Artículo original

Seguridad de dispositivos móviles y aplicaciones en función de la educación en tiempos de COVID-19

Security of mobile devices and applications as a function of education in times of COVID-19

Yoisel Leopoldo Rojas Hernández[1*] https://orcid.org/0000-0002-5284-1616

[1]Universidad de Ciencias Médicas de Sancti Spíritus. Cuba.

[*]Autor para la correspondencia: yoisel07044@gmail.com

RESUMEN

Introducción: En tiempos de COVID-19 constituye una necesidad utilizar dispositivos y aplicaciones móviles para el desarrollo del proceso docente-educativo en la Universidad de Ciencias Médicas de Sancti Spíritus, sin descuidar elementos de seguridad que permiten garantizar la preservación de la confidencialidad de los datos personales de estudiantes y profesores.

Objetivo: Identificar el estado de preparación inicial de estudiantes y profesores de la carrera Licenciatura en Sistemas de Información en Salud, en temas orientados a la seguridad de dispositivos y aplicaciones móviles en función de la educación.

Métodos: Estudio exploratorio realizado en los cursos académicos 2019-2020 y 2020-2021. Se trabajó con una muestra probabilística de 50 estudiantes y profesores. Se emplearon métodos teóricos, empíricos y estadístico-matemático. Se estructuró la variable dependiente en tres dimensiones y seis indicadores, y se definieron las fuentes de información y los principios éticos.

Resultados: Se identificaron los conocimientos teórico-prácticos de estudiantes y profesores en seguridad de dispositivos y aplicaciones móviles en función de la educación; adicionalmente, la actitud y motivación que manifestaron en cuanto al uso de métodos técnicos de seguridad y superación.

Esta obra está bajo una licencia https://creativecommons.org/licenses/by-nc/4.0/deed.es_ES

Conclusiones: Existen insuficientes métodos de seguridad técnica en dispositivos y aplicaciones móviles, y falta de cultura tecnológica orientada al uso de las redes de la Empresa de Telecomunicaciones de Cuba para el acceso a internet; de ahí la importancia de proteger los datos personales almacenados en dispositivos y aplicaciones móviles. Asimismo, desconocimiento de avisos y políticas de privacidad de las aplicaciones móviles, e insuficientes acciones formativas orientadas al uso correcto de las aplicaciones y la protección de los datos personales.

Palabras clave: infecciones por coronavirus; aplicaciones móviles; seguridad; riesgo; teléfono celular.

ABSTRACT

Introduction: In times of COVID-19 it constitutes a necessity to use mobile devices and applications for the development of the teaching-educational process at the University of Medical Sciences of Sancti Spíritus, without neglecting security elements that allow guaranteeing the preservation of the confidentiality of personal data of students and teachers.

Objective: To identify the state of initial preparation of students and teachers of the Bachelor's Degree in Health Information Systems, in topics oriented to the security of mobile devices and applications in terms of education.

Methods: Exploratory study conducted in the academic years 2019-2020 and 2020-2021. We worked with a probability sample of 50 students and teachers. Theoretical, empirical and statistical-mathematical methods were used. The dependent variable was structured in three dimensions and six indicators, and the sources of information and ethical principles were defined.

Results: Theoretical-practical knowledge of students and teachers in security of mobile devices and applications as a function of education was identified; additionally, the attitude and motivation they manifested regarding the use of technical methods of security and self-improvement.

Conclusions: There are insufficient technical security methods in mobile devices and applications, and lack of technological culture oriented to the use of the networks of the Cuban Telecommunications Company for Internet access; hence the importance of protecting personal data stored in mobile devices and applications. Likewise, lack of knowledge of privacy notices and policies of mobile applications, and insufficient training actions oriented to the correct use of applications and the protection of personal data.

Esta obra está bajo una licencia https://creativecommons.org/licenses/by-nc/4.0/deed.es_ES

Keywords: coronavirus infections; mobile applications; security; risk; cellphone.

