Revista Logos, Ciencia & Tecnología
ISSN 2145-549X (impreso)
ISSN 2422-4200 (en línea)

Estudio de caso

Prácticas de seguridad de información del Nivel Ejecutivo de la Policía Nacional de Colombia: Escuela de Policía Simón Bolívar (Tuluá, Colombia)

Information security practices of the executive level of the Colombia national police. Escuela de Policía Simón Bolívar Tuluá case

Práticas de segurança da informação do nível executivo da Polícia Nacional da Colômbia: Escola de Polícia Simón Bolívar Tuluá, Colômbia

Royer David Estrada-Esponda[a*] | José Luis Unás-Gómez[b] | Oleskyenio Enrique Flórez-Rincón[c]

[a] http://orcid.org/0000-0002-6849-1278
[b] http://orcid.org/0000-0001-6359-3104
[c] http://orcid.org/0000-0002-4056-6565
Universidad del Valle, Tuluá, Colombia

- **Fecha de recepción:** 2019-10-03
- **Fecha concepto de evaluación:** 2019-10-30
- **Fecha de aprobación:** 2019-11-04
http://dx.doi.org/10.22335/rlct.v12i1.1050

Para citar este artículo / To reference this article / Para citar este artigo: Estrada-Esponda, R. D., Unás-Gómez, J. L. y Flórez-Rincón, O. E. (2019). Prácticas de seguridad de información del Nivel Ejecutivo de la Policía Nacional de Colombia: Escuela de Policía Simón Bolívar (Tuluá, Colombia). *Revista Logos Ciencia & Tecnología*, *12*(1), 121-131. http://dx.doi.org/10.22335/rlct.v12i1.1050

RESUMEN

El uso de diferentes tipos de tecnología es cada vez más frecuente en un mayor y variado grupo de personas. En ese sentido, los estudiantes del programa Técnico Profesional en Servicio de Policía y policías profesionales de la Escuela de Policía Simón Bolívar no son la excepción. Por ello, se decidió estudiar, desde los enfoques cuantitativo y cualitativo, el tipo de prácticas, desde el punto de vista de seguridad de la información, que ambos grupos aplican en la cotidianidad de sus actividades. Así pues, se validó y aplicó un instrumento conformado por cinco variables, para determinar fortalezas y debilidades en la seguridad de la información. Como resultados, se encontró que en promedio los comportamientos y conocimientos sobre seguridad de la información son de nivel medio y, por tanto, el riesgo de verse asociados a problemas en esa materia es alto, lo cual implica una necesidad de rediseñar programas de capacitación continua y mantener en el *pensum* académico asignaturas que incluyan unidades referentes a buenas prácticas de seguridad de la información.

Palabras clave: Alfabetización informacional, seguridad de los datos, protección de datos, seguridad, policía

* Autor para correspondencia. Correo electrónico: royer.estrada@correounivalle.edu.co

SUMMARY

The use of different types of technology is increasingly common in a larger and more varied group of people. In that sense, the students of the Professional Technical Program in Police Service and professional police officers of the Simón Bolívar Police School are no exception. Therefore, it was decided to study, from the quantitative and qualitative approaches, the type of practices, from the point of view of information security, which both groups apply in the daily life of their activities. Thus, an instrument consisting of five variables was validated and applied to determine strengths and weaknesses in information security. As a result, it was found that on average the behaviors and knowledge about information security are medium level and, therefore, the risk of being associated with problems in this area is high, which implies a need to redesign continuous training programs and keep in the academic curriculum subjects that include units referring to good information security practices.

Keywords: information literacy, data security, data protection, security, police (Unesco Thesaurus).

SUMÁRIO

O uso de diferentes tipos de tecnologia é cada vez mais comum em um grupo maior e mais variado de pessoas. Nesse sentido, os alunos do Programa Técnico Profissional no Serviço Policial e os policiais profissionais da Escola de Polícia Simón Bolívar não são exceção. Portanto, optou-se por estudar, a partir das abordagens quantitativa e qualitativa, o tipo de práticas, do ponto de vista da segurança da informação, que ambos os grupos aplicam no cotidiano de suas atividades. Assim, um instrumento composto por cinco variáveis foi validado e aplicado para determinar os pontos fortes e fracos da segurança da informação. Como resultado, verificou-se que, em média, os comportamentos e conhecimentos sobre segurança da informação são de nível médio e, portanto, o risco de estar associado a problemas nessa área é alto, o que implica a necessidade de redesenhar os programas de treinamento contínuo. e manter no currículo acadêmico assuntos que incluem unidades referentes a boas práticas de segurança da informação.

