Entre Ciencia e Ingeniería, vol. 17, no. 33, enero-junio de año, páginas 16-23. DOI: https://doi.org/10.31908/19098367.2832
ISSN 1909-8367 (Impreso), ISSN 2539-4169 (En línea)

Prácticas de seguridad de la información en estudiantes de escuela secundaria en Colombia

Cybersecurity Practices of Colombian high school students

M. J. Rojas, A. Pulido y Y.I. Serrato

Recibido: junio 15 de 2022 – Aceptado: mayo 23 de 2023

***Resumen*—El objetivo de este artículo es identificar las prácticas de seguridad de la información de estudiantes de escuela secundaria a partir de sus representaciones sociales. Esta investigación se realizó con la participación de estudiantes de instituciones públicas y privadas de las ciudades de Bogotá D.C. y Florencia-Caquetá en Colombia. Los datos fueron recolectados a través de una entrevista semiestructurada. El análisis de la información se realizó con el software cualitativo NVIVO v12. El estudio determina que la falta de cibereducación de los estudiantes de secundaria amplía el escenario de vulnerabilidades que pueden deteriorar la confianza y seguridad del entorno digital en el país.**

Palabras clave: prácticas de seguridad, comunicación digital, estudiantes, representaciones sociales, NVIVO.

***Abstract*—The objective of this article is to identify the cybersecurity practices of high school students based on their social representations. This research was carried out with the participation of students from state and private institutions in the cities of Bogotá D.C. and Florencia-Caquetá in Colombia. The data was collected through a semi-structured interview. The analysis of the information was carried out using the qualitative software NVIVO v12. The study determines that the lack of cyber-education of high school students becomes an important vulnerable condition that deteriorates the trust and digital security in the country.**

Keywords: cybersecurity practices, digital communication, students, social representations, NVIVO.

Proyecto desarrollado en el marco de la Especialización en Seguridad de la información de la Fundación Universitaria Los Libertadores.

M.J. Rojas-Bahamón, Secretaría de Eduación de Florencia, Colombia., Email: mjulissa@gmail.com

A. Pulido, Fundación Universitaria Los Libertadores., Email: alejo.pulido.jimenez@gmail.com.

Y.I. Serrato, Fundación Universitaria Los Libertadores. Email: yiserrator@gmail.com.

Como citar este artículo: Rojas-Bahamón, M. J., Pulido, A., y Serrato, Y. I. Prácticas de seguridad de la información en estudiantes de escuela secundaria en Colombia, Entre Ciencia e Ingeniería, vol. 17, no. 33, pp. 16-23, enero-junio 2023. DOI: https://doi.org/10.31908/19098367.2832

I. INTRODUCCIÓN

En un entorno en que prácticamente cualquier aparato tiene conexión a Internet, los usuarios deben ser responsables y conscientes de los riesgos que estos avances conllevan. En antaño quedaron las cifras de delitos informáticos asociados únicamente a entornos corporativos; en la actualidad, la evidencia apunta a determinar que este tipo de delitos aplican a población de cualquier edad.

Según el informe de fraudes emitido por el FBI [1], las denuncias por estafas en Estados Unidos aumentaron significativamente en 2021 en comparación con 2020, así como las pérdidas económicas ocasionadas por delitos cibernéticos. El reporte establece que todos los sectores poblacionales son susceptibles de ser víctimas, por ejemplo, en 2021 la población con edades entre 20 y 29 años de edad tuvo un incremento del 118.4% de denuncias en relación con el año anterior; así mismo, personas con edades entre 30 y 39 años un incremento del 90.5%, los de edades entre 40 y 49 tuvieron un incremento de 66,3%; el grupo con edades entre 50 y 59 un incremento del 48,8% y el grupo poblacional de más de 60 años un aumento del 74,4%. Llama la atención el sector poblacional de menores de 20 años, con un incremento del 42,9%, que, si bien es una cifra menor que las anteriormente señaladas, no es un porcentaje despreciable considerando el tipo de población a la que afecta.

En este sector poblacional no solo importan las cifras de pérdidas económicas -que están por el orden de los 71 millones de dólares según el informe del FBI-, sino el impacto que este tipo de delitos puede generar en el entorno emocional del individuo y la familia. El informe ha determinado que el medio por el cual se materializan los ataques son los canales de comunicación digital.

En Colombia, el Centro Cibernético Policial reveló que durante el 2021 este tipo de delitos ascendieron a 33.465, lo que significa un aumento de 17 % en relación con 2020 [2]. Se detalló que entre los principales delitos informáticos está el grooming, nombre que recibe la acción deliberada de un adulto de acosar sexualmente a una niña, niño o adolescente a través de un medio digital. Se registraron 516 incidentes de

este crimen. En segundo y tercer lugar está la sextorsión con 62 casos, y el ciberbullying con 325 casos.

En consideración a estas cifras, el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia hizo una serie de recomendaciones para prevenir que los ciudadanos sean víctimas de criminales en línea, sin embargo, se desconoce si al menos los menores están tomando acciones para mitigar las implicaciones de estos riesgos.

La conectividad actual de los electrodomésticos del hogar y de otros aparatos con conexión a Internet también conlleva riesgos, como el robo de credenciales, infecciones de virus, pérdidas de información y robos de dinero. Por lo tanto, es esencial que la población, especialmente los menores, adopte prácticas de seguridad para proteger su información y evitar estos incidentes.

