Ciberseguridad: Conocimiento imprescindible en un mundo digital

[1] CATALINA DURÁN. Universidad Latinoamericana de Ciencia y Tecnología, Costa Rica

Resumen

Sólo en el primer trimestre del año 2020 Costa Rica experimentó 32 millones de ataques cibernéticos subiendo en un 131% en comparación al mismo lapso del 2019. Lamentablemente, cada vez son más los costarricenses que caen en estas trampas, que pierden su privacidad y que muchas veces terminan perdiendo su dinero. La exposición al uso de la Web comienza en etapas tempranas donde desafortunadamente no existe la educación adecuada para estar preparados y así evitar ser víctimas de estos cibercriminales. Por eso, por medio de esta investigación, se indagó para encontrar respuesta a la pregunta ¿de qué manera se puede educar a la población costarricense en las mejores prácticas para prevenir el fraude cibernético? Se investigó cuáles son las mejores normas en seguridad cibernética a nivel global en los países más preparados y cuáles de ellas podrían ser aplicadas en Costa Rica. Además, al ser esta investigación de índole cuantitativa con enfoque exploratorio, se realizó una encuesta a 70 personas entre las edades de 17 y 45 años para entender su nivel de conocimiento del tema de acuerdo con cada generación y la educación recibida. Con base en el análisis de los resultados obtenidos y de la revisión bibliográfica realizada, se recomienda seguir las normas utilizadas por países como Finlandia, Dinamarca y Suecia que se enfocan en fortalecer la educación e investigación en niños y jóvenes, en la integración de programas de entrenamiento en educación vocacional y universidades, así como sensibilizar a los ciudadanos en general en cuanto a este tema. Asimismo, se formuló una propuesta para el Ministerio de Educación Pública de un manual que sería incluido en los colegios públicos del país como parte de las clases de informática, siendo la población colegial la beneficiada directamente ya que estarían adquiriendo conocimiento valioso desde temprana edad. Esto con el principal objetivo de generar un impacto positivo al crear conciencia sobre la ciberseguridad y lograr que el público meta tome acción con respecto a la problemática real y actual que representa el fraude cibernético.

Palabras clave

Ciberseguridad: La ciberseguridad es la práctica de defender computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques maliciosos.

Internet: Red informática global que consta de redes interconectadas que utilizan protocolos de comunicación estandarizados.

---

[1] **Catalina Durán Ramírez** es traductora y educadora, estudiante de la Maestría en Gerencia de Proyectos de la ULACIT, cuenta con cerca de 10 años de experiencia en el área de Mercadeo Digital en conjunto con manejo de personal; en los recientes 8 años se ha desempeñado como gerente, actualmente maneja un equipo de producción de campañas publicitarias para grandes clientes norteamericanos de manufactura como Nestlé, Pepsi, Kimberly Clark, Kellogg's, así como más de 40 clientes adicionales, generando más del 50% de las ganancias de la compañía. Email: cata.qwerty3@gmail.com

Privacidad: El estado o condición de estar libre de ser observado o perturbado por otras personas.

Educación Pública: Sistema nacional educativo de cada país, que está gestionado por la administración pública y sostenido con los impuestos.

Mejores prácticas: Procedimientos que se aceptan o prescriben como correctos o más eficaces.

Abstract

During the first quarter of 2020 Costa Rica experienced 32 million cyber-attacks, increasing by 131% compared to the same period during 2019. Unfortunately, more and more Costa Ricans fall into these traps, losing their privacy and often times losing their money. People are exposed to using the Web since the early stages of their lives where, unfortunately, there is no adequate education to get prepared and thus avoid being victims of cybercriminals. Therefore, this research was done to find an answer to the question *how can the Costa Rican population be educated in the best practices to prevent cyber fraud?* The research included finding the best cybersecurity standards at a global level in the most prepared countries and which ones could be applied in Costa Rica. Also, since this research is quantitative in nature with an exploratory approach, a survey was conducted to 70 people between the ages of 17 and 45 years old to understand their level of knowledge on this subject according to each generation and the education received. Based on the analysis of the results obtained and the bibliographic review carried out, it is recommended to follow the norms used by countries such as Finland, Denmark and Sweden. they focus on strengthening education and research in children and young people, on the integration of training programs in vocational education and universities, as well as sensitizing citizens in general regarding this issue. Moreover, a proposal was made to the Ministry of Public Education to include a cybersecurity training manual in the country's public schools as part of computer classes. High school students are benefited directly through this investigation and plan since they would be acquiring valuable knowledge from an early age. All the above with the main objective of causing a positive impact by raising awareness about cybersecurity and getting the target audience to act and avoid being part of the problem that cyber-fraud represents.

Keywords:

Cybersecurity: Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

Internet: A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.

Privacy: The state or condition of being free from being observed or disturbed by other people.

Public Education: National educational system of each country, which is managed by the public administration and supported by taxes.

Best practices: Procedures that are accepted or prescribed as being correct or most effective.

Introducción

Tal es la dependencia al Internet que el tema de la invasión de la privacidad y manipulación de los datos personales en la red pasa desapercibido; se ignoran los riesgos que existen cada vez que se ingresa a Internet. La Red se ha convertido en el centro de nuestras vidas, poco a poco todos los trámites de trabajo, vivienda, estudio, estética, compras y muchas otras actividades dejaron de hacerse de manera presencial y ahora prácticamente todo se puede gestionar por medio de Internet. Especialmente en los tiempos actuales de pandemia, el COVID-19 vino a acelerar la digitalización de cientos de trámites en este 2020.

El teléfono es hoy el centro de información que transita por las vías costarricenses y del mundo; tanto así que olvidarlo es quedar excluidos a no recibir noticias o sentirnos incomunicados. Esta dependencia ayuda a la a cibercriminalidad que se puede apropiar de datos, para venderlos o controlar directa o indirectamente nuestras vidas. Un ejemplo de esto sucedió el día 15 de julio del 2020 cuando fueron violentadas 130 cuentas de la red social Twitter, las personas atacadas son de alto perfil como Bill Gates y Barak Obama. El ataque se enfocó en robar la identidad de estas personas y colocar un mensaje pidiendo a los seguidores depositar bitcoins a una cuenta de criptomonedas específica prometiendo doblar la cantidad y devolverlo como un gesto de caridad (Sánchez, 2020) y, si esto les sucedió a ellos, le puede suceder a cualquier persona.

Cómo navegar la Internet de forma segura es información valiosa que debe ser accesible para todas las personas desde temprana edad para que puedan evitar ser víctimas y, a partir de esa problemática surge esta investigación. Existe una necesidad de compilar y compartir las mejores prácticas actualizadas de ciberseguridad de forma que la población, desde sus primeras experiencias navegando y puedan tener acceso a ellas, en este caso desde un aula o laboratorio estudiantil.

La investigación proporcionará conocimiento que será útil a la comunidad estudiantil de colegios públicos para mejorar su comprensión de las mejores prácticas para identificar cuando un sitio es seguro o cuando su información está en riesgo y cómo prevenir el fraude cibernético. Además, este trabajo es beneficioso para alcanzar a la población costarricense desde sus etapas tempranas y así hacer de su conocimiento tanto la problemática como la solución.

Asimismo, la investigación contribuye a actualizar los datos existentes sobre la cibercriminalidad y proponer la inclusión de un manual de seguridad con la posibilidad de ser actualizado de acuerdo con los avances tecnológicos que surjan, de manera que la información no se vuelva obsoleta. El COVID-19 ha incrementado la navegación en Internet de forma exponencial y desde una nueva perspectiva que nos trae otras estrategias de fraude que se deben investigar y documentar.

Pregunta de investigación

¿De qué manera se puede educar a la población costarricense en las mejores prácticas para prevenir el fraude cibernético?

Objetivo general de la investigación

Compilar las mejores prácticas sobre ciberseguridad para educar a la población colegial costarricense y así prevenir el fraude cibernético.

Objetivos específicos de la investigación

1. Evaluar cuáles son las mejores prácticas a nivel global para evitar el fraude cibernético.
2. Compilar las mejores normas aplicables a nuestro país.
3. Crear un manual de mejores prácticas de ciberseguridad para incluirlo en las clases de informática de los colegios públicos del país.
4. Formular una propuesta de implementación del manual para el Ministerio de Educación Pública (MEP).

Forma de alcanzar dichos objetivos

Aunque a la información tratada en esta investigación no se le haya dado la importancia que merece para ser transmitida a la población desde temprana edad en Costa Rica, sí hay información disponible en artículos de seguridad en la Web de sitios confiables como CrowdStrike, compañía de ciberseguridad que ha estado involucrada en la investigación de grandes fraudes cibernéticos, así como de empresas internacionales del sector privado, las cuales han creado cursos para sus empleados y los han facilitado en la red como Western Area Power Administration (WAPA), también recursos de diferentes gobiernos como los de Finlandia, Suecia y Dinamarca; además, será utilizado el juicio de expertos como el señor Pablo Garita, actual gerente de seguridad de la información en una compañía de mercadeo con trayectoria de más de 30 años a la que le es imperativo resguardar la información de su base de datos de la manera más segura posible, así como el señor Juan Pablo Elizondo, actual analista de seguridad de la información en una compañía de tecnología, ellos confirmarán la validez de la información. De estas fuentes se obtendrá el compilado de mejores prácticas en ciberseguridad.