Recibido: 20/02/2022

Aceptado: 04/03/2022

Introducción

La sociedad del conocimiento ha etiquetado de manera significativa los métodos y medios de aprendizaje que utilizan los jóvenes que transitan hoy en día por las instituciones educativas. El cada vez más creciente uso de las tecnologías informáticas ha propiciado el origen de nuevos enfoques teóricos del aprendizaje, que desplazan, de manera paulatina, los métodos tradicionales de enseñanza y le imprimen a la actividad pedagógica un quehacer cada vez más dependiente de los medios tecnológicos y las aplicaciones en función de la educación.

En tiempos de COVID-19 son muchas las instituciones universitarias que, en aras de evitar la propagación de la epidemia, han migrado a la modalidad a distancia, donde utilizan como principal apoyo a las tecnologías de la información y las comunicaciones (TIC), a las cuales se accede a través de los diferentes medios tecnológicos en propiedad de estudiantes y profesores. Esto da paso a desarrollar el proceso docente educativo, mediante tecnologías emergentes, tales como *Mobile Learning* y *Bring Your Own Device*.[1]

Tal es así que, *StatCounter*, dedicado a publicar estadísticas relacionadas con el análisis de tráfico web, muestra cómo, en junio de 2021, Cuba contabilizaba un 68,12 % de acceso a internet, a través de teléfonos celulares, un 31,28 % mediante el uso de computadoras de escritorio y un 0,6 % por tablet. Sin embargo, en diciembre de 2019 se contabilizó que el 48,26 % del acceso a internet se realizaba mediante teléfonos móviles y el 50,96 % por computadoras de escritorio, mientras que el 0,7 a través de tablet.[2]

El Gobierno cubano ha realizado cuantiosos esfuerzos para actualizar la infraestructura tecnológica en las instituciones educativas del país, en aras de potenciar el modelo tecno-pedagógico en el proceso docente-educativo. Es frecuente encontrar universidades con una óptima adecuación tecnológica, capaz de ofrecer diferentes servicios *online*, que apoyan los procesos de enseñanza-

Esta obra está bajo una licencia https://creativecommons.org/licenses/by-nc/4.0/deed.es_ES

aprendizaje y favorecen el uso de aplicaciones en función de la educación. A lo anterior se le añade el cada vez más creciente acceso a internet, desde diferentes planes y servicios que ofrece la Empresa de Telecomunicaciones de Cuba (ETECSA), lo cual incide directamente en la inserción de la Isla en estadísticas cada vez más creciente de uso de dispositivos portables, entre las variantes que utiliza el ciudadano promedio para el estudio, la capacitación y la investigación.

Por otro lado, resulta cada vez más frecuente que estudiantes y profesores utilicen sus propios dispositivos electrónicos en función del proceso enseñanza-aprendizaje, a pesar de que muchas instituciones educativas manifiestan preocupación en temas de seguridad, teniendo en cuenta aspectos relacionados con la brecha tecnológica y la neutralidad de las plataformas educativas implementadas. No obstante, la tendencia del número de modelos que apoyan el uso de la tecnología emergente *Bring Your Own Device* es creciente; por ende, se augura una atenuación de la preocupación, relacionada con el riesgo de uso de estos dispositivos en el ámbito pedagógico.[3,4,5,6]

De igual manera, el aprendizaje móvil ha ganado terreno y popularidad en estudiantes y profesores; muchos investigadores coinciden en que constituye una modalidad educativa que favorece la construcción del conocimiento, la resolución de problemas de aprendizaje, y la adquisición de habilidades de manera autónoma y ubicua, debido al apoyo de dispositivos móviles portables.[7,8,9,10]

En tiempos de COVID-19, la Universidad de Ciencias Médicas de Sancti Spíritus no ha estado exenta del uso de las tecnologías emergentes mencionadas anteriormente, al mostrar buenos resultados en el uso del teléfono móvil y Whatsapp en función del proceso docente-educativo durante los períodos académicos 2019-2020 y 2020-2021.

En estos cursos, *Rojas* y otros[11] realizaron un estudio exploratorio relacionado con el uso del teléfono móvil y Whatsapp en función de la educación en tiempos de COVID-19, en cuarto y quinto años de la carrera Licenciatura en Sistemas de Información en Salud, donde concluyeron: “el estudio tuvo la capacidad de demostrar un uso racional, planificado y correcto del teléfono celular y Whatsapp en el proceso enseñanza-aprendizaje, al potenciar métodos productivos y habilidades tecnológicas que le permiten a la actividad pedagógica articularse con las características del contexto actual, lo que demuestra estándares de calidad que demanda la educación superior en Cuba, en tiempos de COVID-19”.

