28 de setiembre pasado, Puntarenas recibió el Código QR Destino Turístico Inteligente, creado por la Ing. María Teresa Jiménez Ramírez, docente e investigadora de la Sede del Pacífico de la Universidad de Costa Rica (UCR).

El lanzamiento de esta iniciativa contó con la presencia del ministro de Turismo, William Rodríguez López, y de representantes de la Cámara de Turismo de Puntarenas (Catup).

Para la Ing. Jiménez, el cantón central de Puntarenas tiene mucho potencial que

aún no se ha explotado, ya que la provincia cuenta con los recursos, facilidades e infraestructura para innovar en la región.

“Yo soy del puerto y siempre he querido potenciar todo lo que Puntarenas tiene”, dijo la investigadora, principalmente ante la imagen negativa que se promueve en el resto del país de la ciudad de Puntarenas y que la economía local gira únicamente en torno al turismo.

“Con Códigos QR —argumentó— estamos sentando las bases para un futuro más conectado, no es solo un proyecto tecnológico, sino una manifestación tangible a nuestra dedicación e impulso local, con un futuro más brillante y conectado”.

El proyecto de investigación se encuentra inscrito en la Sede del Pacífico. Este se inició a principios del 2023 con la búsqueda de organizaciones locales de diversa índole, de sectores como turismo, hotelería, cultura, gastronomía, comercio, iglesias y transportes, entre otros.

Actualmente, esta iniciativa se encuentra en su primera fase de desarrollo. Alrededor de 130 empresas están afiliadas.

Jiménez tiene, además, otros proyectos futuros en los que aprovecha la tecnología,

como la realidad aumentada, para dar a conocer el valor del patrimonio histórico de la ciudad de Puntarenas.

“Todo esto apunta a que Puntarenas sea realmente una ciudad inteligente”, añadió.

Por otra parte, en representación de la dirección de la Sede del Pacífico, Maureen Manley Baeza, recalcó que “esta investigación es un testimonio del compromiso de la Universidad con la comunidad, estamos aquí para demostrar que el conocimiento académico puede ser una fuerza para el campo positivo de la sociedad y que Puntarenas tiene el potencial para convertirse en un destino turístico inteligente”.

Alianza estratégica con el fútbol

La Sede del Pacífico de la UCR y el Puntarenas Fútbol Club (PFC) llevaron a cabo el acto simbólico de darse la mano para sellar un acuerdo de colaboración. Esta alianza entre ambas instituciones conlleva el respaldo y el compromiso con

el proyecto de Códigos QR en Puntarenas.

Jean Carlo Bonilla Montero, representante legal del PFC, destacó este acuerdo con la UCR con el fin de contribuir al desarrollo de la provincia de Puntarenas.

“Cualquier institución se llena de orgullo de trabajar con la UCR. Es importante crear esta alianza para aportar a nuestro cantón”, dijo Bonilla.

Jiménez resaltó el apoyo del PFC al proyecto sobre los códigos QR en Puntarenas y la importancia de que esa organización se haya unido a la investigación.

“El apoyo inquebrantable del PFC ha sido esencial para el avance de este proyecto. Puntarenas reconoció el potencial de este trabajo para fortalecer los lazos entre la academia y la industria local”, detalló la coordinadora de la iniciativa.

El Puntarenas Fútbol Club ha colaborado con la participación de algunos jugadores en videos para las redes sociales, en los cuales invitan a la comunidad puntarenense a que formen parte de la plataforma tecnológica.

Continúa en la página 6



Al ingresar al sitio web desde el código QR, las personas encontrarán actividades y comercios del cantón central de Puntarenas. Foto: cortesía de María Teresa Jiménez.

Con el apretón de manos entre Maureen Manley Baeza, en representación de la UCR, y Jeancarlo Bonilla Montero, del PFC, las instituciones dieron su apoyo al proyecto de investigación.

¿Qué podemos esperar?

El objetivo del proyecto Códigos QR es hacer de la provincia de Puntarenas la primera ciudad inteligente de Costa Rica,

según comentó la responsable de la investigación. Se espera que al finalizar el 2023, la iniciativa cuente con más de 500 comercios asociados a la plataforma, mencionó la Ing. Jiménez. ■

¿Cómo puede inscribirse a este proyecto?