Además, se investigará cuál es el procedimiento y los lineamientos aprobados por el Ministerio de Educación Pública de Costa Rica para formular la propuesta para la junta pertinente.

Marco teórico

En marzo del 2020, el escritor técnico, defensor de la privacidad y experto en redes virtuales privadas (VPNs) Paul Bischoff realizó un estudio sobre ciberseguridad a nivel global donde tomó 76 países como referencia (Bischoff, 2020).

Comentó Bischoff en su artículo *Which countries have the worst (and best) cybersecurity?* "Descubrimos que las puntuaciones de la mayoría de los países mejoraron desde el año pasado. Pero debido a los mayores esfuerzos de seguridad cibernética de la mayoría de los países, esto

significa que algunos de los que mejor se desempeñaron el año pasado han caído en la clasificación. Esto incluye a EE. UU., Que ha caído del quinto país más ciberseguro al 17" (Bischoff, 2020).

La imagen 1 muestra la clasificación de los países de acuerdo con que tan seguros son siendo 70 el mejor y 10 el peor.

Imagen 1
Cybersecurity Rankings by Country
Fuente: Comparitech, Bischoff, 2020.

Según este artículo de Bischoff, los países con mayor puntuación por categoría fueron:

- Mayor porcentaje de infecciones de malware móvil - Irán - 52,68% de los usuarios.
- Mayor número de ataques de malware financiero - Bielorrusia - 2,9% de los usuarios.
- Porcentaje más alto de infecciones de malware informático - Túnez - 23,26% de los usuarios.
- Mayor porcentaje de ataques de telnet (por país de origen) - China - 13,78%.
- Mayor porcentaje de ataques de criptomineros - Tayikistán - 7,9% de usuarios.
- Menos preparado para los ataques cibernéticos - Turkmenistán - 0,115.
- La peor legislación actualizada sobre ciberseguridad - Argelia - 1 categoría clave cubierta.

Los países con la puntuación más baja por categoría fueron de acuerdo con Bischoff (2020):

- Porcentaje más bajo de infecciones de malware móvil - **Finlandia** - 0,87% de los usuarios.
- Número más bajo de ataques de malware financiero: **Dinamarca, Irlanda y Suecia**: 0,1% de los usuarios.
- Porcentaje más bajo de infecciones de malware informático - **Dinamarca** - 3,15% de los usuarios.
- Porcentaje más bajo de ataques de telnet (por país de origen) - Turkmenistán - 0%.
- Porcentaje más bajo de ataques de criptomineros - Japón - 0.17% de usuarios.

- Mejor preparado para ataques cibernéticos - **Reino Unido** - puntuación de 0.931.
- La legislación más actualizada sobre ciberseguridad - **Francia, China, Rusia y Alemania** – tienen las siete categorías cubiertas.

Los países europeos son los considerados más seguros en cuanto a ciberseguridad; Finlandia, por ejemplo, aplica estrategias como la cooperación internacional, es parte de la Unión Europea y tiene un rol activo en las decisiones en cuanto a las normas de ciberseguridad, además se enfoca en fortalecer la educación y la investigación, considera que

> cada individuo es, por tanto, un importante actor que puede mejorar la seguridad cibernética a través de sus acciones a diario y por lo tanto, impactar su propia seguridad cibernética y la de otros". Para lograr la integración de la información de ciberseguridad crea programas de entrenamiento cibernético y la información de seguridad, desarrollo de software y aplicaciones, redes de información y telecomunicaciones en educación vocacional y universidades. (The Security Committee, 2019, p. 8)

En el caso de Dinamarca, el gobierno creó un plan de ciberseguridad que abarca del 2018 al 2021 que incluye, entre otros, los siguientes puntos:

- Mejorar el juicio digital y las habilidades digitales entre niños y jóvenes.
- Sensibilizar sobre la seguridad cibernética y de la información a ciudadanos, empresas y autoridades públicas.
- Apoyar la mejora continua del conocimiento especializado y la experiencia en el área.
- Apoyar los esfuerzos de seguridad cibernética y de la información en la comunidad empresarial. (The Danish Government, 2018, p. 28)

Por otra parte, Suecia emplea entre sus lineamientos mejorar las asociaciones entre las instituciones de educación superior, los institutos de investigación industrial y los sectores públicos y privados para aumentar la utilización y la innovación en el área de la seguridad cibernética y, tener en cuenta la ciberseguridad en todos los programas de asociación estratégica de innovación (Johansson and Ygeman, 2017).

Los países de América Latina deben aprender a adoptar normas como las anteriormente mencionadas donde, entre otros, hay un enfoque por expandir el conocimiento a la población. Sin embargo, hasta el momento se sabe que

> La OEA se ha enfocado en favorecer la cooperación entre el sector público, privado, académico y los usuarios finales, recalcando que los Estados deben promover una cultura de seguridad cibernética y actuar en pos de la protección de los usuarios individuales que en definitiva son los actores más vulnerables, además que con el fin de alcanzar plenamente estos objetivos, las estrategias nacionales de Ciberseguridad latinoamericanas, deben – además de ser construidas a través de la cooperación internacional- ser armonizadas con los

valores y derechos fundamentales desarrollados a nivel socio-cultural en cada país, tales como la privacidad, la libertad de expresión y el debido proceso, así como con los principios técnicos clave que han permitido la innovación en Internet, como la apertura, la universalidad y la interoperabilidad (Valdebenito y Sánchez, 2018)

Según la imagen 2 que muestra el Ranking Internacional de Ciberseguridad (NCSI), Costa Rica ocupa el puesto #48 de 160 y al ser comparado con países altos como Grecia, Finlandia y Dinamarca y bajos como Brasil y México, se genera el siguiente gráfico (e-Governance Academy, 2020).

Rank	Country	National Cyber Security Index	Digital development	Difference
1.	Greece	96.10	65.44	30.66
10.	Finland	81.82	82.26	-0.44
11.	Denmark	81.82	83.55	-1.73
48.	Costa Rica	53.25	64.34	-11.09
61.	Brazil	46.75	59.17	-12.42
76.	Mexico	36.36	54.37	-18.01

Imagen 2
Ranking Timeline
Fuente: e-Governance Academy, 2020.

Costa Rica debe adoptar las normas de países como Dinamarca, Suecia y Finlandia donde, entre otras cosas, tienen como prioridad que la información sobre ciberseguridad fluya entre los ciudadanos desde temprana edad, esta calza con el plan de esta investigación. Para lograrlo, la investigación incluye las mejores prácticas para navegar en la Red. Por ejemplo, según Elliot Bolland de usecure, la tabla 1 muestra los temas más importantes a tratar.

Most important security awareness training topics
1. Ataques de suplantación de identidad
2. Media removible
3. Contraseñas y autenticación
4. Seguridad física
5. Seguridad de dispositivos móviles
6. Trabajando de forma remota
7. Wi-Fi público
8. Seguridad en la Nube
9. Uso de redes sociales
10. Uso de Internet y correo electrónico
11. Ingeniería social
12. Seguridad en casa

Tabla 1
Most important security awareness training topics
Fuente: Elaboración propia de acuerdo con Bolland, usecure blog, 2020.

Además, el Fondo Común de Riesgo Intergubernamental de la Liga Municipal de Texas del 2020 desarrolló un entrenamiento que no solo explica los puntos en los que hay que enfocarse, sino que va más allá y explica qué son ataques, los define como

> cualquier intento de obtener acceso o control de los datos o sistemas de información de una organización, no importa cuál sea el nivel de sofisticación. Los ataques pueden ser simples correos electrónicos o incluso llamadas telefónicas, correos electrónicos con malware adjunto o correo electrónico a gran escala ataque a los puntos de acceso de un sistema

De tal manera, cómo es posible reconocer los ataques más comunes y los tipos de tácticas empleados en un ataque. Por ejemplo, en la imagen 3 explica cómo identificar un ataque por correo electrónico (Intergovernmental Risk Pool, 2020).

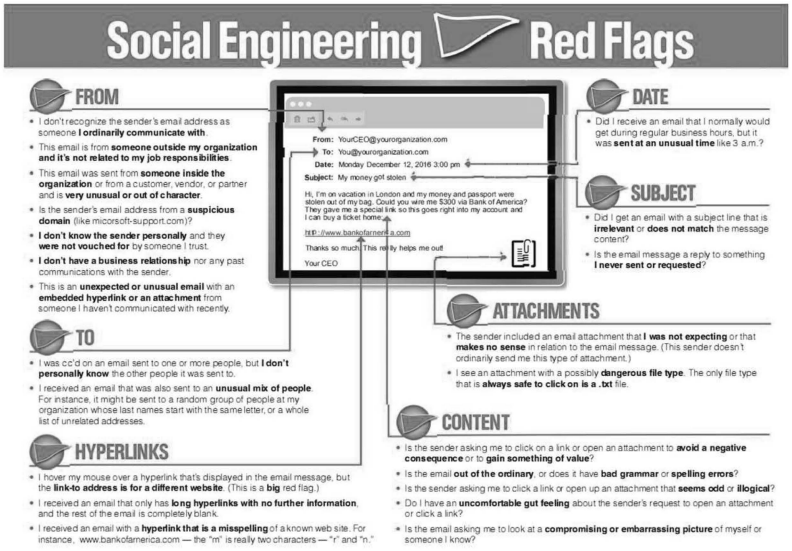


Imagen 3
Social Engineering Red Flags
Fuente: Texas Municipal League Intergovernmental Risk Pool, 2020.