Ante el desarrollo de la enseñanza móvil en la institución, resulta necesario analizar los aspectos que giran en torno a la seguridad de las aplicaciones que apoyan actualmente el proceso docente-educativo, porque, a través de estas existe el riesgo de que los datos personales de estudiantes y profesores queden

Esta obra está bajo una licencia https://creativecommons.org/licenses/by-nc/4.0/deed.es_ES

expuestos a personas mal intencionadas, los cuales pueden utilizarlos con fines malsanos, y provocar daños y perjuicios a personas naturales y jurídicas.

El presente estudio exploratorio tuvo como objetivo identificar el estado de preparación inicial de estudiantes y profesores de la carrera Licenciatura en Sistemas de Información en Salud, en temas orientados a la seguridad de dispositivos y aplicaciones móviles en función de la educación.

Métodos

El estudio exploratorio tuvo lugar en la Universidad de Ciencias Médicas de Sancti Spíritus, durante los cursos académicos 2019-2020 y 2020-2021.

El universo estuvo conformado por 50 profesores y estudiantes de la carrera Licenciatura en Sistemas de Información en Salud. Se trabajó con una muestra probabilística de 28 de ellos y se efectuó un muestreo estratificado en aras de evitar la presencia de sesgos relacionados con la selección de la muestra.

Los métodos teóricos utilizados fueron los siguientes:

- Histórico-lógico: permitió identificar las diferentes etapas por las que ha transitado el proceso docente-educativo en Cuba, apoyado por las tecnologías emergentes *Mobile Learning* y *Bring Your Own Device*.
- Sistematización teórica: facilitó organizar los conocimientos a través del comportamiento de la práctica y la literatura consultada, y generar indicadores.
- Analítico-sintético: posibilitó entrar en la esencia del proceso enseñanza-aprendizaje, perfeccionado por el uso de las tecnologías emergentes aplicadas a la educación en Cuba.
- Inductivo-deductivo: favoreció el procesamiento de la información empírica para la descripción de la experiencia adquirida, al determinar sus fortalezas y debilidades.

Como método empírico se empleó la encuesta, mediante la cual se obtuvo información relacionada con la preparación inicial de estudiantes y profesores. Esta se orientó a la seguridad de los dispositivos móviles y las aplicaciones en función del proceso docente-educativo y su pertinencia.

Esta obra está bajo una licencia https://creativecommons.org/licenses/by-nc/4.0/deed.es_ES

El método matemático utilizado fue la estadística descriptiva, que permitió procesar la información recolectada mediante el uso del *software* SPSS/*, lo que facilitó la interpretación de los datos.

Se estableció para el estudio, como variable dependiente: "Nivel de preparación inicial de estudiantes y profesores orientada a la seguridad de los dispositivos móviles y aplicaciones en función del proceso docente-educativo". Para esta se definen las siguientes dimensiones con sus respectivos indicadores:

- Dimensión I. Conocimientos teóricos
  - Indicador 1. Dominio teórico de los conocimientos orientados a la seguridad de dispositivos móviles y aplicaciones.
  - Indicador 2. Dominio de habilidades sobre el contexto de existencia, y uso de la seguridad de dispositivos móviles y aplicaciones.
- Dimensión II. Conocimientos prácticos
  - Indicador 3. Dominio práctico de métodos técnicos y/o administrativos orientados a la seguridad de dispositivos móviles y aplicaciones.
  - Indicador 4. Nivel de uso de los métodos técnicos y/o administrativos orientados a la seguridad de dispositivos móviles y aplicaciones.
- Dimensión III. Estado afectivo
  - Indicador 5. Actitud que manifiestan estudiantes y profesores con respecto a la superación y autosuperación orientada a la seguridad de dispositivos móviles y aplicaciones.
  - Indicador 6. Nivel de motivación para el uso de métodos técnicos y/o administrativos orientados a la seguridad de dispositivos móviles y aplicaciones.

