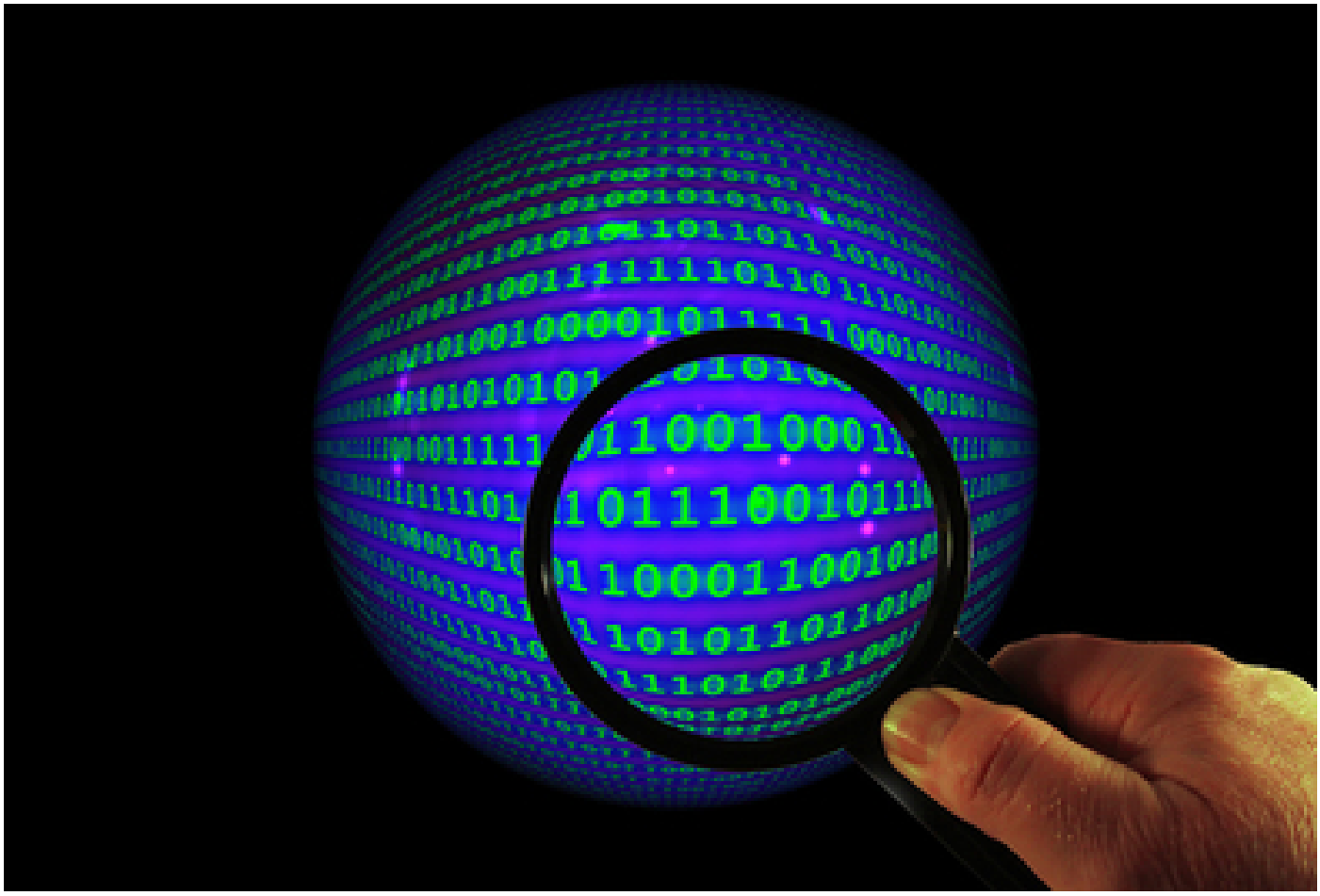
UNIVERSIDAD DE COSTA RICA

Ciencia más tecnología

Debemos navegar en internet a la defensiva

La seguridad informática no es un tema nuevo, pero en nuestro país no se le ha dado la importancia que amerita.

9 JUN 2022 Ciencia y Tecnología



Los especialistas concuerdan en que el desarrollo de la seguridad informática es aún incipiente en Costa Rica. Foto tomada de www.publicdomainpictures.net.

Desde hace varias décadas, la **seguridad informática es motivo de atención y preocupación** por parte de los especialistas de las **tecnologías de la información.**

Sin embargo, la alta dependencia tecnológica de nuestra sociedad actual, la globalización y la facilidad de acceso a las tecnologías de la información hacen que cada día tengamos mayores probabilidades de **sufrir ciberataques** en comparación con años atrás.