Por lo anterior, conviene indagar si en nuestro país la población juvenil tiene prácticas de seguridad que eviten la afectación de la integridad, disponibilidad o confidencialidad de su información. Aunque cada ataque informático tiene un modo de operación diferente y tiene implicaciones diferentes en la información, algunas prácticas de seguridad permiten evitar este tipo de incidentes.

En este artículo, se presentarán los resultados del estudio realizado a estudiantes de educación media de instituciones educativas públicas y privadas, en el cual se indagó por las prácticas de seguridad de los estudiantes. El alcance de la investigación involucra determinar qué tan afianzadas están las buenas prácticas de seguridad en estudiantes de escuela secundaria para plantear posibles acciones para mitigar el problema planteado.

II. MARCO CONCEPTUAL

A. Herramientas de comunicación digital

Las herramientas de comunicación digital utilizan las tecnologías de la información y la comunicación para fomentar el diálogo, la interacción y el intercambio de información [3]. En el ámbito educativo, estas herramientas son fundamentales para el proceso de enseñanza y aprendizaje, ya que han revolucionado la forma en que estudiantes y profesores interactúan en el hecho educativo [4]. Las TIC son un apoyo en los entornos de aprendizaje presencial y virtual, y son utilizadas como instrumentos pedagógicos para innovar en los métodos de enseñanza.

Existen dos tipos de herramientas de comunicación digital: las asincrónicas y las sincrónicas. Las herramientas asincrónicas, como el correo electrónico y los foros, permiten la comunicación en tiempo no real, mientras que las herramientas sincrónicas, como los chats y las videoconferencias, posibilitan la comunicación en tiempo real. Ambas categorías de herramientas son útiles en el ámbito educativo y personal.

Las herramientas de comunicación digital son esenciales en la sociedad actual. En la educación, estas herramientas han cambiado la forma en que se enseña y se aprende, y han creado un nuevo paradigma de aprendizaje. Para la presente investigación, se tuvieron en cuenta herramientas sincrónicas y asincrónicas, pues ambas categorías de herramientas son demandadas en el ámbito educativo y de comunicación personal.

B. Prácticas de seguridad como parte de una representación social

Existe una relación muy estrecha entre las prácticas de un individuo y su representación social (en adelante RS). Una RS es el conjunto de conocimientos, valoraciones y actitudes que una persona tiene respecto a un objeto o concepto y que se establece a partir una construcción social. Las RS se estudian en el campo de la psicología social y constituyen la forma como una persona ve, comprende y entiende el mundo que lo rodea.

El concepto de RS fue acuñado por Moscovici [5] y caracteriza el pensamiento de sentido común como un conocimiento colectivo producto y proceso de una elaboración psicológica y social de lo real muy distinto al conocimiento científico. Este aspecto implica que las RS están relacionadas con el conocimiento que se construye cotidianamente.

Según Moscovici [4], las RS se integran en un grupo o en una relación cotidiana de intercambios; esto significa que, además de tener un carácter integrador porque en ellas confluyen varios elementos comunicativos, dan pautas de interacción en un contexto social. Es decir, las RS posibilitan un marco de referencia para la acción de los sujetos, ligadas a un conocimiento construido socialmente.

En consecuencia, las acciones que manifiestan los sujetos, son determinadas por su representación social; así mismo, estas acciones, vistas como formas espontáneas u organizadas dadas a nivel individual o grupal es lo que se denomina práctica. Cabe aclarar que no toda práctica se remite a una única representación, ni toda representación se asocia a una única práctica. Por esa razón, una práctica representa el accionar de un individuo a partir de sus hábitos y de la interiorización de un conocimiento que se ha adquirido a partir de un contexto social. Luego entonces, las prácticas en seguridad se conciben como aquellas acciones realizadas por un individuo, encaminadas a salvaguardar la seguridad de la información que maneja.

Muchos autores coinciden en que los usuarios son el eslabón más débil de la seguridad informática [6][7][16] y por esa razón, las prácticas de esos usuarios son especialmente importantes ya que determinan el inicio o no de la cadena de seguridad. A continuación, se presentan algunas prácticas de seguridad que normalmente se pueden considerar para conservar la integridad, confidencialidad y seguridad de la información:

a) Uso de antivirus con garantías. El antivirus es una herramienta fundamental para proteger equipos de cómputo. El objetivo del antivirus es escanear archivos con el fin de lograr la detección, identificación y eliminación de aplicaciones maliciosas o malware.

b) Actualización constante de las versiones de los programas. Cada programa informático desarrollado aborda el método de control de versiones para registrar los cambios que se incorporan en él. De esta manera, en cada versión se realizan mejoras encaminadas a disminuir los problemas y brechas de seguridad. Por esta razón, es muy importante que

el usuario se asegure de efectuar actualizaciones constantes de las versiones de sus programas, para asegurarse de contar con las mejoras en términos de vulnerabilidades.

c) Sistema de copias de seguridad o backup. Una copia de seguridad es una copia de datos que se hace con el fin de recuperarlos en caso de pérdida. Esta práctica es muy importante y debe realizarse cada vez que se hagan cambios a los archivos.

d) Evita usar redes públicas sin seguridad. las conexiones inalámbricas en lugares públicos como restaurantes, centros comerciales o aeropuertos pueden ser peligrosas para la seguridad de tu información. Los usuarios malintencionados pueden interceptar los datos que circulan en la red abierta. Es mejor evitar estas redes y utilizar una conexión segura y confiable en casa o en la oficina para proteger tu información.