Las fuentes de información consultadas fueron *Web of Science* (WoS), Scopus, Dialnet, Emerald, Sage, DOAJ, Redalyc y SciELO. Adicionalmente, se consultaron revistas científicas, sitios web y ponencias de jornadas virtuales como: *Acimed*, *Apertura*, *Educar*, *International Journal of Science and Technology*, *Journal of Information Technology*, *Revista Cubana de Educación Superior*, *Revista Científica de Educomunicación*, *Revista de Docencia Universitaria*, StatCounter, *Journal of Computer Assisted Learning*, *Computers & Education*, *Revista de Innovación Educativa*, *Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, *Ciencias de la Información* y XXI Jornada Provincial de Bibliotecas Médicas Sancti Spíritus, GlobalNET Solutions, is4k INTERNET SEGURA FORKiDS, *Gaceta Oficial de la República de Cuba* y Oficina de Seguridad del Internauta.

(cc) BY-NC Esta obra está bajo una licencia https://creativecommons.org/licenses/by-nc/4.0/deed.es_ES

Por su parte, los criterios de búsqueda estuvieron enfocados en garantizar la obtención de trabajos recientes. Por ello, el número de artículos consultados ascendió a 50, de los que se seleccionaron 20, debido a que, en su mayoría, constituyen investigaciones recientes y abordan directamente la temática del estudio.

Los principios éticos de la información recolectada por el presente estudio se definieron a partir de la Declaración de Helsinki de la Asamblea Médica Mundial.[12] Se consideró, específicamente, el 24, referido a la privacidad y confidencialidad de la información, donde se garantizó la intimidad de los participantes, mediante el anonimato. Se preservaron los registros de la investigación bajo la custodia del autor, mediante acta de compromiso, asumiendo la responsabilidad de salvaguardar y velar por la integridad de la documentación producida. Adicionalmente, la participación del personal en el estudio fue totalmente voluntaria y los resultados de la implementación de los instrumentos se utilizaron solo con fines propios y relacionados con la investigación. En ningún caso los resultados obtenidos se usaron para evaluar a los participantes. La anuencia se obtuvo a través de un acta de consentimiento informado, donde, al concluir el estudio, se ofrecieron los resultados, según lo establecido en el principio 25 de la mencionada declaración.

Resultados

Los resultados de la encuesta realizada a los estudiantes y profesores de la carrera Licenciatura en Sistemas de Información en Salud se muestran en la tabla.

Tabla - Resultado de la encuesta realizada a estudiantes y profesores

Preguntas	Respuestas
¿Cuál dispositivo electrónico utiliza usted con mayor frecuencia en función del proceso docente-educativo?	75 % teléfono móvil
	20 % computadora
	5 % tablet
¿Cuál aplicación utiliza usted con mayor frecuencia en función del proceso docente-educativo?	60 % Whatsapp
	36 % Messenger

Esta obra está bajo una licencia https://creativecommons.org/licenses/by-nc/4.0/deed.es_ES

	4 % correo electrónico
¿Con qué frecuencia utiliza usted la aplicación en función del proceso docente-educativo?	86 % diario
	10 % de 1 a 3 veces por semana
	4 % de 1 a 10 veces por mes
¿Qué busca usted obtener al usar la aplicación en función del proceso docente-educativo?	62 % autoaprendizaje
	30 % colaboración en grupo
	8 % motivación
¿Cuáles métodos de seguridad utiliza usted en dispositivos y aplicaciones que trabaja en función del proceso docente-educativo?	10 % antivirus
	35 % contraseñas
	0 % Antispyware
	0 % Antimalware
	55 % Ninguno
En el caso de los métodos de seguridad técnica, ¿conoce usted el procedimiento de instalación en su dispositivo móvil?	72 % No
	28 % Sí
¿Tiene usted alguna protección técnica en su dispositivo móvil o aplicación que utiliza en función del proceso docente-educativo?	83 % No
	17 % Sí
¿Cuál red utiliza usted con frecuencia para trabajar la aplicación en función del proceso docente-educativo?	68 % WIFI Pública
	30 % datos móviles
	2 % Nauta hogar
¿Conoce usted la importancia de proteger sus datos personales, mientras utiliza dispositivos y aplicaciones conectadas a una red?	12 % Sí
	70 % No
	18 % nunca me ha preocupado ese tema
¿Conoce usted los avisos y políticas de privacidad de las aplicaciones que utiliza en función del proceso docente-educativo?	0 % Sí
	78 % No
	22 % ni sabía que existía