Actualmente, hay un **mayor uso de internet** por parte de toda la población, mediante una **gran cantidad de dispositivos**, desde computadoras y teléfonos celulares hasta cámaras y un sinfín de aplicaciones.

"**Es muy lógico que haya tantos ataques ante un mayor uso de internet en las actividades de la vida diaria**. Los que trabajamos en tecnologías de la información sabemos desde hace muchos años que estamos frente al ataque constante de grupos organizados", aseveró la Dra. Gabriela Barrantes Sliesarieva, profesora e investigadora de la Escuela de Ciencias de la Computación e Informática, de la Universidad de Costa Rica (UCR).

El 17 de mayo de este año, la Promotora de Comercio Exterior de Costa Rica (Procomer) presentó el estudio *Caracterización del uso y necesidades potenciales de ciberseguridad en empresas costarricenses*, en el cual se encuestó a 64 empresas demandantes de servicios de distintos sectores, sobre el mercado local en ciberseguridad. En el análisis se señala que **cada hora Costa Rica está expuesta, en promedio, a cerca de 22 945 ataques cibernéticos.**

LEA TAMBIÉN: Por el MTI Henry Lizano Mora, director del Centro de Informática de la UCR Voz experta: Taxonomía del malware, el caso Ransomware Conti

"No estamos navegando en este nuevo mundo a la defensiva, asumimos que las cosas siguen con las mismas reglas de antes. Suponemos que cualquier cosa en internet es segura y no lo es", enfatizó Barrantes.

De acuerdo con la especialista en seguridad informática, a esta área **no se le ha dado la importancia debida y no se ha actuado de manera defensiva**, tanto por parte de quienes desarrollan los *softwares*, como de los usuarios.

Diego González Villachica, coordinador del Capítulo de Ciberseguridad de la Cámara Costarricense de Tecnologías de Información y Comunicación (Camtic) y fundador de ŠTÍT Cybersecurity, concuerda con esta afirmación. Agrega que aun cuando se han hecho esfuerzos en los últimos años por educar a la población en el tema, este no ha tomado la suficiente fuerza debido a que **se suelen adoptar acciones una vez que sucede el incidente**, en vez de preverlo.

José Adalid Medrano Melara, abogado especialista en derecho informático y consultor internacional, expresó que **"la ciberseguridad no es algo que se pueda comprar, es un proceso que nunca termina"**. También explica que la capacitación y los *softwares* son importantes, pero que la continuidad de estos es esencial, así como la enseñanza y actualización constantes, tanto de los programas informáticos como del factor humano.

La Dra. Gabriela Barrantes, especialista en seguridad informática de la UCR, dijo que nuestro país “ha habido una interpretación muy ingenua sobre el manejo de los datos personales, pues todos están en sistemas informáticos abiertos". Karla Richmond

González considera que la ciberseguridad en Costa Rica tiene profesionales formados y con experiencia en el campo. Sin embargo, el país está en una etapa incipiente y necesita continuar avanzando y educándose en esta materia.

La seguridad en capas

Es imposible establecer una **seguridad informática absoluta**. Nunca se está completamente protegido contra posibles ataques. Lo que sí existen son diferentes grados de seguridad, al igual que se hace cuando se protege una casa con diversos recursos que se colocan para resguardar al inmueble. Se trata de una seguridad en capas que busca desestimular, en este caso, el robo de información.

Medrano comentó que, a nivel internacional, los especialistas recomiendan que las personas deben mantener la posición de “no es si me van a atacar, es cuándo me van a atacar” para poder **prevenir una acción de este tipo,** porque asegura que en la seguridad informática no se puede garantizar un cien por ciento de eficacia.

Los sistemas informáticos presentan distintas vulnerabilidades, por lo tanto, no existe una seguridad total frente a los ciberataques a los que los usuarios están expuestos de forma permanente, los cuales son realizados por organizaciones de delincuentes que operan en distintas partes del mundo.

LEA: La desatención de la **seguridad informática** podría amenazar el periodismo en Costa Rica

“Todos los sistemas informáticos están sujetos a ataques por **muchas motivaciones**, hoy en día son sobre todo **económicas**”, indicó Barrantes.

Según el estudio de la Procomer, **la mayoría de las empresas consideran el secuestro de datos (*ransomware*) como su mayor amenaza**. Este consiste en un *software* que impide utilizar el sistema que fue atacado hasta que se haya pagado la cantidad de dinero que se solicita a cambio. En el 2021, este fenómeno afectó al **66 % de las empresas del mundo**, confirma el estudio.