e) Cifrado de información importante o confidencial. Un software de encriptación codifica la información para mantenerla segura y solo se puede leer con una clave secreta. Debe ser una práctica común en línea para evitar que la información importante sea entendida o utilizada por personas no autorizadas.

f) Uso de contraseñas seguras y diferentes para cada cuenta en línea. Muchos usuarios utilizan contraseñas débiles como números secuenciales o datos personales que pueden ser vulnerados desde la ingeniería social. Además, es común que los usuarios utilicen la misma contraseña en varias cuentas, lo que aumenta el riesgo de que sus datos sean comprometidos. Por esta razón, se recomienda utilizar contraseñas fuertes que contengan mayúsculas y minúsculas, caracteres alfanuméricos y que no estén relacionadas con información personal.

g) Evitar el acceso a sitios web desde enlaces externos. En su lugar, introduce directamente la URL del sitio en la barra de direcciones del navegador. Acceder a sitios web desde enlaces externos aumenta el riesgo de redireccionamiento a páginas falsas que buscan capturar contraseñas y datos personales. Para proteger tus datos, es importante que te asegures de estar accediendo al sitio web correcto.

h) Precaución con las descargas de archivos. Descargar archivos solo de fuentes confiables, como contactos de correo electrónico o sitios web, puede evitar que la información sea comprometida o que los equipos de cómputo o celulares sean vulnerados. Es importante tener en cuenta que la descarga de archivos malintencionados puede afectar la integridad, confiabilidad o seguridad de la información y, en algunos casos, incluso pueden ser utilizados para hackear los dispositivos.

C. Programas de seguridad digital en Colombia

El gobierno colombiano ha desarrollado programas para democratizar el acceso a internet y aumentar la competitividad desde 2010 [8]. "En TIC Confío" es un programa destacado que se enfoca en desarrollar habilidades digitales y prevenir riesgos en niños, jóvenes y adultos mayores, concientizándolos sobre la convivencia segura y responsable en el entorno digital y fomentando el uso positivo y transformador de internet para convertirse en agentes de cambio social en sus comunidades.

Este programa se potenció a través del documento CONPES 3854 de 2016, que establece lineamientos para la implementación de estrategias en seguridad digital y promoción de la cultura ciudadana en la era digital.

D. Normatividad colombiana en relación con las prácticas de seguridad de la información

En sintonía con la necesidad de formación de la población colombiana en temas de ciberseguridad, el Departamento Nacional de Planeación, a través del Consejo Nacional de Política Económica y Social -CONPES-, emitió unas acciones encaminadas a alcanzar estos objetivos. De esta manera, ha planteado dos documentos muy importantes: el CONPES 3701 de 2011, CONPES 3854 de 2016 y CONPES 3995 de 2020.

a) Ciberseguridad y ciberdefensa del país. Los lineamientos de política para ciberseguridad y ciberdefensa en el país se establecieron en el CONPES 3701 de 2011. A partir de esta política, se asignaron tareas a diferentes entes de control para la estandarización y acompañamientos en temas de ciberseguridad en el estado colombiano; esto conllevó a establecer planes de trabajo, alianzas nacionales e internacionales para promover el crecimiento de los temas de seguridad digital y ciberseguridad en las academias. Además, se dio instrucciones al Ministerio de Educación para establecer dichos lineamientos [9].

Este documento emitió la directriz de solicitarle a los ISP implementar controles de seguridad a las plataformas de conectividad del país, pues se convierten en infraestructura crítica para el tema de las comunicaciones digitales.

Adicionalmente, esta política de ciberseguridad y ciberdefensa permitió la creación de nuevas instancias como: el grupo de respuesta a emergencias cibernéticas de Colombia (colCERT); El Comando Conjunto Cibernético (CCOC); El Centro Cibernético Policial (CCP); El equipo de respuesta a incidentes de seguridad informática de la Policía Nacional (CSIRT PONAL); La Delegatura de protección de datos en la Superintendencia de Industria y Comercio; La Subdirección técnica de seguridad y privacidad de tecnologías de información del Ministerio de Tecnologías de la Información y las Comunicaciones y el Comité de ciberdefensa de las Fuerzas Militares. Todas estas instancias, de gran importancia para la Seguridad digital y ciberseguridad del país.

*b) Política Nacional de Seguridad Digital***.** La Política Nacional de Seguridad Digital fue establecida en el CONPES 3854 de 2016, convirtiendo a Colombia en el primer país latinoamericano en incluir las mejores prácticas internacionales en seguridad digital emitidas por la OCDE [10]. El objetivo de este documento fue establecer nuevos lineamientos para la defensa en entornos digitales, considerando diversos componentes. Desde la perspectiva educativa, el documento promovió la capacitación de los agentes del sistema educativo para generar confianza en el entorno digital y promover comportamientos responsables en el ciberespacio. Como parte de esta estrategia, el Ministerio de Educación Nacional implementó contenidos educativos

complementarios y capacitación para estudiantes de educación básica, media y superior a través del Portal Educativo "En TIC confío".

c) Política Nacional de Confianza y Seguridad Digital. Esta política fue establecida en el CONPES 3995 de 2020 [11] debido a la creciente vinculación de los ciudadanos al ciberespacio y al aumento de las amenazas y ataques de seguridad digital con consecuencias económicas y sociales. Esta política busca ampliar la confianza y mejorar la seguridad digital para lograr una sociedad más incluyente y competitiva en el ciberespacio. Aborda dos problemáticas: las debilidades en las capacidades de seguridad digital y la adopción de modelos y estándares de seguridad digital.