Esta obra está bajo una licencia https://creativecommons.org/licenses/by-nc/4.0/deed.es_ES

¿Qué cree usted que pueda hacer una persona mal intencionada que obtenga su información personal?	58 % venta de mi información para fines de *marketing* digital
	42 % suplantación de identidad en internet
¿Conoce usted alguna ley, norma o reglamento, dictado por el Gobierno cubano que hable acerca de la seguridad informática o seguridad de la información?	6 % Sí
	94 % No
¿Conoce usted los riesgos informáticos a los que se expone cuando conecta un dispositivo a una red y hace uso de una aplicación?	4 % Sí
	96 % No
¿Conoce las vulnerabilidades técnicas que tiene la aplicación que usted utiliza en función del proceso docente-educativo?	0 % Sí
	100 % No
¿Ha participado usted en alguna charla, conferencia o curso relacionados con la importancia del uso correcto de las aplicaciones en función de la educación o la protección de los datos personales de estudiantes y profesores?	0 % Sí
	100 % No
¿Se siente usted motivado(a) por el uso de métodos técnicos de seguridad para dispositivos móviles y aplicaciones en función del proceso enseñanza-aprendizaje?	28 % Sí
	72 % No

Discusión

La Agencia Española de Protección de Datos, de conjunto con las diferentes asociaciones de centros educativos, realizaron una investigación pedagógica, cuyos resultados constituyeron "una guía sobre las implicaciones que dichas aplicaciones podían tener para la protección de los datos personales", donde se definió la información personal contenida usualmente en estas, tales como fotos, videos y mensajes de voz.[13]

Un aspecto fundamental a tener en cuenta para seleccionar una aplicación móvil, en función de la educación, resulta asegurarse de que esta contemple adecuados algoritmos de cifrado de las comunicaciones y de los datos almacenados, "ya sea localmente o en servicios en la nube, la copia de seguridad de los datos, así como el cumplimiento con las garantías exigidas por la legislación de protección de datos (LOPD) en el almacenamiento y tratamiento de los datos".[14]

Con relación a lo anterior, la Resolución 124 de 2019 dicta el "Reglamento para la Producción de los Programas y Aplicaciones Informáticas y la Evaluación de su

Esta obra está bajo una licencia https://creativecommons.org/licenses/by-nc/4.0/deed.es_ES

Calidad en Cuba", que establece: "La evaluación de las características de la calidad de programas y aplicaciones informáticas incluye pruebas de usabilidad, adecuación funcional, eficiencia de desempeño, fiabilidad, portabilidad y de seguridad; esta última de acuerdo con la protección de la información y los datos que contiene, evita que otros productos o sistemas tengan capacidad de acceso a los datos según sus tipos y niveles de autorización".[15]

Por su parte, la Resolución 127 de 2019 dicta el "Reglamento del Proveedor de Servicios Públicos de Alojamiento y de Hospedaje en el Entorno Internet", que establece en el Artículo 21:

> El proveedor tiene las obligaciones siguientes: […] adoptar las medidas necesarias para garantizar el cumplimiento de los principios de: iii. protección de la juventud y de la infancia; […] garantizar, en lo que le corresponde, la seguridad de las Tecnologías de la Información y la Comunicación en la red que utilice; […] sistematizar la gestión de vulnerabilidades, versiones y actualizaciones, parches, de las aplicaciones, *software* y *firmware*, sobre la base de la publicación de alertas de los fabricantes y la vigilancia tecnológica; […] implementar las medidas y herramientas que garanticen la seguridad de las infraestructuras de la red y la detección e investigación de incidentes de seguridad; […] reportar los incidentes de seguridad informática que se detecten por las vías y procedimientos establecidos en la legislación vigente; […] cumplir con la protección y tratamiento de los datos personales de sus clientes.