Todas las instituciones son diferentes y, por ende, su enfoque de seguridad varía. Pero hay organizaciones que manejan datos muy sensibles y, por lo tanto, tienen que invertir mucho más en seguridad informática, en congruencia con la **Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales** y su Reglamento (N.° 8968), la cual establece en el artículo 10 que los responsables de las bases de datos deben tener las medidas necesarias para garantizar la seguridad de la información de carácter personal y evitar su alteración.

Datos abiertos

Un tema relacionado con la seguridad informática son los **datos de la ciudadanía reunidos en sistemas informáticos abiertos**, los cuales en algunos casos no están lo suficientemente resguardados por las entidades responsables de su custodia.

Según argumentó Barrantes, **“la responsabilidad de proteger esta información es de quienes la custodian”**. En ese sentido, el país ha fallado, ya que “la mayoría de la gente no aprecia que esos datos que recoge son sensibles, que alguien se los puede robar, cortar el acceso, publicar o borrar. Falta una mentalidad defensiva”, advirtió la experta de la UCR.

La seguridad informática no se ha desarrollado lo suficiente en Costa Rica, debido a que se adoptan acciones una vez que sucede el incidente, aseguró Diego González Villachica, coordinador del Capítulo de Ciberseguridad de la Cámara Costarricense de Tecnologías de Información y Comunicación (Camtic).

Laura Rodríguez Rodríguez

Desde la perspectiva de los usuarios, Barrantes argumenta que en Costa Rica hay **demasiados datos en sistemas informáticos abiertos** y esto **pone en peligro nuestra privacidad.**

"Ha habido una interpretación muy ingenua sobre el manejo de los datos personales, todos están en sistemas abiertos. Eso violenta los derechos a la privacidad de todos los costarricenses", aseveró.

En otras partes del mundo, como Estados Unidos y Europa, la situación es diferente, allí hay muchas restricciones para dar a conocer información privada, por ejemplo, los salarios que ganan las personas. "En Europa, las leyes de seguridad están muy avanzadas y han logrado doblegar a gigantes globales como Facebook y Google", recordó.

Manifestó que, si bien actualmente hay una mayor demanda social de la transparencia del quehacer institucional, una cosa es el funcionamiento de las instituciones y otra son las personas. **"Como ciudadanos tenemos derecho a ciertas protecciones"**, advirtió.

En cuanto a las estafas a usuarios bancarios, la especialista destacó que falta legislación en el país para proteger a los tarjetahabientes y a otros usuarios de los servicios públicos.

"Falta educación informática para los usuarios, pero también nos falta legislación que obligue a los bancos a que aumenten las medidas de seguridad y se responsabilicen de la custodia de los datos de sus clientes", señaló.

Indicó, además, la importancia de que existan **organizaciones de la sociedad civil que defiendan los derechos a la privacidad**, pues, aunque hay una ley en ese sentido, la ciudadanía no sabe que existe y que la puede usar.

¿Quién me apoya a mí?

La ley que protege a las personas en relación con el manejo de sus datos tiene como objetivo darles la potestad de determinar por sí mismas el tratamiento de la información referente a su vida o actividad privada, que esté en bases de datos, tanto de organismos públicos como privados.

Sin embargo, González y Medrano consideran que **esta ley no se aplica en todas las empresas.** Asimismo, el experto en derecho informático agregó que la Agencia de Protección de Datos de los Habitantes (Prodhab) tampoco fiscaliza los incumplimientos de esta normativa.

Por otro lado, recientemente se creó en Costa Rica la Fundación Privacidad y Datos (Pridat), una organización sin fines de lucro, que tiene la misión de **proteger "los datos personales de los costarricenses"**, promover "una cultura de privacidad digital" e incidir en el diseño de políticas públicas que alineen al país con "la democracia y los derechos fundamentales".

A pesar de esto, Medrano concluye que **nuestra sociedad tiene mucho que mejorar en esta área.** "No es una sola institución a la que le falta cultura de derechos digitales, de respeto a

los derechos digitales y a la ciberseguridad, es un estado nacional de desinterés en esta materia", concluyó el experto en derecho informático.

Karol Quesada Noguera
Asistente de la Sección de Prensa de la Oficina de Divulgación e Información
karol.quesadanoguera@ucr.ac.cr

Patricia Blanco Picado
Periodista, Oficina de Divulgación e Información
Área de cobertura: ciencias básicas
patricia.blancopicado@ucr.ac.cr

Etiquetas: seguridad, informatica, ciberseguridad, escuela de ciencias de la computacion e informatica, ciberataques, #cmast, #c+t.