Por esa razón, en el marco de la Estrategia de Gobierno en Línea de la República de Colombia, se desarrolló el Modelo de Seguridad y Privacidad de la Información – MSPI con una recopilación de las mejores prácticas, nacionales e internacionales para conducir a la preservación de la confidencialidad, integridad, disponibilidad de la información y con ello, garantizar la privacidad de los datos mediante la aplicación de procesos de gestión de riesgos [12]. Este modelo fue desarrollado como parte del componente de Seguridad y privacidad de la información a través del Decreto Único Reglamentario 1078 de 2015.

La metodología del MSPI involucra buenas prácticas vigentes en normas como la 27005:2018, Margerit, Octave, ISO 31000 o la Guía No 7 - Gestión de Riesgos emitida por el MinTIC. Cabe aclarar, que el modelo aplica para entidades públicas de orden nacional y territorial, así como, proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptarlo. Esto significa que las instituciones educativas son una audiencia susceptible de aplicación.

Desde la perspectiva educativa, el plan de acción del CONPES 3995 delegó al SENA la coordinación y diseño de la estrategia de formación de capacidades en materia de seguridad digital. También se facultó al MinEducación para diseñar e implementar una estrategia para la creación de los hábitos de uso seguro y responsable de las TIC en el desarrollo de competencias y formación en seguridad y confianza digital que puedan incorporarse en los diferentes niveles de formación educativa.

d) Protección de datos personales. Uno de los grandes avances que se obtuvo a través de la expedición de los CONPES está relacionado con la generación de confianza digital. Desde esta perspectiva, se emitió la ley de protección de Datos Personales, Ley 1581 de 2012, cuyo objetivo es la regulación de la actividad de los datos, su carácter privado, semiprivado o público. Esto quiere decir que todos los ciudadanos colombianos de poder conocer, actualizar y rectificar la información que se haya recolectado y almacenado en bases de datos, archivos, videos o, verbal y que permita garantizar los demás derechos, libertades y garantías constitucionales como lo describe el artículo 15 de la Constitución Política. Desde la perspectiva de las instituciones educativas, esta ley de Habeas Data es muy importante porque brinda garantías sobre la preservación de la información, sobre todo cuando se trata de menores de edad.

III. Metodología

Esta investigación, con enfoque cualitativo y nivel descriptivo, involucró tres fases:

- Revisión documental de las categorías de análisis de la política colombiana sobre prácticas de seguridad.
- Recopilación de información mediante entrevistas semiestructuradas a 155 estudiantes de educación media de instituciones públicas y privadas en Bogotá y Florencia, Colombia, seleccionados por su nivel de uso y acceso a herramientas digitales.
- Descripción de las prácticas de seguridad en aplicaciones de comunicación digital de los estudiantes, utilizando técnicas de jerarquización y análisis de contenido.

El análisis de la información se realizó desde el enfoque estructural de la teoría de representaciones sociales con base en lo propuesto por Abric [13]. Este enfoque es reconocido porque asume características cercanas a la psicología social cognitiva de la línea estadounidense e involucra el abordaje del discurso como proceso socio-semiótico. Esto significa que, se emplean técnicas para abordar el lenguaje representado en el discurso como la forma más básica de construcción de la realidad social que se produce en la conversación espontánea y en las prácticas cotidianas. De esta manera, en la vía de lo planteado por Abric [13] se hizo uso de técnicas de jerarquización para la comprensión de su contenido y su estructura.

Se utilizó el software de análisis NVivo versión 12 de QRS Internacional para la codificación interactiva y automática de materiales de texto, así como el análisis de datos codificados y la construcción de modelos visuales basados en la frecuencia de palabras. Los mapas de nube generados permitieron identificar el núcleo central y elementos periféricos de las representaciones sociales de los estudiantes que participaron en el estudio.

IV. Resultados y Discusión

En esta investigación participaron 155 estudiantes de instituciones educativas públicas y privadas de Bogotá y Florencia, Colombia, con edades entre 14 y 17 años, de los cuales el 61.3% fueron estudiantes de sexo femenino. El 89.7% de los estudiantes cuenta con servicio de internet, siendo el 57.6% el que utiliza internet banda ancha, seguido de fibra óptica (27.3%) y telefonía móvil (37.4%). (Fig. 1).

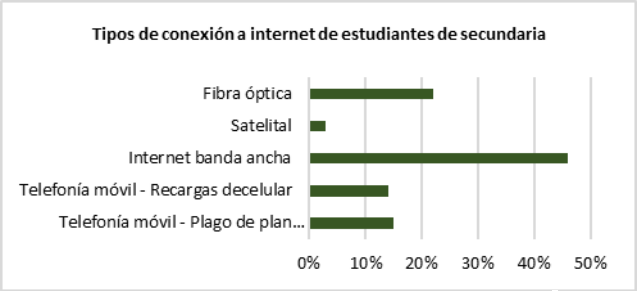

Fig. 1. Tipos de conexión a internet de estudiantes de secundaria.

Los principales dispositivos desde los que se conectan a internet son el celular y el computador, seguidos de los equipos de videojuegos. (Fig. 2)

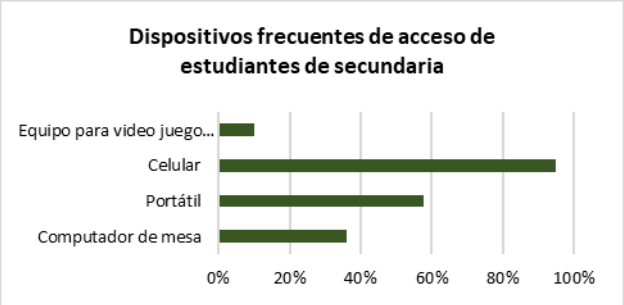

Fig. 2. Dispositivos frecuentes de acceso en estudiantes de secundaria.