Mientras, el Artículo 23 establece: "El proveedor, cuando detecte vulnerabilidades que afectan la seguridad de la infraestructura tecnológica o que puedan propiciar la afectación de otros clientes hospedados o alojados por el propio proveedor, o de la infraestructura de terceros países, debe gestionar su solución y, en dependencia del impacto, resolver el contrato con el cliente que la origina e informar a las autoridades competentes".[16]

De acuerdo con los resultados de la encuesta, los estudiantes y profesores prefieren utilizar las aplicaciones móviles Whatsapp y Messenger, en función de desarrollar el proceso docente-educativo en tiempos de COVID-19. Ambas constituyen recursos informáticos de procedencia extranjera, que, sin dudas, están fuera del alcance de las Resoluciones 124 y 127; por ende, es difícil afirmar

Esta obra está bajo una licencia https://creativecommons.org/licenses/by-nc/4.0/deed.es_ES

que cumplan con todos los elementos técnicos de seguridad, que garanticen una adecuada protección de la información personal de sus clientes.

En otro orden de ideas, la Resolución 128/2019 dicta el Reglamento de Seguridad de las Tecnologías de la Información y las Comunicaciones en Cuba, donde el Capítulo IV Seguridad de las Operaciones, Artículo 30, declara:

> En el uso de credenciales de acceso, cuya contraseña es textual, como método de autenticación de usuarios, se cumplen los requisitos siguientes: a) ser privadas e intransferibles, b) su estructura, fortaleza y frecuencia de cambio se corresponden con el riesgo estimado para el acceso que protegen, implementado a través de mecanismos automatizados de validación, c) la composición de los caracteres es alfanumérica (letras, números y símbolos) sin un significado trivial, con una longitud mínima de 8 caracteres.[17]

Sin embargo, la mayoría de los encuestados manifestaron no utilizar ningún método de seguridad para dispositivos o aplicaciones utilizadas en función del proceso docente-educativo. Así quedó en evidencia un desconocimiento de la existencia de leyes, normas o reglamentos, dictados por el Gobierno cubano para garantizar la protección de información personal en los medios tecnológicos utilizados.

Por otro lado, las redes WIFI (inalámbricas) continúan presentando dificultades para garantizar la seguridad de la información de los clientes que se conectan a ellas. Los protocolos diseñados para encriptar los datos que circulan por la red, no son lo suficientemente robustos y suelen vulnerarse por personas mal intencionadas, con el ánimo de obtener información personal de los usuarios conectados a la red.[18]

Acorde con los resultados de la encuesta, estudiantes y profesores utilizan la red WIFI pública de ETECSA para acceder a las aplicaciones móviles y desarrollar las actividades docentes, propias del proceso enseñanza-aprendizaje. En este caso particular, la red inalámbrica se encuentra dentro de la cobertura de la Resolución 128/2019, la cual establece en el Artículo 36:

> El administrador de una red informática tiene, en relación con la seguridad de las TIC, los deberes siguientes: a) garantizar la aplicación de mecanismos que implementen las políticas de seguridad definidas

Esta obra está bajo una licencia https://creativecommons.org/licenses/by-nc/4.0/deed.es_ES

> en la red, d) comunicar a la dirección de la entidad los nuevos controles técnicos que estén disponibles y cualquier violación o anomalía detectada en los existentes, e) activar los mecanismos técnicos y organizativos de respuesta ante distintos tipos de incidentes y acciones nocivas que se identifiquen, y preservar toda la información requerida para su esclarecimiento, g) informar a los usuarios de las regulaciones de seguridad establecidas y controlar su cumplimiento, j) implementar y operar los controles que se establezcan para gestionar los riesgos de seguridad.[17]

Adicionalmente, la red WIFI pública de ETECSA se encuentra dentro del alcance del Decreto 360/2019 "Sobre la Seguridad de las Tecnologías de la Información y las Comunicaciones y la Defensa del Ciberespacio Nacional", el cual declara en su Artículo 26: "El Ministerio de Comunicaciones, de conformidad con sus atributos y funciones específicas, es el responsable de las actividades siguientes: f) establecer los mecanismos a emplear para la prevención y respuesta a incidentes de seguridad informática que involucren las TIC ubicadas en los hogares y las áreas públicas para el acceso al ciberespacio, por parte de las personas naturales y jurídicas".[19]