Por otro lado, la compañía WAPA hace pública una presentación realizada para expandir el conocimiento sobre ciberseguridad en su empresa, dicha información calza con lo mencionado por Bolland anteriormente y además incluye prácticas específicas como el manejo de contraseñas y cómo deben contener al menos un carácter especial, una letra mayúscula, una letra minúscula un número. Además, menciona cómo no se debe utilizar información personal o frases comunes ni reutilizar contraseñas o compartirlas con otras personas, también habla de la importancia de cambiar las contraseñas con regularidad Western Area Power Administration. (2020). Estas son prácticas básicas que todos los costarricenses deben conocer para evitar ser víctimas de un crimen tan simple como robar una contraseña.

Costa Rica ha experimentado un alza en el uso de Internet gracias al COVID-19, que se presentó este 2020 y requiere así el conocimiento de los riesgos que esto trae. Siobhan Gorman de la compañía CrowdStrike menciona que la ciber educación debe ser una prioridad e indaga sobre la situación mundial en cuanto a la pandemia y su afectación directa

> COVID-19 está acelerando las amenazas cibernéticas como los ataques de software maliciosos y extorsión. Los ciberataques se han disparado durante la pandemia, ya que los ciberdelincuentes explotan sin piedad la situación actual, y los softwares maliciosos que bloquean los sistemas de las empresas sigue siendo una de las principales opciones para los piratas cibernéticos. Los adversarios están ajustando sus tácticas para atacar las operaciones corporativas externas que van más allá del robo de datos e interrumpen las operaciones. Los lugares de trabajo tradicionales están diseñados para ser resistentes a los ciberataques, pero la capacidad de responder rápidamente a ellos es ahora más desafiante. (Gorman, 2020).

Metodología de investigación

El enfoque de la investigación es de índole cuantitativo. Este enfoque plantea un problema de estudio delimitado y concreto sobre el fenómeno, aunque en evolución. Sus preguntas de investigación versan sobre cuestiones específicas (Hernández, Fernández y Baptista, 2014). En este caso, se centra en el problema específico del fraude cibernético. Por medio de este enfoque se va a procurar obtener datos válidos que vayan a responder los objetivos planteados

Además, la investigación es de tipo exploratorio ya que el tema de la ciberseguridad es relativamente desconocido en nuestro país y de acuerdo con Hernández, Fernández y Baptista (2014) "los estudios exploratorios sirven para familiarizarnos con fenómenos relativamente desconocidos, obtener información sobre la posibilidad de llevar a cabo una investigación más completa respecto de un contexto particular, indagar nuevos problemas, identificar conceptos o variables promisorias" (p. 91).

También, las medidas de ciberseguridad seguirán cambiando de acuerdo con el ritmo con el que nuevas amenazas surjan en la web y la investigación sobre nuevas tendencias es un tema que se debe actualizar recurrentemente para tener el conocimiento necesario y evitar ser víctimas. Los estudios exploratorios en pocas ocasiones constituyen un fin en sí mismos. Generalmente determinan tendencias, identifican áreas, ambientes, contextos y situaciones de estudio, relaciones potenciales entre variables; o establecen el "tono" de investigaciones posteriores más elaboradas y rigurosas (Hernández, Fernández y Baptista, 2014).

Cabe recalcar que, al ser una investigación de tipo exploratorio no se presenta una hipótesis ya que, según Hernández, Fernández y Baptista (2014):

> no en todas las investigaciones cuantitativas se plantean hipótesis. El hecho de que formulemos o no hipótesis depende de un factor esencial: el alcance inicial del estudio. Las investigaciones cuantitativas que formulan hipótesis son aquellas cuyo planteamiento define que su alcance será correlacional o explicativo, o las que tienen un alcance descriptivo, pero que intentan pronosticar una cifra o un hecho. La imagen 4 muestra esta indicación de manera más clara.

Alcance del estudio	Formulación de hipótesis
Exploratorio	No se formulan hipótesis.
Descriptivo	Sólo se formulan hipótesis cuando se pronostica un hecho o dato.
Correlacional	Se formulan hipótesis correlacionales.
Explicativo	Se formulan hipótesis causales.

Imagen 4
Formulación de hipótesis en estudios cuantitativos con diferentes alcances.
Fuente: Hernández, Fernández y Baptista, 2014.

Para esta investigación, se van a recolectar datos de 50+ personas entre las edades de 17 y 38 años. Este rango corresponde a personas de las generaciones digitales y virtuales definidas por un estudio llamado *La Verdad sobre las Generaciones en Costa Rica* realizado por Kolbi y UNIMER en el 2017 donde se definen generaciones específicas para Costa Rica de acuerdo con el comportamiento de la población.

Este estudio menciona que

> las empresas costarricenses erróneamente han recurrido a propuestas mundiales de segmentación, sobre todo aquellas relacionadas con grupos generacionales. Erróneamente, porque cada uno de los grupos de personas que nacen en una fecha determinada, se han ido formando dentro de una sociedad y tienen sus propias vivencias y experiencias influenciadas por el entorno y la coyuntura política, social, cultural y económica que les ha correspondido vivir, por lo que son propuestas que no necesariamente se pueden adaptar a la realidad nacional (Sanabria, Chacón, Linares y Salas, 2017).

La imagen 5 muestra las generaciones establecidas desde 1924. Como se menciona anteriormente, para la presente investigación se obtendrá información de personas de 17 a 38 años, que corresponde a la generación digital (21-38 años [1982-1999]) y, además, abarca una parte de la generación virtual, específicamente personas que ya hayan acabado sus estudios colegiales (17-20 años [2008-2020]). Esto con el fin de medir su conocimiento en cuanto a ciberseguridad una vez concluido el colegio.

Generación	AM	Pregonera	Satelital	Digital	Virtual
Período	1924 - 1939	1940 -1960	1961 -1981	1982 - 1999	2000...
Duración	15 años	20 años	20 años	17 años	17...
Edad	78 0 más	57 a 77 años	36 a 56 años	18 a 35 años	0 a 17 años
Cantidad de Población (*)	70.713	459.008	1.094.165	1.343.764	398.907
% de la población (**)	2,1%	13,6%	32,5%	39,9%	11,8%

Imagen 5.
Grupos Generacionales en Costa Rica.
Fuentes: Cuadro elaborado por UNIMER. (*) e (**) Instituto Nacional de Estadística y Censos (INEC), Censo Costa Rica, 2017.

En cuanto a métodos de recolección de datos, "la encuesta es uno de los métodos más utilizados en la investigación de mercado porque permite obtener información real directamente de los consumidores" (QuestionPro, 2020), por lo que en esta investigación se utilizará el cuestionario de

preguntas de selección en forma de encuesta donde se presentarán 13 preguntas por medio de la herramienta surveymonkey.com.

Propuesta de encuesta:

1. Por favor, escoja su rango de edad:
    a. Entre 17 y 21 años
    b. Entre 22 y 38 años
    c. Entre 39 y 45 años
2. Por favor, escoja su nivel de escolaridad:
    a. Primaria completa
    b. Primaria incompleta
    c. Secundaria completa
    d. Secundaria incompleta
    e. Bachillerato universitario completo
    f. Bachillerato universitario incompleto
    g. Licenciatura completa
    h. Licenciatura incompleta
    i. Maestría completa
    j. Maestría incompleta
3. ¿Conoce usted el término ciberseguridad? Sí/No
4. ¿Ha escuchado en las noticias u otros medios sobre el fraude cibernético? Sí/No
5. ¿Ha sido usted, o alguien conocido, víctima de fraude cibernético? Sí/No
6. ¿Conoce usted la diferencia entre un sitio web que comience con "http://" y uno que comience con "https://"? Sí/No
7. De las siguientes prácticas, ¿cuáles cree que son las mejores opciones para evitar el fraude cibernético?
    a. Borrar el correo donde haya recibido archivos que parezcan peligrosos y que no estaba esperando recibir.
    b. Escribir sus contraseñas en un papel para que no se le pierdan.
    c. Cambiar su contraseña cada 6 meses para evitar que alguien más la aprenda.
    d. Entrar al enlace de un correo de un remitente desconocido pero que parece tener información interesante.
    e. Entrar al enlace que me indique alguien que me llame de parte del banco, aunque yo no haya solicitado ninguna información ni trámite, para saber de qué se trata.