Estos resultados coinciden con el Digital 2021 Global Overview Report [14] que indica que el 68% de la población colombiana utiliza internet y que las conexiones telefónicas móviles aumentaron en un 1.9% en 2021.

Según la misma fuente, para 2022 se proyectó alrededor de 1.1 millones de nuevos dispositivos móviles conectados, lo que significa que el porcentaje de usuarios de Internet aumentó en un 4.0% a lo largo de un año, es decir, aproximadamente 1.3 millones de nuevos internautas.

Es importante aclarar que, en el grupo indagado, el 81,3% de los estudiantes que poseen celular, no tienen un plan permanente de datos, situación que hace factible que los estudiantes se conecten desde redes públicas para acceder a internet. Esta práctica sin duda representa un riesgo, dado que la conexión a redes públicas, que en su mayoría carecen de configuraciones de seguridad, aumentan la vulnerabilidad de interceptación de comunicaciones.

En relación con aplicaciones de mensajería, la investigación permitió determinar que las aplicaciones de mensajería de uso más frecuente en estudiantes de secundaria son: WhatsApp, Messenger de Facebook e Instagram. (Fig. 3).

Fig. 3. Aplicaciones de mensajería más usadas por estudiantes de secundaria.

En términos de seguridad, esta información ratifica lo dispuesto por la Policía Colombiana que manifiesta que WhatsApp, Telegram, Facebook, Instagram y Snapchat son las aplicaciones de mayor uso para ejercer el delito de distribución de material de abuso sexual infantil, delito que pone en riesgo la seguridad digital de los niños, niñas y adolescentes. En necesario, en este aspecto, aumentar los esfuerzos de formación que permitan afianzar buenas prácticas de seguridad para el manejo de estas aplicaciones.

Por otro lado, es importante resaltar que las plataformas de mensajería institucionales, como las usadas en aulas virtuales o sistemas de notas no son habituales para los estudiantes. De hecho, el 44% manifestó no usarlas nunca (Fig. 4). Esto significa que hace falta incentivar a los estudiantes en este tipo de plataformas privadas, dado que pueden evitar riesgos como: suplantación y acoso, presentados normalmente en plataformas comerciales. Adicionalmente, el uso de mensajería privada, como la institucional, presenta ventajas porque se plantean protocolos de netiqueta en donde se cumplen reglas de comunicación respetuosas.

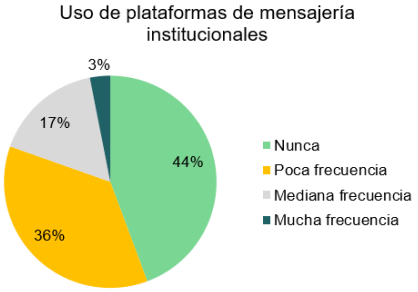

Fig. 4. Uso de plataformas institucionales

Es importante destacar que los autores consideran que esta actividad de uso y apropiación de las plataformas educativas, sin duda, deberían hacerlas las instituciones, quienes son las encargadas de implementar y capacitar a los actores vinculados (estudiantes, maestros y padres de familia).

En relación con las prácticas de seguridad, la investigación encontró conveniente indagar en los estudiantes qué comprendían por prácticas de seguridad para identificar qué tan arraigado estaba el concepto. Los datos del discurso se muestran en la Fig. 5.

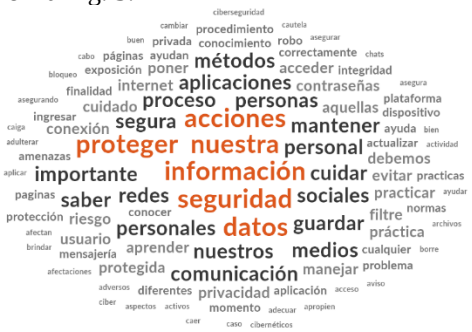

Fig. 5. Concepto de prácticas de seguridad de los estudiantes de secundaria

Los estudiantes conciben las prácticas de seguridad como las acciones personales que se ejecutan para proteger la información y la seguridad de los datos. Esta concepción sin duda está relacionada con el concepto de práctica de seguridad, pues se incorporan cogniciones como “acción”, “proteger”, “información”, “datos” y “nuestra”. Estas cogniciones dejan entrever que las prácticas son acciones que debe realizar cada sujeto por su cuenta y dependen del individuo, no de personas externas.

Posteriormente, se indagó por las prácticas de seguridad más comunes de los estudiantes; el resultado del discurso arrojó el mapa de nube que se muestra en la Fig. 6.

Fig. 6. Mapa de nube de prácticas de seguridad de estudiantes de secundaria

De acuerdo con la gráfica anterior, el núcleo central de la representación gira en torno a las cogniciones “ninguna”, “desconocidos”, “contraseña”, “personas”, “seguridad” y “correo”. Esto indica que, desde el contenido del discurso de los estudiantes, gran parte del grupo no aplica prácticas de seguridad y las que se aplican, están relacionadas con dos aspectos: a) el uso de contraseñas del correo electrónico y b) precauciones al interactuar con personas desconocidas. Las cogniciones asociadas al núcleo central permiten identificar otras prácticas con menor frecuencia, como: no abrir links extraños, uso de antivirus, no revelar datos o información personal (fotos, números de teléfono), por considerarse información privada. Esta frecuencia de palabras hallada en el discurso permite concluir que los estudiantes de educación secundaria son una población altamente susceptible a sufrir ataques informáticos debido a que las buenas prácticas de seguridad de la información no se llevan a cabo con frecuencia.