El servicio es gratuito y cualquier comercio puede inscribirse en él. Los negocios deben acceder a las redes sociales de Puntarenas 4.0 y llenar el formulario en línea que se encuentra en la página. También pueden ingresar directamente desde el siguiente enlace:



- Contactos:**
- Facebook: Puntarenas 4.0
 - Instagram: Puntarenas 4.0
 - Correo: maria.jimenezramirez@ucr.ac.cr



La provincia de Puntarenas es la primera en el país en promover la reactivación económica mediante una herramienta tecnológica como los códigos QR. Foto: cortesía de María Teresa Jiménez.



Uno de los 146 especímenes de la recopilación. Su nombre es *Learedius learedi* y es un helminto trematodo extraído del corazón de la tortuga verde (*Chelonia mydas*). Fotografía: Colección Helmintológica de Costa Rica.

Científicos recopilan, por primera vez en Costa Rica, 146 especies de parásitos de organismos marinos

La revisión permite que el país obtenga la base necesaria para nuevas investigaciones en el campo de la biología y de la salud.

Jennifer Jiménez Córdoba
jennifer.jimenezcordoba@ucr.ac.cr

Los biólogos Alberto Solano Barquero y Jorge Cortés Núñez, así como la microbióloga Alicia Rojas Araya, todos de la Universidad de Costa Rica (UCR), generaron un precedente científico sin igual al compilar, por primera vez en la historia, todo el conocimiento existente sobre los parásitos en ambientes marinos de nuestro país, en un único documento.

El estudio, que duró tres años y actualmente está publicado en la revista científica internacional *Parasitologia*, analizó más de 50 artículos publicados desde 1930 hasta el 2022, los cuales abordaban el reconocimiento o identificación de nuevos parásitos marinos en Costa Rica. El resultado obtenido fue impresionante.

Los tres profesionales encontraron que en Costa Rica se conoce un total de 146 especies que pertenecen a 113 géneros de cinco filos (grupo taxonómico mayor). Estos parásitos corresponden en su gran mayoría a helmintos —gusanos de varios tipos— y crustáceos parásitos encontrados en 61 especies hospedadoras.

Además, detectaron que, de ese grupo de 146 parásitos, 32 fueron reportados como especies nuevas descritas a partir del material recolectado en Costa Rica, tres fueron mencionadas como géneros totalmente nuevos (grupos de especies emparentadas) y 38 especies entraron en la categoría de informes inéditos (nunca antes vistos) para el Pacífico Tropical Oriental.

“Hasta donde nosotros conocemos, ningún otro país posee una recopilación comprehensiva de las especies parasitarias en ambientes marinos como esta que nosotros hicimos para una nación entera. Lo otro es que, justamente, al ser un estudio comprehensivo, no solo nos enfocamos en los parásitos helmintos —diversos grupos de gusanos—, sino también en otros

grupos de organismos parásitos, como crustáceos, que tienen especies que pueden parasitar a las especies marinas”, manifiesta el Dr. Solano.

El Dr. Cortés concuerda: “Con este estudio nos dimos cuenta de cuáles grupos habían sido estudiados, porque los parásitos pertenecen a muchos grupos diferentes. Entonces, nos interesaba ver cuáles grupos de parásitos habían sido estudiados y cuáles grupos de animales marinos eran parasitados. Encontramos que la gran mayoría de los trabajos eran solo con peces”.

Los más parasitados

¿Y cuáles animales marinos alojan a estos 146 parásitos? De acuerdo con Solano, por el momento se sabe que ese grupo se distribuye en 61 hospederos distintos, que varían desde peces óseos y tortugas marinas, hasta delfines e, incluso, elasmobranchios —tiburones y rayas—, principalmente.

Otros parásitos, eso sí en menor cantidad, fueron encontrados en cangrejos, camarones y langostas. La principal parte de ubicación en los organismos marinos fue en el tracto digestivo, seguido por el aparato respiratorio y la piel.

“De los miles de especies marinas de nuestro país (cuya extensión patrimonial es más mar que tierra), solo 61 se han investigado por la presencia de parásitos metazoos. La importancia de esta publicación es que por primera vez se establece un análisis histórico y una línea base de la cual partir, para empezar a impulsar la investigación de parásitos marinos como una línea permanente de estudio multidisciplinaria y multicéntrica”, destaca Solano.

Esa base que menciona el investigador es crucial. Solo con cimientos sólidos se puede generar nuevo conocimiento en diversidad de áreas y un ejemplo claro está en el campo de la biología marina.

Según el Dr. Jorge Cortés, al conocer

Continúa en la página 7



Los científicos implicados en el hallazgo son la Dra. Alicia Rojas, el Dr. Jorge Cortés y el Dr. Alberto Solano. Fotos: OCI-UCR.

los parásitos se puede comprender mejor cómo estos se relacionan con sus huéspedes. Esta relación podría funcionar como un potencial predictor sobre el estado de un ecosistema específico, qué tanta diversidad existe en ese ambiente, o bien, si una especie está modificando alguna conducta, está consumiendo a otras presas distintas a las esperadas y lo que implicaría dicho cambio en la biodiversidad marina.