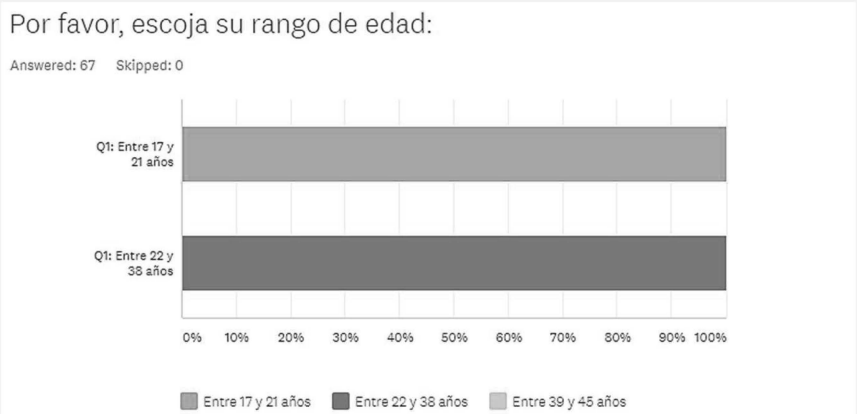
8. ¿Cree usted que el exceso de uso de internet aumenta las probabilidades de violación de su seguridad informática? Sí/No
9. ¿Está usted de acuerdo con el siguiente enunciado? Los niños a partir de los 12 años consumen Internet de una manera más amplia que en los años anteriores. Sí/No

10. ¿Considera usted que en el sistema educativo de Costa Rica se imparte una buena educación en cuanto al tema de ciberseguridad? Pésima/Mala/Buena/Muy buena/Excelente
11. Su conocimiento en cuanto a ciberseguridad, lo adquirió en:
    a. Primaria
    b. Secundaria
    c. Universidad
    d. Cursos en el trabajo
    e. Otro: _____.

12. ¿Estaría interesado en conocer las buenas prácticas que a nivel global ayudan a evitar el fraude cibernético? Sí/No
13. ¿Estaría de acuerdo con implementar un taller de ciberseguridad como parte de las clases de informática en los colegios? Sí/No

Análisis de resultados

Como método de recolección de datos, se utilizó el cuestionario, el cual fue aplicado por medio de la técnica encuesta. Dicha encuesta fue completada por 69 personas entre las edades de 17 y 45 años, de las cuales el 97.1% son parte de la generación digital; ese porcentaje se divide en un 44.93% para el grupo de 17-21 años y 52.17% para el grupo de 22-38 años. Para efectos de esta investigación se toman en cuenta los resultados del grupo de enfoque de 17 a 38 años. El *gráfico 1* muestra los porcentajes de manera visual.



	ENTRE 17 Y 21 AÑOS	ENTRE 22 Y 38 AÑOS	ENTRE 39 Y 45 AÑOS	TOTAL
Q1: Entre 17 y 21 años	100,00 % 31	0,00 % 0	0,00 % 0	46,27 % 31
Q1: Entre 22 y 38 años	0,00 % 0	100,00 % 36	0,00 % 0	53,73 % 36
Total de encuestados	31	36	0	67

Gráfico 1. Rango de edad.

Fuente: Elaboración propia, 2020.

Además, el *gráfico 2* muestra que el 60.93% de los encuestados del rango de edad entre 17 y 38 años tiene un nivel de educación mínimo del bachillerato incompleto.

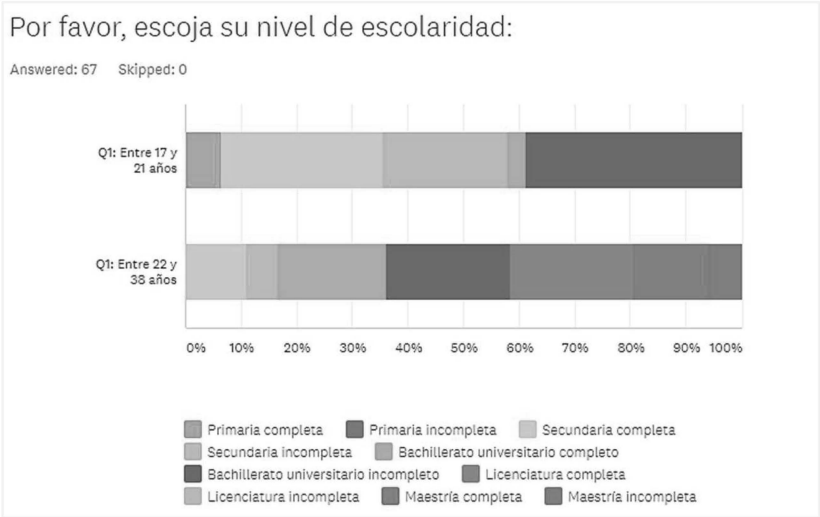
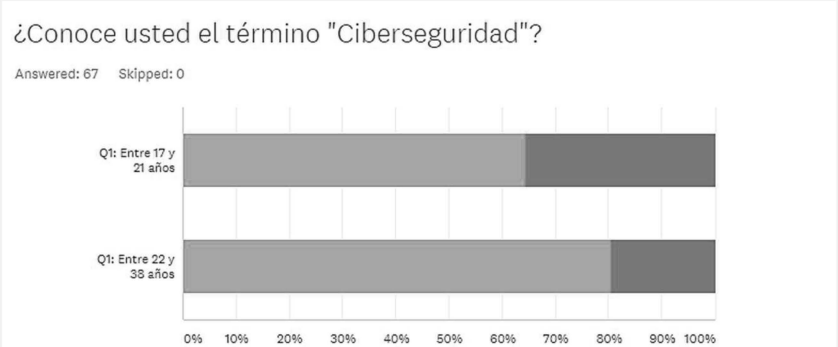


Gráfico 2. Nivel de escolaridad.
Fuente: Elaboración propia, 2020.

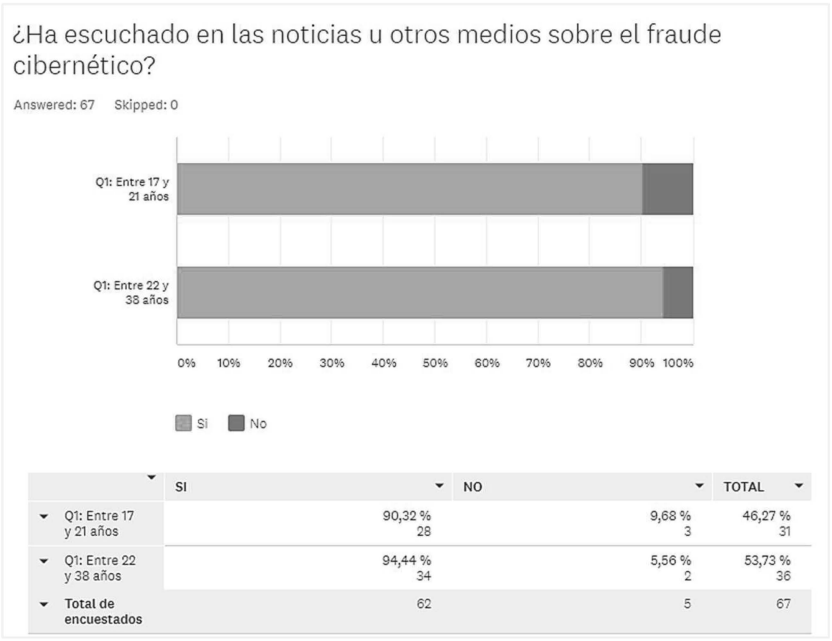
De las 67 personas entrevistadas de la generación digital (17-38 años), más de la mitad no conoce el término "ciberseguridad". El *gráfico 3* muestra los porcentajes de manera que se puede observar los dos grupos, la generación entre 17 y 21 años y la generación entre 22 y 38 años.



	SI	NO	TOTAL
Q1: Entre 17 y 21 años	64,52 % 20	35,48 % 11	46,27 % 31
Q1: Entre 22 y 38 años	80,56 % 29	19,44 % 7	53,73 % 36
Total de encuestados	49	18	67

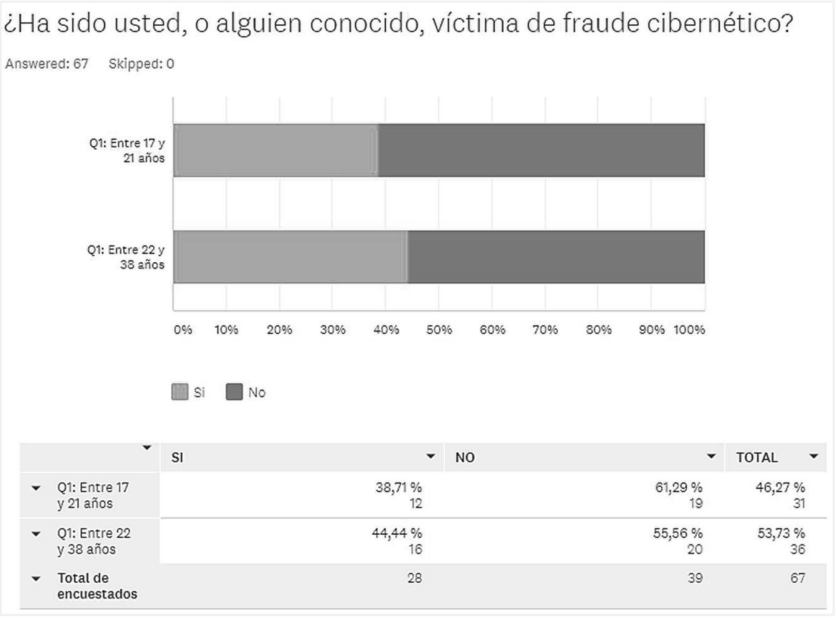
Gráfico 3. Conocimiento del término *Ciberseguridad*.
Fuente: Elaboración propia, 2020.