Además, se les pidió a los estudiantes que informaran la frecuencia con la que llevan a cabo buenas prácticas de seguridad en línea, como el cambio regular de contraseñas, la actualización de aplicaciones en dispositivos móviles y computadoras, evitar el almacenamiento de contraseñas en el navegador y rechazar solicitudes de amistad de desconocidos, entre otras. Sin embargo, los resultados revelaron que muchas de estas prácticas importantes no son llevadas a cabo con regularidad por los estudiantes, lo que representa un gran riesgo para su seguridad en línea. La Fig. 6 presenta los resultados detallados.

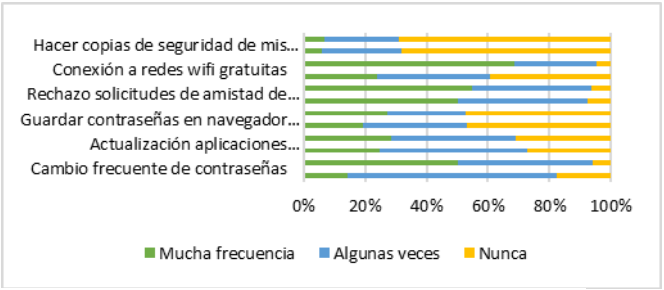

Fig. 7. Frecuencia de buenas prácticas de seguridad de estudiantes de secundaria.

Los resultados indican que menos del 10% de los estudiantes de secundaria ejecutan el conjunto de buenas prácticas de seguridad. Se denota que solo el 15% de los estudiantes de secundaria realiza con frecuencia el cambio de contraseñas, menos del 30% hace uso de contraseña segura, el 5% realiza copias de seguridad con frecuencia y solo el 8% evita usar la misma contraseña para todas sus cuentas.

En relación con acceso a las cuentas que implican registro con usuario y contraseña, preocupa en la información encontrada que solo el 32,3% de los estudiantes de secundaria tienen activado el doble factor de autenticación; el 13,5% no lo tiene activado y el 54,2% no sabe qué es. (Ver Fig. 8)

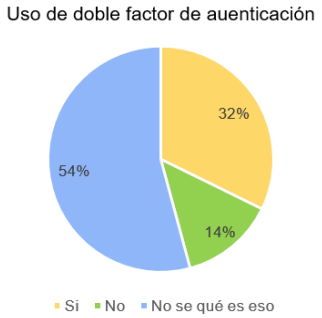

Fig. 8. Uso de doble factor de autenticación de estudiantes de secundaria

Los resultados dejan entrever que los estudiantes de escuela secundaria son usuarios que tienen alta vulnerabilidad de ser víctimas de ataques informáticos y están expuestos constantemente a estos peligros debido al uso frecuente de aplicaciones de mensajería. El estudio mostró que el 73% de los estudiantes de secundaria ha sido contactado por desconocidos a través de redes sociales y de ese grupo, el 52% ha aceptado las solicitudes de amistad. Así mismo, el estudio reveló que del 24% de los estudiantes que entablan conversaciones con desconocidos a través de redes sociales, el 25% materializó encuentros presenciales con personas extrañas. Esta situación es particularmente, grave porque esta falta de precauciones en los jóvenes puede conllevar a situaciones más graves como: abuso sexual, secuestro o incluso el asesinato.

Las anteriores cifras nos permiten esbozar que se debe realizar un trabajo importante en términos de ciber educación para lograr que esta población juvenil comprenda los riesgos de contactar con extraños. Para los autores, la cibereducación se constituye en el proceso de enseñanza y aprendizaje de temas relacionados con ciberseguridad que van más allá de la concienciación, como normalmente son llamados las acciones de capacitación en seguridad de la información. En consecuencia, la cibereducación es un proceso que involucra la apropiación de buenas prácticas de seguridad de un individuo de manera que se haga cotidiana su actuación cuando esté navegando por el ciberespacio. La apropiación en TIC se aborda desde lo concebido por Rojas-Bahamón [15], esto es, un proceso de interiorización de las acciones tecnológicas de un individuo de tal manera que se incorporen a su comportamiento diario debido a la repetición contante.

En Colombia, se han implementado políticas y estrategias desde 2011 para brindar seguridad y defensa en el ciberespacio, según se puede ver en la figura 9. La normativa comenzó con el documento CONPES 3701, seguido por la Ley 1581 en 2012 y el CONPES 3854 en 2016. En 2018, la política de Gobierno Digital estableció la seguridad digital como habilitador transversal, y en 2019 se generaron varios documentos enmarcados en la seguridad de la información,

incluyendo la política de seguridad y confianza digital en el plan Nacional de Desarrollo 2018-2022 y el Plan TIC 2018-2022 con proyectos e iniciativas relacionadas con la seguridad digital. También se estableció la política de Defensa y Seguridad y se emitió el CONPES 3975 que formuló una política pública sobre ciberseguridad. La última normativa generada fue el CONPES 3995 de 2020, que abordó la política Nacional de Confianza y Seguridad Digital.