“Es necesario saber qué tenemos. Costa Rica resalta mucho por su biodiversidad, pero esto es porque hay investigación científica. Esta es una forma muy clara de cómo la ciencia contribuye al desarrollo nacional. ¿Y dónde se hace? En las universidades públicas, la gran mayoría de la biología marina por la UCR y la UNA”, Dr. Jorge Cortés, biólogo marino.

Algo que nunca se debe olvidar, enfatizan los expertos, es que los parásitos, desde el punto de vista ecológico, ayudan

a controlar la cantidad de poblaciones de una especie. Por lo tanto, vigilar ese comportamiento es vital para la generación de alertas ambientales.

“Hace algunos años encontramos una publicación de un grupo de rayas que tenían parásitos. Entonces, podemos volver a buscar a esas rayas y ver si continúan con los mismos parásitos, si tienen más o menos y tratar de entender por qué es eso. Es decir, si es que se está deteriorando el ambiente y eso hace que estén siendo más parasitadas, o bien, lo contrario, que se ha reducido la presión y ahora hay una recuperación de la población. La única forma de saberlo es teniendo estos datos de línea base”, ejemplifica Cortés.

Otro de los aportes de este estudio base también estarían vinculados a la salud humana. Solano menciona que, al conocer y profundizar el conocimiento de los parásitos marinos, se podría identificar aquellos con potencial zoonótico; es decir, los que tienen la capacidad de enfermar al ser humano.

“Si sabemos que un pez que consumimos tiene algún parásito que haga que una persona se enferme, entonces podemos prevenirlo. De ahí la importancia de seguir investigando, porque este tipo de enfermedades zoonóticas se dan más que todo por el consumo accidental. Un ejemplo de esto son los nematodos (gusanos) *Anisakis*, que se han encontrado en peces

de Costa Rica. Este gusano ingresa en la carne del pescado o calamares y, si las personas no lo cocinan bien, les puede producir inflamaciones y hasta perforaciones en el intestino”, ahondó el biólogo.

Lo que viene

La investigación llena un vacío importante y pone en evidencia el gran potencial que todavía tiene Costa Rica por indagar.

El Dr. Solano dijo que, de las cerca de 1 760 especies de peces marinos que se conocen en Costa Rica, solamente se han muestreado 35 en busca de parásitos. Asimismo, de las casi 28 especies de cetáceos (ballenas y delfines, por ejemplo), únicamente se han estudiado cuatro con tal fin.

Además, de las 97 especies de tiburones, tan solo se han analizado tres y, de las rayas, que hay cerca de 53 reportadas en Costa Rica, al día de hoy solo a cinco se les ha estudiado la existencia de parásitos. Por lo tanto, la cantidad de parásitos aún por conocer es muy alta.

Solano comenta que la investigación sirvió para establecer un primer convenio internacional de investigación entre la Estación Zoológica Anton Dohrn, de Nápoles, y la Universidad de Tuscia, ambas en Italia, de la mano con el Centro de Investigación en Enfermedades Tropicales (CIET-UCR).

Este convenio se da por medio del Dr. Mario Santoro de Italia, que fue estudiante del Doctorado en Ciencias de la UCR. El convenio está en las últimas fases de formalización y permitirá colaboraciones muy importantes en esta área, recalcó el científico.

Si bien el convenio todavía está en proceso, ya se inició el monitoreo de los parásitos en algunos peces y tiburones costarricenses. En esta alianza, además de la UCR, participa el Instituto Costarricense de Pesca y Acuicultura (Incopesca), el Sistema Nacional de Áreas de Conservación (Sinac) y la Estación de Ciencias Marinas y Costeras (Ecmar), en Punta Morales, de la Universidad Nacional (UNA).

Esos muestreos preliminares ya arrojaron la presencia de muchas especies de parásitos conocidos en Costa Rica y que están alojadas en el tiburón *Alopias pelagicus* y, también, algunas especies no identificadas en peces y rayas.

“Muchas de esas muestras aún no las hemos terminado de identificar y es muy probable que varias sean especies nuevas para la ciencia. El material aún se está analizando morfológica y molecularmente, por lo que esperamos tener nuevos reportes y especies nuevas. Formalmente, iniciaremos en el 2024”, concluyen Solano y Cortés. ■