En los resultados mostrados en el *gráfico 4* también se puede ver que cerca del 100% en cada grupo ha escuchado sobre fraudes cibernéticos. Además, en el *gráfico 5* se muestra como 31 personas de 67 tienen algún conocido o han sido víctimas de fraude ellos mismos.



	SI	NO	TOTAL
Q1: Entre 17 y 21 años	90,32 % 28	9,68 % 3	46,27 % 31
Q1: Entre 22 y 38 años	94,44 % 34	5,56 % 2	53,73 % 36
Total de encuestados	62	5	67

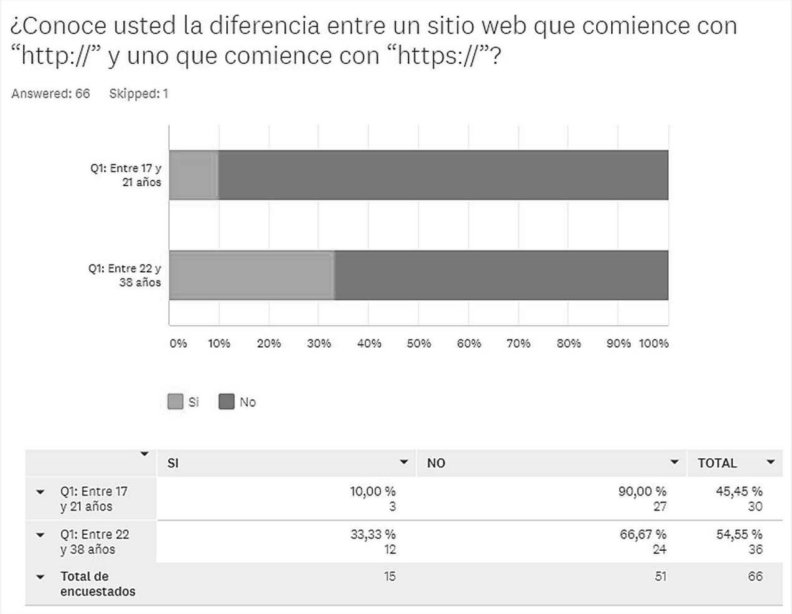
Gráfico 4. Conocimiento del fraude cibernético.
Fuente: Elaboración propia, 2020.



	SI	NO	TOTAL
Q1: Entre 17 y 21 años	38,71 % 12	61,29 % 19	46,27 % 31
Q1: Entre 22 y 38 años	44,44 % 16	55,56 % 20	53,73 % 36
Total de encuestados	28	39	67

Gráfico 5. Cercanía al fraude cibernético.
Fuente: Elaboración propia, 2020.

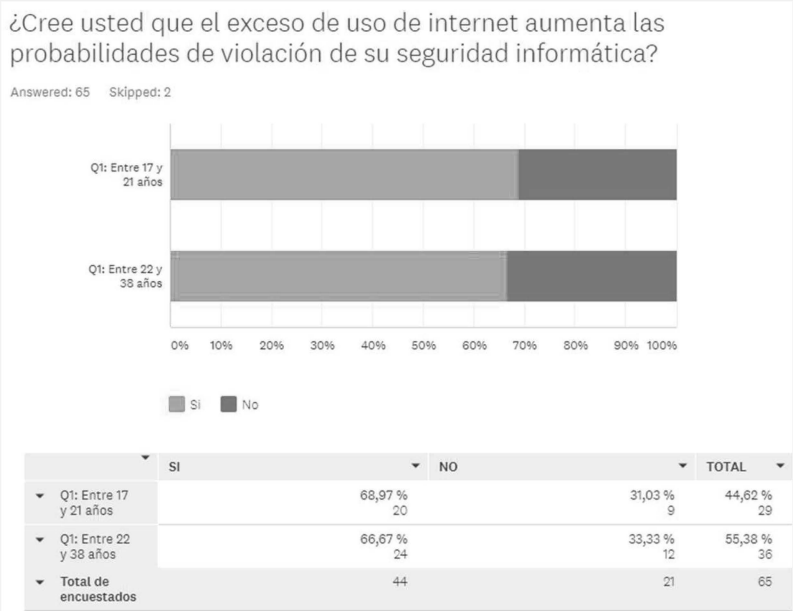
Asimismo, en el *gráfico 6* se puede apreciar cómo solo el 10% de la generación más reciente conoce la diferencia entre un sitio seguro (https) y uno que no lo es (http). Por otro lado, del grupo entre 22 y 38 años el 33.33% sí conoce la diferencia.



	SI	NO	TOTAL
Q1: Entre 17 y 21 años	10,00 % 3	90,00 % 27	45,45 % 30
Q1: Entre 22 y 38 años	33,33 % 12	66,67 % 24	54,55 % 36
Total de encuestados	15	51	66

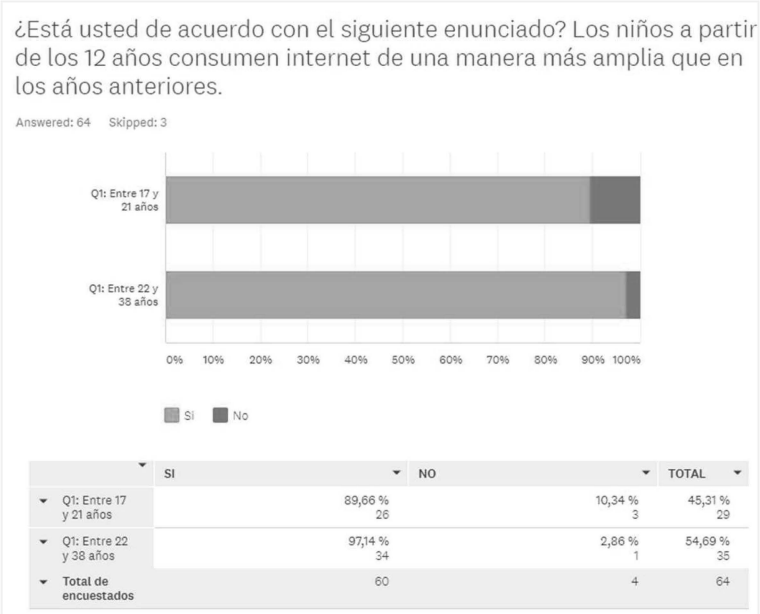
Gráfico 6. Reconocimiento de un sitio seguro vs. un sitio inseguro.
Fuente: Elaboración propia, 2020.

Los resultados en el *gráfico 7* también muestran como la mayoría de las personas en los 2 grupos no asocian el exceso de uso de Internet con la probabilidad de estar más expuestos a ataques cibernéticos. De igual manera, el *gráfico 8* confirma como 60 de 64 persona concuerdan con que los niños hacen un uso mucho más amplio a partir de los 12 años.



	SI	NO	TOTAL
Q1: Entre 17 y 21 años	68,97 % 20	31,03 % 9	44,62 % 29
Q1: Entre 22 y 38 años	66,67 % 24	33,33 % 12	55,38 % 36
Total de encuestados	44	21	65

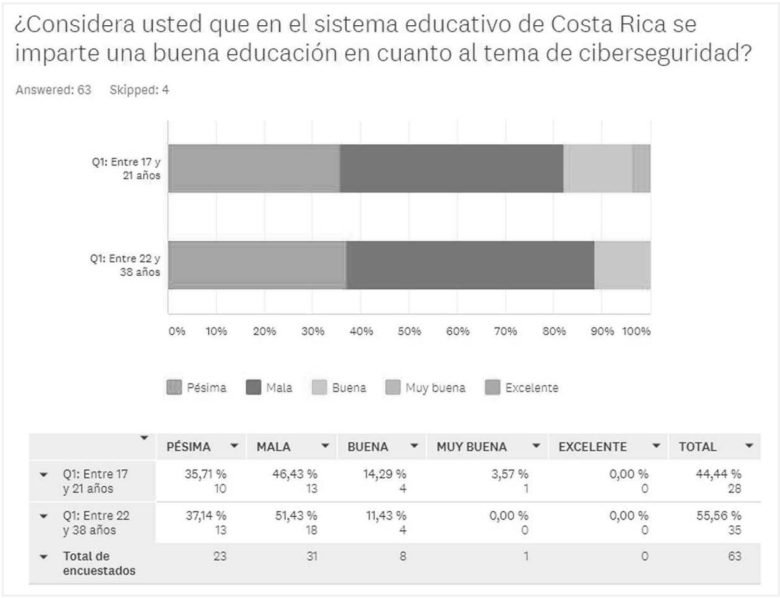
Gráfico 7. Exceso de Internet.
Fuente: Elaboración propia, 2020.