Fig. 9. Normatividad colombiana relacionada con seguridad de la información

Sin embargo, aunque el país está a la vanguardia en el planteamiento de políticas relacionadas con la seguridad de la información y el ciberespacio, aún falta mucho camino por recorrer en relación con la ejecución de acciones que conlleven a la educación en ciberseguridad o cibereducación, término que proponen los autores.

Es importante reconocer que existen avances reconocidos en términos de capacitación, como el programa En TIC Confío que provee diversos cursos de formación, como se muestra en la Fig. 10.

Fig. 10. Cursos de formación en TIC confío por rangos de edad. Basado en web En TIC Confío [17]

Otras entidades desarrollan programas importantes como el instituto Colombiano de Bienestar Familiar, la Policía Nacional y diversas universidades públicas y privadas del país que incorporan en sus sitios web diversos *tips* de seguridad mientras el usuario está en el ciberespacio.

No obstante, estos procesos de capacitación aún no son ampliamente difundidos en la población escolar colombiana. El 60% de los estudiantes consultados afirmó que sus instituciones educativas no han brindado capacitación en seguridad de la información, y el 43,2% no ha recibido capacitación del programa "En TIC confío". Estos resultados indican la necesidad de establecer procesos de formación en temas de buenas prácticas de seguridad digital para los estudiantes.

Además, según López et al. [18], los profesores son una parte esencial en este proceso. La implementación de prácticas de seguridad digital para estudiantes de escuela secundaria solo es posible si se establecen procesos sólidos de integración de los profesores en el uso y la apropiación de las TIC [19] [20]. Este aspecto también se convierte en un elemento clave de la política de calidad en educación y seguridad digital en el país. A pesar de la falta de capacitación formal, el 94,8% de los estudiantes de secundaria se muestra interesado en aprender sobre seguridad de la información, lo que indica una disposición a desarrollar hábitos de seguridad digital.

Finalmente, la comprensión de la problemática relacionada con la cibereducación en instituciones educativas requiere resolver nuevos interrogantes, como los siguientes: ¿cómo es la infraestructura de las instituciones educativas colombianas públicas y privadas en términos de seguridad?, ¿Cuál es la prospectiva que tienen las instituciones educativas en estos campos?, ¿Cuál es el papel de los entes territoriales en la consolidación de la política de ciberseguridad estatal?, ¿Qué prácticas de seguridad están realizando los diferentes miembros de la comunidad educativa de las instituciones en el país?

Seguramente las respuestas a estas preguntas, que deberán hallarse a partir de procesos de investigación, podrán ampliar el panorama de acciones a seguir para mejorar las prácticas de seguridad en estudiantes de escuela secundaria.

IV. Conclusiones

Colombia es un país pionero y líder en la región en cuanto a la existencia de políticas relacionadas con la seguridad en el entorno digital, normativa que se ha implantado en gran medida por la adherencia de Colombia a la OCDE. Esta normativa se puede evidenciar con la emisión del documento CONPES 3701 de 2011, Ley 1581 de 2012, el documento CONPES 3854 de 2016, la política de Gobierno Digital en 2019, la política de seguridad y confianza digital dispuesta en el plan Nacional de Desarrollo 2018-2022, el Plan TIC 2018-2022, la política de Defensa y Seguridad, el documento CONPES 3975 de 2019 y el CONPES 3995 de 2020.

A pesar de la existencia de la política, que sin duda es un gran avance, aún existen falencias con el proceso de implementación de esta normativa en lo relacionado específicamente con prácticas de seguridad de la información.

El estudio permite determinar que en Colombia aún se tienen deficiencias relacionadas con la cibereducación (educación en seguridad de la información), a la población estudiantil de básica secundaria, tanto en el ámbito público como privado. Esto, causa que el país presente bajos niveles de preparación y avance en la materia, facilitando al ciberdelincuente el aprovechamiento de las vulnerabilidades del usuario.

La falta de cibereducación de los estudiantes de secundaria se convierten en una vulnerabilidad importante que puede llegar a afectar a los menores en términos de seguridad personal e incluso emocional. Así mismo, pueden aumentar significativamente los casos ya reportados por el Centro Cibernético Policial Colombiano, como sextorsión, ciberbullying, distribución de material de abuso sexual infantil o incluso, secuestro y asesinato.

La falta de procesos educativos de la población objeto de estudio en esta investigación, abren la brecha de seguridad que podría deteriorar la confianza y seguridad del entorno digital en el País, aspecto que, sin duda, tendría una incidencia importante en la seguridad estatal.

REFERENCIAS

[1] FBI, “Elder Fraud Report”. Recuperado de https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3ElderFraudReport.pdf (accedido el 28 de marzo de 2022).

[2] Infobae. "Delitos informáticos en Colombia subieron un 17 % en el 2021: sepa cómo prevenirlos". infobae. https://www.infobae.com/america/colombia/2021/12/27/delitos-informaticos-en-colombia-subieron-un-17-en-el-2021-sepa-como-prevenirlos/ (accedido el 14 de marzo de 2022).

[3] F. Tiberio, M.L. Sevillano, and M. C. Ricoy, "Competencias para la utilización de las herramientas digitales en la sociedad de la información," Educación XX1, vol. 13, no. 1, pp. 199-219, 2010, ISSN: 1139-613X, disponible en: https://www.redalyc.org/articulo.oa?id=70618037009.