La seguridad de la información concibe dentro de su estructura el componente humano, porque puede invertirse en tecnología de punta orientada a garantizar estándares elevados de seguridad informática; asimismo, efectuarse una planificación precisa de los procesos que rigen el funcionamiento de la institución, en aras de controlar sus entradas y salidas. Pero, qué sucede si el capital humano encargado de gestionar el proceso docente-educativo (estudiantes y profesores) y destinado a utilizar las tecnologías en función de la educación, no se encuentra lo suficientemente informado acerca de los riesgos a los cuales se exponen sus datos personales en las aplicaciones utilizadas con fines pedagógicos.[20]

Hacia este punto el autor dirige su preocupación, puesto que los resultados de la encuesta revelan una falta de cultura de seguridad en estudiantes y profesores de la carrera Licenciatura en Sistemas de Información en Salud, orientada a dispositivos y aplicaciones móviles en función de la educación. Esta cuestión puede traer consigo afectaciones en la preservación de la confidencialidad de sus datos personales, lo cual incrementa el riesgo de que existan daños y perjuicios a futuro, tanto para ellos como para la institución.

Para concluir, resultan insuficientes los métodos de seguridad técnica que utilizan estudiantes y profesores en dispositivos y aplicaciones móviles en función del proceso docente-educativo. Se evidenció un desconocimiento elevado acerca del procedimiento de instalación de estos en los teléfonos móviles, y falta de cultura

Esta obra está bajo una licencia https://creativecommons.org/licenses/by-nc/4.0/deed.es_ES

tecnológica orientada al uso de las distintas redes que ofrece ETECSA para el acceso a internet; de ahí la importancia de proteger los datos personales almacenados en dispositivos y aplicaciones móviles. Asimismo, hubo baja percepción del riesgo, al desconocer los avisos y las políticas de privacidad de las aplicaciones que se utilizan en función del proceso docente-educativo, e insuficientes acciones formativas orientadas al uso correcto de las aplicaciones en función de la educación y la protección de los datos personales de estudiantes y profesores.

Referencias bibliográficas

1. Reyes Y, Martínez D. Acciones para la implementación en el sistema educativo cubano de tecnologías emergentes identificadas por el informe Horizon. Revista Cubana de Educación Superior. 2019 [acceso 06/07/2021];38(2). Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0257-43142019000200010

2. StatCounter. Dublín: GlobalStat; 2021 [acceso 06/07/2021]. Disponible en: https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/cuba

3. Crescenzi L, Valente R, Suárez R. Aplicaciones educativas, seguras e inclusivas: La protección digital desde una perspectiva ética y crítica. Revista Científica de Educomunicación. 2019 [acceso 07/07/2021];27(61):93-102. Disponible en: https://www.revistacomunicar.com/ojs/index.php/comunicar/article/view/C61-2019-08

4. Herodotou C. Young children and tablets: A systematic review of effects on learning and development. Journal of Computer Assisted Learning. 2017 [acceso 07/07/2021];34(1):1-9. Disponible en: https://onlinelibrary.wiley.com/doi/abs/10.1111/jcal.12220

5. Howard S, Yang J, Ma J, Maton K, Rennie E. App clusters: Exploring patterns of multiple app use in primary learning contexts. Computers & Education. 2018 [acceso 07/07/2021];127:154-64. Disponible en: https://www.sciencedirect.com/science/article/abs/pii/S0360131518302318

6. Porter J. Entering Aladdin's cave: Developing an app for children with Down syndrome. Journal of Computer Assisted Learning. 2018 [acceso 07/07/2021];34(4):429-39. Disponible en: https://onlinelibrary.wiley.com/doi/full/10.1111/jcal.12246

Esta obra está bajo una licencia https://creativecommons.org/licenses/by-nc/4.0/deed.es_ES

7. Soler I, López C, Lacave T. Percepción de riesgo online en jóvenes y su efecto en el comportamiento digital. Revista Científica de Educomunicación. 2018 [acceso 07/07/2021];56:71-9. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6483054

8. Conde S, Boza A. La educación del futuro: perspectiva del alumnado. Validación de una escala. Apertura. Revista de Innovación Educativa. 2019 [acceso 07/07/2021];11(2):86-103. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-61802019000200086

9. De la Rosa P. Aplicaciones educativas digitales y la falta de seguridad de los datos personales de sus usuarios. Revista Iberoamericana para la Investigación y el Desarrollo Educativo. 2021 [acceso 07/07/2021];12(23). Disponible en: https://www.ride.org.mx/index.php/RIDE/article/view/980