	SI	NO	TOTAL
Q1: Entre 17 y 21 años	89,66 % 26	10,34 % 3	45,31 % 29
Q1: Entre 22 y 38 años	97,14 % 34	2,86 % 1	54,69 % 35
Total de encuestados	60	4	64

Gráfico 8. Exposición de los niños a Internet a partir de los 12 años.
Fuente: Elaboración propia, 2020.

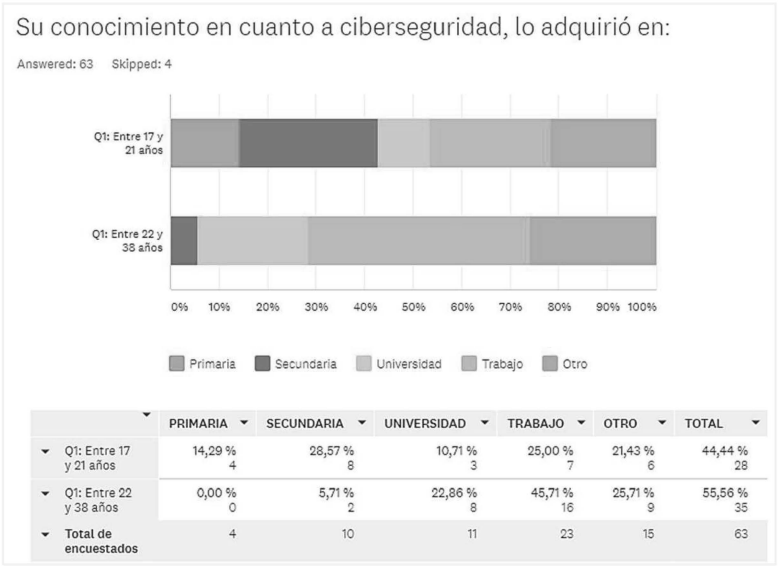
Se muestra además que cerca de la mitad de las personas encuestadas entre los 17 y 38 años considera que la educación sobre ciberseguridad en Costa Rica es mala, mientras que cerca del 35% opina que es pésima.



	PÉSIMA	MALA	BUENA	MUY BUENA	EXCELENTE	TOTAL
Q1: Entre 17 y 21 años	35,71 % 10	46,43 % 13	14,29 % 4	3,57 % 1	0,00 % 0	44,44 % 28
Q1: Entre 22 y 38 años	37,14 % 13	51,43 % 18	11,43 % 4	0,00 % 0	0,00 % 0	55,56 % 35
Total de encuestados	23	31	8	1	0	63

Gráfico 9. Ciberseguridad en el sistema educativo en Costa Rica.
Fuente: Elaboración propia, 2020.

En cuanto a la fuente de conocimientos de ciberseguridad, en el *gráfico 10* se muestra que la mayoría de los encuestados ha aprendido al respecto en sus trabajos con un 47.71% para la generación entre 22 y 38 años y un 25% para la generación más joven.



	PRIMARIA	SECUNDARIA	UNIVERSIDAD	TRABAJO	OTRO	TOTAL
Q1: Entre 17 y 21 años	14,29 % 4	28,57 % 8	10,71 % 3	25,00 % 7	21,43 % 6	44,44 % 28
Q1: Entre 22 y 38 años	0,00 % 0	5,71 % 2	22,86 % 8	45,71 % 16	25,71 % 9	55,56 % 35
Total de encuestados	4	10	11	23	15	63

Gráfico 10. Lugar de adquisición de conocimiento en ciberseguridad.
Fuente: Elaboración propia, 2020.

Además, en la imagen 6 podemos observar las respuestas escritas por las personas encuestadas donde se muestra que el conocimiento, en su mayoría poco, ha sido adquirido por otros medios ajenos a la educación pública del país.

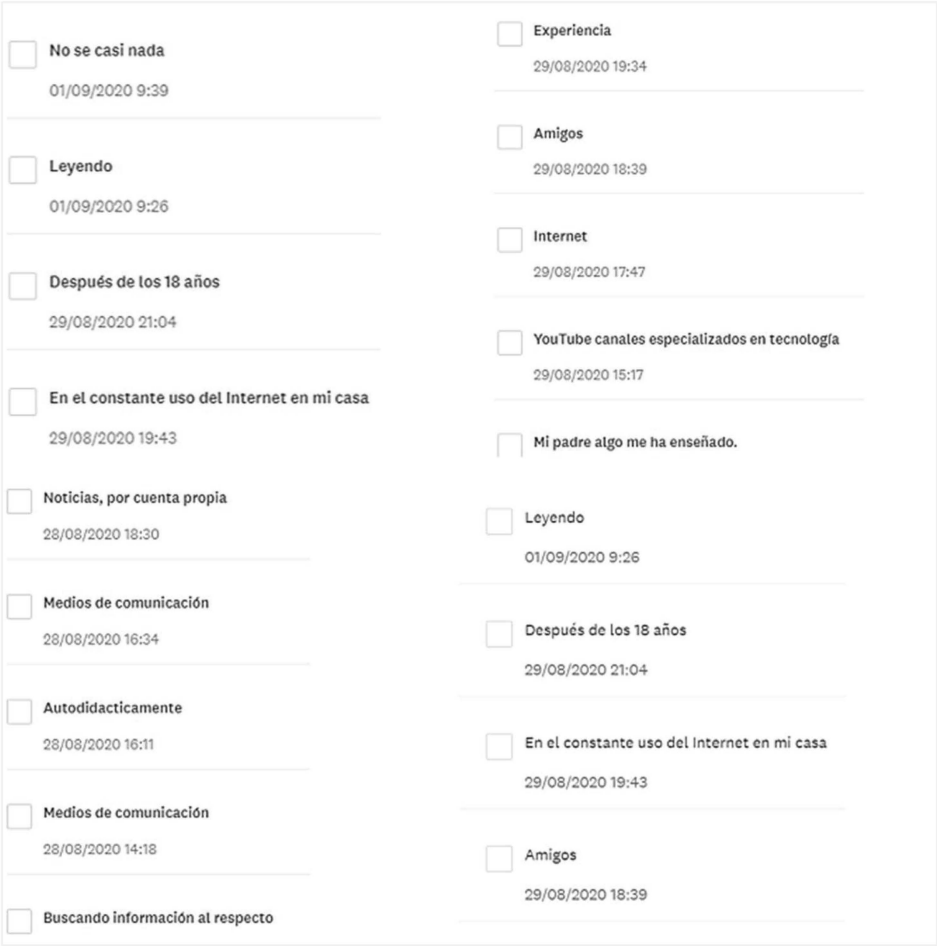
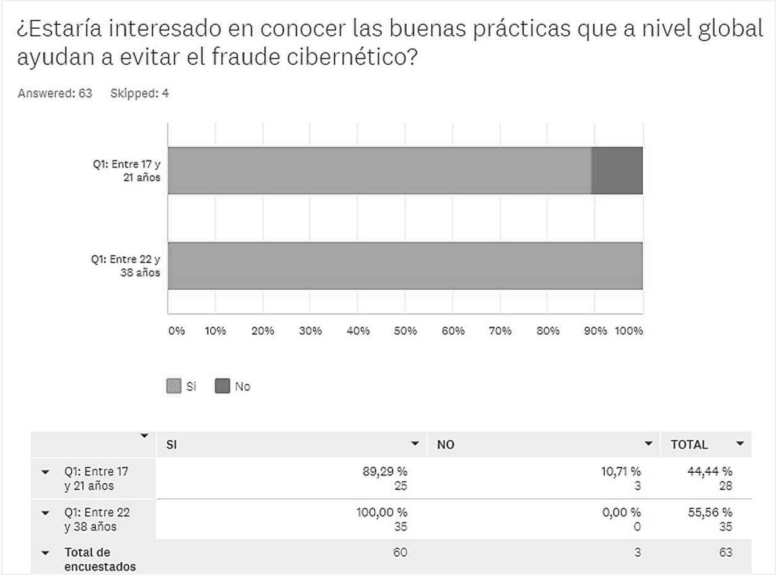


Imagen 6. Respuestas de los encuestados en cuanto a la fuente de conocimiento de ciberseguridad.
Fuente: Elaboración propia, 2020.

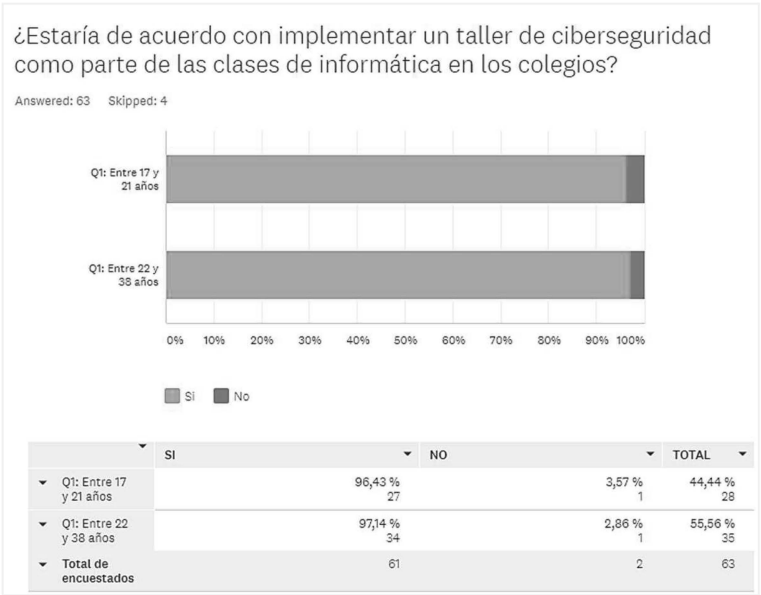
Adicionalmente, en el *gráfico 11* se presenta que de 63 personas que respondieron si tendrían interés en conocer las buenas prácticas a nivel global para evitar el fraude cibernético, 60 se manifestaron de manera positiva.