[4] M. J. Rojas-Bahamón, «La publicación científica en docentes colombianos», Eduweb, vol. 16, n.º 1, pp. 72–89, abr. 2022.

[5] S. Moscovici. El psicoanálisis, su imagen y su público. Buenos Aires: Huemul S.A., 1979.

[6] CYBEREOP. “Los usuarios, el eslabón débil de la seguridad informática”. https://www.cybereop.com/blog/los-usuarios-el-eslabon-debil-de-la-seguridad-informatica.html. 2021.

[7] C. Milio, Homo Sapiens, el eslabón débil de la seguridad de la información. Revista Abierta De Informática Aplicada, 4. http://portalreviscien.uai.edu.ar/OjS/index.php/RAIA/article/view/12. 2021.

[8] MinTIC.ProgramaViveDigital.https://mintic.gov.co/portal/vivedigital/612/w3-article-1511.html. (accedido 14 May 2022).

[9] Consejo Nacional de Política Económica y social. “Documento CONPES 3701. Lineamientos de política para ciberseguridad y ciberdefensa·. Bogotá. 2011.

[10] Portafolio. “Para el país, la seguridad digital es una política nacional”. https://www.portafolio.co/economia/gobierno/conpes-aprobo-nueva-politica-seguridad-digital-colombia-494057. 2016. (accedido el 18 de abril 2022)

[11] Consejo Nacional de Política Económica y social. Documento CONPES 3995. Política Nacional de Confianza y Seguridad digital. Bogotá. 2020.

[12] MinTIC. Modelo de Seguridad y Privacidad de la Información. https://bit.ly/3zioYTB3. 2016.

[13] J.C. Abric. Les représentations sociales: aspects théoriques. Paris: Presses universitaires de France. 1994.

[14] "Digital Report 2021: El informe sobre las tendencias digitales, redes sociales y mobile. - We Are Social Spain". We Are Social Spain. https://wearesocial.com/es/blog/2021/01/digital-report-2021-el-informe-sobre-las-tendencias-digitales-redes-sociales-y-mobile/. (accedido el 11 de mayo de 2022)

[15] M. Rojas Bahamón, "Diagnóstico acerca del uso y apropiación de las TIC como mediación didáctica," Amazonia Investiga, vol. 1, no. 1, pp. 5-18, Dec. 2012.

[16] D. F. Arbeláez-Campillo, M. Andreyevna Dudareva, y M. J. Rojas-Bahamón, «Las pandemias como factor perturbador del orden geopolítico en el mundo globalizado», CP, vol. 36, n.º 63, pp. 134-150, mar. 2020.

[17] Ministerio de Tecnologías de la información y las comunicaciones. Programa en TIC Confío. Disponible en: www.enticconfio.gov.co. (accedido en: 11 de mayo de 2022)

[18] L. López de Parra, L. Correa Cruz, y M. J. Rojas Bahamón, «Representaciones sociales: formación y uso de tecnologías de información y comunicación. Profesores de educación básica secundaria», Rev. virtual univ. catol. norte (En línea), n.º 50, pp. 256–276, may 2017.

[19] O. Budnyk, “Formation of tolerance in the inclusive environment of an educational institution”, Amazonia Investiga, vol. 11, no. 56, pp. 305-319, Oct. 2022.

[20] O. Kozmenko, I. Popovych, D. F. Arbeláez-Campillo, M. J. Rojas-Bahamón, and L. Volchenko, “Structural and functional model of the successful person training in USA colleges and universities”, Amazonia Investiga, vol. 11, no. 55, pp. 143-155, Oct. 2022.

Magda Julissa Rojas-Bahamón. Ingeniera de Sistemas de la Universidad Distrital Francisco José de Caldas. Esp. en Seguridad de la Información. Magíster en Ciencias de la Educación, Doctora en Educación y Cultura Ambiental de la Universidad Surcolombiana y Posdoctora en Ciencias de la Educación. Directora del grupo de investigación PRIMMATE categoría C de Colciencias. Ha desarrollado varios proyectos de investigación en el ámbito de TIC y educación, educación ambiental, residuos tecnológicos, conflictos socioambientales, publicación científica y seguridad de la información en ambientes educativos.
ORCID: https://orcid.org/0000-0003-4882-1476.

Alejandro Pulido Jiménez. Ingeniero de sistemas de la Fundación Universitaria Los Libertadores y Especialista en Seguridad de la Información de la misma universidad. Es Certificado Auditor ISO 27001. Tiene formación como project management profesional (PMP), interno, ITIL Fundamentos y auditoría interna. Tiene amplia experiencia en soluciones de seguridad informática, análisis de bases de datos a través de ACL, Revisión e implementación de herramientas equipos perimetrales firewall, IDS analizadores de eventos y actividades relacionadas con seguridad de la información en empresas públicas y privadas. ORCID: https://orcid.org/0000-0001-7609-4961

Yenny Isabel Serrato Rodríguez. Especialista en Seguridad de la Información de la Universidad Sergio Arboleda e Ingeniera en Telemática de la Universidad Distrital Francisco José de Caldas. Es certificada como: CEH, Auditor Líder e interno ISO 27001:2013, Auditor interno ISO 22301:2019, ITIL, Cobit, Scrum Foundations, entre otros. Adicional, posee conocimientos en informática forense, ciberseguridad, auditoría interna y manejo de proyectos. Se ha desempeñado como Oficial de seguridad de la información para empresas multinacionales, consultor para empresas públicas y privadas liderando equipos de trabajo multidisciplinarios, además docente universitario en varias universidades.