10. Aguilera O, Pérez O, de Jesús E, Rivero R. La protección de la información. Una visión desde las entidades educativas cubanas. Ciencias de la Información. 2017 [acceso 07/07/2021];48(3):41-7. Disponible en: http://cinfo.idict.cu/index.php/cinfo/article/view/885

11. Rojas Y, González A, Álvarez S, Rodríguez-Amaya I. El teléfono móvil y whatsapp apoyando a la educación en tiempos de COVID-19. XXI Jornada Provincial de Bibliotecas Médicas Sancti Spíritus; 2021 [acceso 08/07/2021]. Disponible en: https://bibliotecologiassp2021.sld.cu/index.php/bibliotecologiassp/2021/schedConf/presentations

12. Helsinki. Principios éticos para las investigaciones médicas en seres humanos. 2013 [acceso 08/07/2021]. Disponible en: https://www.unisabana.edu.co/fileadmin/Documentos/Investigacion/comite_de_etica/Declaracion_Helsinki_2013.pdf

13. GlobalNET Solutions. España; 2021 [acceso 11/07/2021]. Disponible en: http://www.globalnetsolutions.es/blog/aplicaciones-tecnologicas-en-los-colegios-si-pero-primando-la-seguridad-de-los-datos/

14. is4k INTERNET SEGURA FORKiDS. España; 2021 [acceso 11/07/2021]. Disponible en: https://www.is4k.es/blog/uso-seguro-de-aplicaciones-de-gestion-educativa-que-debemos-saber

15. Ministerio de Informática y Comunicaciones. Resolución No. 124/2019: Reglamento para la Producción de los Programas y Aplicaciones Informáticas y la Evaluación de su Calidad. Gaceta Oficial de la República de Cuba. La Habana: MIC; 2019 [acceso 11/07/2021]. Disponible en:

Esta obra está bajo una licencia https://creativecommons.org/licenses/by-nc/4.0/deed.es_ES

https://www.gacetaoficial.gob.cu/es/resolucion-124-de-2019-de-ministerio-de-comunicaciones

16. Ministerio de Informática y Comunicaciones. Resolución No. 127/2019: Reglamento del Proveedor de Servicios Públicos de Alojamiento y de Hospedaje en el Entorno Internet. Gaceta Oficial de la República de Cuba. La Habana: MIC; 2019 [acceso 11/07/2021]. Disponible en: https://www.gacetaoficial.gob.cu/es/resolucion-127-de-2019-de-ministerio-del-comercio-exterior-y-la-inversion-extranjera

17. Ministerio de Informática y Comunicaciones. Resolución No. 128/2019: Reglamento de Seguridad de las Tecnologías de la Información y las Comunicaciones. Gaceta Oficial de la República de Cuba. La Habana: MIC; 2019 [acceso 11/07/2021]. Disponible en: https://www.gacetaoficial.gob.cu/es/resolucion-128-de-2019-de-ministerio-de-comunicaciones

18. Oficina de Seguridad del Internauta. España; 2021 [acceso 12/07/2021]. Disponible en: https://www.osi.es/es/actualizaciones-de-seguridad

19. Consejo de Ministros. Decreto 360/2019: Sobre la Seguridad de las Tecnologías de la Información y las Comunicaciones y la Defensa del Ciberespacio Nacional. Gaceta Oficial de la República de Cuba. La Habana: CM; 2019. Disponible en: https://www.gacetaoficial.gob.cu/es/decreto-360-de-2019-de-consejo-de-ministros

20. Basantes A, Naranjo M, Gallegos M, Benítez N. Los dispositivos móviles en el proceso de aprendizaje de la Facultad de Educación, Ciencia y Tecnología de la Universidad Técnica del Norte de Ecuador. Formación Universitaria. 2017 [acceso 11/07/2021];10(2):79-88. Disponible en: https://scielo.conicyt.cl/scielo.php?script=sci_abstract&pid=S0718-50062017000200009&lng=es&nrm=iso

Conflicto de intereses

El autor declara que no existe conflicto de intereses.

Esta obra está bajo una licencia https://creativecommons.org/licenses/by-nc/4.0/deed.es_ES