	SI	NO	TOTAL
Q1: Entre 17 y 21 años	89,29 % 25	10,71 % 3	44,44 % 28
Q1: Entre 22 y 38 años	100,00 % 35	0,00 % 0	55,56 % 35
Total de encuestados	60	3	63

Gráfico 11. Interés en buenas prácticas a nivel global.
Fuente: Elaboración propia, 2020.

Y, el *gráfico 12* muestra que solo una persona de cada grupo estaría en desacuerdo con que se imparta un taller de ciberseguridad como parte de las clases de informática en los colegios.



	SI	NO	TOTAL
Q1: Entre 17 y 21 años	96,43 % 27	3,57 % 1	44,44 % 28
Q1: Entre 22 y 38 años	97,14 % 34	2,86 % 1	55,56 % 35
Total de encuestados	61	2	63

Gráfico 12. Implementación del taller en los colegios.
Fuente: Elaboración propia, 2020.

Discusión

Luego de una amplia revisión bibliográfica y de realizar una encuesta a más de 65 personas, se confirma que la ciberseguridad es un tema de mucho cuidado a nivel global, en especial en la actualidad donde todos los países están atravesando la pandemia por coronavirus y, como menciona Siobhan Gorman de CrowdStrike, "COVID-19 está acelerando las amenazas cibernéticas como los ataques de software maliciosos y extorsión. Los ciberataques se han disparado durante la pandemia, ya que los ciberdelincuentes explotan sin piedad la situación actual" (Gorman, 2020).

La encuesta demuestra que en Costa Rica este tópico es aún desconocido para la mayoría; el segmento en el que se enfocó la encuesta representa una parte de la generación que según virtual (17 años) que a su vez calza con personas que ya han pasado por la educación secundaria en los colegios de Costa Rica, (17-21 años) y la generación digital entera (22-38 años). En los resultados se muestra que la generación que atravesó la secundaria más recientemente conoce aún menos el término: el 35% de los entrevistados entre 17 y 21 años expresó no conocer la palabra "ciberseguridad", mientras que en la generación de 22-38 años, cerca del 20% no la conoce.

Esto deja al descubierto que las personas más jóvenes que atravesaron el colegio recientemente no recibieron la educación necesaria para, al menos, conocer qué significa el término. Y, de acuerdo con las respuestas de 18 de los encuestados, el conocimiento sobre seguridad es mínimo, con respuestas de "No sé casi nada" y/o ha sido aprendido por su cuenta, con amigos, familia o medios de comunicación, fuera de las aulas de secundaria. Además, según los resultados de la investigación, el lugar de trabajo ha sido donde más se ha aprendido sobre seguridad cibernética con cerca del 50% para los encuestados entre 22 y 38 años y un 25% para los de edades entre 17 y 22. Esto comprueba el esfuerzo que hacen las compañías para educar a sus empleados y evitar fraudes, justo como lo hace la compañía WAPA anteriormente mencionada que comparte – incluso de manera pública – una presentación que incluye consejos importantes para expandir el conocimiento de sus colaboradores como el manejo inteligente de contraseñas, que es vital para evitar fraudes (Western Area Power Administration, 2020).

Lo mencionado en el párrafo anterior demuestra el hecho de que Costa Rica ocupe el puesto número 48 de 160 y no uno peor, se puede atribuir a razones externas a la educación secundaria, por lo que se podría decir que si se incluye un taller detallado sobre esto en las lecciones de Informática en los colegios, el país podría estar en un puesto mejor al lado de países como Finlandia y Dinamarca, así como crecen en desarrollo digital, también crecen en seguridad informática (e-Governance Academy, (2020).

Según los encuestados, solo 51 de 66 conocen la diferencia entre un sitio seguro certificado (https) y uno que no haya sido reconocido aún por una entidad formal lo que significa que el sitio

Web no ha sido otorgado con un certificado SSL (http). Asimismo, datos como el que un 55.38% no reconoce la relación entre un exceso en el tiempo que se pasa navegando la Web y la probabilidad de sufrir un ataque cibernético, demuestran la falta de conocimiento; esto hace que las personas sean aún más vulnerables porque no ven el peligro avecinarse y, tal como se mencionó en esta investigación, los ataques pueden ser tan simples como correos electrónicos con malware o incluso llamadas telefónicas (Intergovernmental Risk Pool, 2020). Al llenar el vacío de conocimiento en las personas, casos tan simples no pasarían a más, las personas estarían más protegidas y los índices de fraudes exitosos serían más bajos.

Además, tal como se mencionó en esta investigación, según The Danish Government (2018), países como Dinamarca han implementado un plan de ciberseguridad que ha mejorado el juicio y las habilidades digitales entre niños y jóvenes lo que ha ayudado a este país a estar entre los mejores (Bischoff, 2020). Esto concuerda con la opinión de los encuestados al estar en su gran mayoría (97%) de acuerdo con expandir el conocimiento de este tema en las lecciones de informática en los colegios y al reconocer en un 94% que los niños a partir de los 12 años están más expuestos a un consumo mayor de Internet, por lo que la iniciativa de brindarles la oportunidad de aprender cómo protegerse en la web es ideal.

El hecho de que cerca del 100% de los entrevistados haya escuchado de fraudes y que 28 personas de 64 hayan sido víctimas o sean cercanos a alguna víctima son datos preocupantes, ya que refuerza el hecho de que cada vez son más los ataques que se presentan por falta de conocimiento y con este viene la protección ya que "cada individuo es, por tanto, un importante actor que puede mejorar la seguridad cibernética a través de sus acciones a diario y por lo tanto, impactar su propia seguridad cibernética y la de otros" (The Security Committee, 2019).

Conclusiones y recomendaciones

En conclusión, las mejores prácticas a nivel global las presentan los países europeos de:

- Finlandia
- Dinamarca
- Suecia

Además, las mejores prácticas que se realizan en esos países son:

- Implementación de estrategias de cooperación internacional, por ejemplo, ser parte de la Unión Europea y tener un rol y participación activos en las decisiones en cuanto a las normas de ciberseguridad que afectan a todos los países de la Unión.
- Enfoque en fortalecer la educación y la investigación, el juicio y las habilidades digitales en niños y jóvenes (escuelas/colegios).

- Integración de programas de entrenamiento de seguridad, desarrollo de software y aplicaciones, redes de información y telecomunicaciones en educación vocacional y universidades.
- Sensibilizar a los ciudadanos, empresas y autoridades públicas en cuanto a la importancia sobre seguridad.
- Apoyar los esfuerzos de seguridad cibernética y de la información en la comunidad empresarial.
- Emplear entre sus lineamientos mejorar las asociaciones entre las instituciones de educación superior, los institutos de investigación industrial y los sectores públicos y privados para aumentar la utilización y la innovación en el área de la seguridad cibernética.
- Tener en cuenta la ciberseguridad en todos los programas de asociación estratégica de innovación.

Habiendo analizado las normas mencionadas en el párrafo anterior de las mejores prácticas globales, las normas aplicables a Costa Rica que se recomiendan son:

- Enfoque en fortalecer la educación y la investigación, el juicio y las habilidades digitales en niños y jóvenes (implementar talleres en escuelas/colegios).
- Integración de programas de entrenamiento de seguridad, desarrollo de software y aplicaciones, redes de información y telecomunicaciones en educación vocacional y universidades. Para este punto el gobierno podría no solo impartir lecciones al respecto, sino hacer alianzas con entidades enfocadas en tecnología como el ICE para crear campañas en centros universitarios que sean contados como requisitos de graduación (tipo sellos verdes).
- Sensibilización de los ciudadanos, empresas y autoridades públicas en cuanto a la importancia sobre seguridad. Se podrían hacer campañas en radio y televisión para abarcar un segmento más amplio que sólo instituciones educativas.
- Apoyo a los esfuerzos de seguridad cibernética y de la información en la comunidad empresarial. El Ministerio de Ciencia, Tecnología y Telecomunicaciones se podría unir con el CINDE para que las compañías en el país que sean enfocadas en tecnología colaboren con un programa donde sus empleados - como parte sus planes de responsabilidad social - compartan, complementen e impartan sus manuales de seguridad informática para que estas sean impartidas en lugares como el INA, IPECs, salones comunales etc., para abarcar a una población aún mayor.

Los temas recomendados para incluir en el manual de ciberseguridad para las clases de informática de los colegios públicos son los siguientes:

- Ataques de suplantación de identidad.
- Equipos de media removible.
- Manejo de contraseñas y medidas de autenticación.

- Seguridad física.
- Seguridad con dispositivos móviles.
- Normas para el uso de Wi-fi público.
- Seguridad en la nube.
- Uso de redes sociales.
- Uso general de Internet y correo electrónico.

En cuanto a la propuesta para el Ministerio de Educación Pública, esta consta de un manual con 10 capítulos que se verán a través del año lectivo, un capítulo por mes.

- El manual se dividirá de la siguiente manera:

    - CAPÍTULO 1: Ataques de suplantación de identidad.
    - CAPÍTULO 2: Equipos de media removible.
    - CAPÍTULO 3: Manejo de contraseñas y medidas de autenticación.
    - CAPÍTULO 4: Seguridad física.
    - CAPÍTULO 5: Seguridad con dispositivos móviles.
    - CAPÍTULO 6: Normas para el uso de Wi-fi público.
    - CAPÍTULO 7: Seguridad en la nube.
    - CAPÍTULO 8: Uso de redes sociales.
    - CAPÍTULO 9: Uso general de Internet y correo electrónico I.
    - CAPÍTULO 10: Uso general de Internet y correo electrónico II y examen para certificación.

- El manual incluye teoría sobre las mejores prácticas, y a la vez casos como ejemplos y ejercicios para que el estudiante resuelva en clase.
- Cada año cada estudiante debe certificarse con el manual; el profesor agregará ejemplos de casos que se ajusten con la realidad del momento.

Referencias bibliográficas

Bischoff P. (2020). *Which countries have the worst (and best) cybersecurity?* Recuperado de https://www.comparitech.com/es/blog/vpn-privacy/cybersecurity-by-country/

Bolland E. (2020). *12 Security Awareness Training Topics you Need to Know in 2020*. Recuperado de https://blog.usecure.io/12-security-awareness-topics-you-need-to-know-in-2020?hs_amp=true

e-Governance Academy. (2020). *National Cybersecurity Index.* Recuperado de https://ncsi.ega.ee/ncsi-index/?order=rank

Gorman, S. (2020). *Fighting Hackers From Your Couch: Five Things You Should Know.* Recuperado de https://www.crowdstrike.com/blog/fighting-hackers-from-your-couch-five-things-you-should-know/

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación.* (6a. ed.). México D.F.: McGraw-Hill

Johansson M. and Ygeman A. (2017). A national cyber security strategy. Recuperado de https://www.government.se/4ada5d/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213#:~:text=The%20national%20security%20strategy%20states,the%20area%20of%20information%20technology.

QuestionPro (2020) ¿Qué es una encuesta? Recuperado de https://www.questionpro.com/es/una-encuesta.html

Sanabria, P., Chacón, A., Linares, S. y Salas, R. (2017). La verdad sobre las eneraciones en Costa Rica #Gentico. *Yulök Revista de Innovación Académica*, 1(1), 18- 35.

Sánchez, J.M. (2020). Cómo «hackearon» las cuentas de famosos que avergüenza a Twitter, Julio, 2020. https://www.abc.es/tecnologia/consultorio/abci-como-hackearon-cuentas-famosos-averguenza-twitter-202007161424_noticia.html?ref=https:%2F%2Fwww.google.com%2F

Texas Municipal League Intergovernmental Risk Pool. (2020). Cyber Security Training_LESSON PLAN. Recuperado de . http://info.tmlirp.org/cyber-security-training-program

The Danish Government, Ministry of Finance. (2018). Danish Information Security Strategy 2018-2021. Recuperado de https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

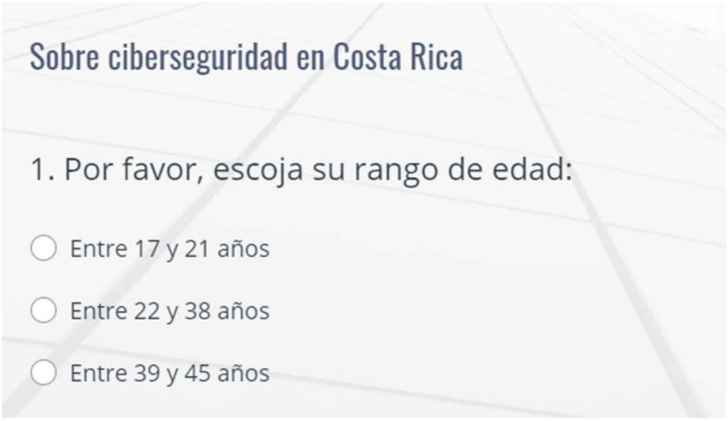
The Security Committee. (2019). *Finland´s Cyber Security Strategy 2019*. Recuperado de https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/#:~:text=The%20Finnish%20Cyber%20Security%20Strategy,based%20on%20the%20Government%20Programme.

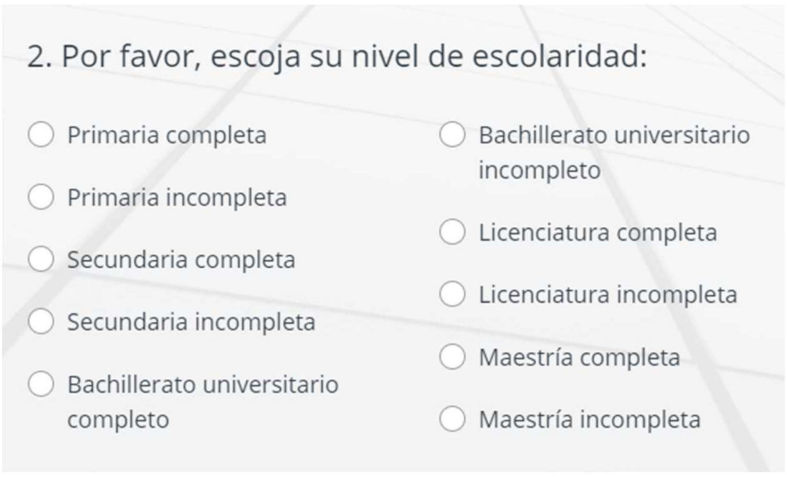
Valdebenito, H.J. y Sánchez A.M. (2018). Seguridad hemisférica latinoamericana adaptada a las nuevas tecnologías: Ciberseguridad y avances de cooperación regional e internacional para la sanción del ciberdelito *Revista ESPACIOS,* 2018. Vol. 39 (N.º 39). Recuperado de http://es.revistaespacios.com/a18v39n39/a18v39n39p31.pdf

Western Area Power Administration. (2020). *Annual Cyber Security Awareness Training.Recuperado* de https://www.wapa.gov/jobs/Documents/annual-cyber-security-training-new-hire.pdf

Anexos

Anexo 1
Encuesta
Enlace: https://www.surveymonkey.com/r/SZQ2KFC





3. ¿Conoce usted el término "ciberseguridad"?

- ◯ Sí
- ◯ No

4. ¿Ha escuchado en las noticias u otros medios sobre el fraude cibernético?

- ◯ Sí
- ◯ No

5. ¿Ha sido usted, o alguien conocido, víctima de fraude cibernético?

- ◯ Sí
- ◯ No

6. ¿Conoce usted la diferencia entre un sitio Web que comience con “http://” y uno que comience con “https://”?

- ◯ Sí
- ◯ No

7. De las siguientes prácticas, ¿cuáles cree que son las mejores opciones para evitar el fraude cibernético?

- ☐ Borrar el correo donde haya recibido archivos que parezcan peligrosos y que no estaba esperando recibir
- ☐ Escribir sus contraseñas en un papel para que no se le pierdan.
- ☐ Cambiar su contraseña cada 6 meses para evitar que alguien más la aprenda.
- ☐ Entrar al enlace de un correo de un remitente desconocido pero que parece tener información interesante.
- ☐ Entrar al enlace que me indique alguien que me llame de parte del banco, aunque yo no haya solicitado ninguna información ni trámite, para saber de qué se trata.

8. ¿Cree usted que el exceso de uso de Internet aumenta las probabilidades de violación de su seguridad informática?

- ◯ Sí
- ◯ No

9. ¿Está usted de acuerdo con el siguiente enunciado?
Los niños a partir de los 12 años consumen Internet de una manera más amplia que en los años anteriores.

- ◯ Sí
- ◯ No

10. ¿Considera usted que en el sistema educativo de Costa Rica se imparte una buena educación en cuanto al tema de ciberseguridad?

- ◯ Pésima
- ◯ Mala
- ◯ Buena
- ◯ Muy buena
- ◯ Excelente

11. Su conocimiento en cuanto a ciberseguridad, lo adquirió en:

- ◯ Primaria
- ◯ Secundaria
- ◯ Universidad
- ◯ Trabajo
- ◯ Otro

Otro (por favor especifique).

12. ¿Estaría interesado en conocer las buenas prácticas que a nivel global ayudan a evitar el fraude cibernético?

- ◯ Sí
- ◯ No

13. ¿Estaría de acuerdo con implementar un taller de ciberseguridad como parte de las clases de informática en los colegios?

- ◯ Sí
- ◯ No