Palavras-chave: alfabetización informacional, seguridad de los datos, protección de datos, seguridad, policía (Tesauro de la Unesco).

La seguridad de la información y la seguridad informática no son sinónimos, sino que la primera abarca la segunda. La seguridad informática hace referencia a la seguridad de los sistemas de información, redes y equipos de cómputo, y por tanto está circunscrita a la información automatizada. Por su parte, la seguridad de la información se ocupa de la información en todas sus formas, tales como oral, escrita, impresa, electrónica, óptica, electromagnética, entre otras (Porras, 2018).

Por otro lado, las tecnologías de la información y de la comunicación (TIC) se han convertido en un aspecto fundamental para todas las personas; hacen parte de su diario vivir, por ello, es común encontrar que una persona pueda tener tres o más dispositivos con acceso a internet, tales como *tablets*, computadores, celulares y, en general, dispositivos móviles. También existe una gran cantidad de aplicaciones y servicios a los que se ingresa frecuentemente, tales como portales bancarios, aplicaciones corporativas, páginas web, compras *on line*, redes sociales, entre otros. Esta facilidad de estar conectado con todo y con todos trae consigo el cuidado del cómo se accede a estos recursos, qué se comparte, con quién se establecen relaciones digitales y las operaciones o transacciones que se practican. En este sentido, de acuerdo con Unisys (2019), la preocupación de los colombianos frente a problemas de seguridad digital ha aumentado y es el más alto en los últimos seis años.

Según Unisys (2019), en Colombia, el 85 % de los ciudadanos han sido víctimas o conocen víctimas de algún tipo de delito o intento de delito informático. Mientras que a nivel global la preocupación por la seguridad digital es de 175 puntos, Colombia está 45 puntos por encima de la media global con 220 puntos sobre 300 posibles. De los países encuestados, Colombia es el segundo con la mayor

preocupación por la seguridad informática, ubicada solo detrás de Filipinas.

En el mismo estudio de Unisys (2019), se puede observar cómo las personas más jóvenes están más preocupadas por su seguridad digital (jóvenes entre 18 y 24 años con un índice de 230 puntos) frente a personas mayores (55 a 65 años con un índice de 212 puntos). Asimismo, las personas que no cuentan con educación universitaria tienen un mayor grado de preocupación por su seguridad digital versus las personas que sí tienen algún grado de formación universitaria; 225 puntos frente a 215 puntos, respectivamente. Por último, se concluye que las personas que generan menos ingresos se preocupan más en este ámbito, frente a las personas con mayores ingresos, con 224 puntos contra 215 de quienes tienen mayores ingresos.

Desde la perspectiva financiera, en 2017 se presentaron 198 millones de incidentes informáticos en el país, es decir, 542 465 incidentes diarios, que representaron pérdidas por USD 6179 millones. El sector financiero se encontró en el primer lugar de los incidentes con 214 000 diarios, seguido del sector de las telecomunicaciones con 138 329 eventos, el Gobierno con 83 756 y el sector industrial con 51 263 (*El Tiempo*, 2017). Según lo anterior, las denuncias por delitos informáticos incrementaron en Colombia de 2017 a 2018 en un 36 %, de modo que es el artículo 269i (hurto por medios informáticos) del Código Penal colombiano el más denunciado, con 41 755 casos (Durán, 2019).

Según el informe anual sobre seguridad de Symantec, en Colombia uno de cada 328 correos electrónicos son maliciosos y una de cada 11 URLs en correos electrónicos también lo son; este mismo informe deja en descubierto que los empleados de organizaciones pequeñas tienen una posibilidad más alta de ser víctimas de correos electrónicos fraudulentos tipo *spam*, *phishing* y *malware*, frente a empleados de grandes corporaciones. El *phishing* pasó de uno de cada 2995 correos electrónicos en 2017 a uno de cada 3207 en 2018 (Symantec, 2019).

Entretanto, en 2018, hubo un crecimiento del 400 % de eventos de *cryptojacking*, comparado con los detectados en 2017. Por ello, la seguridad de los dispositivos móviles es un gran desafío para la industria tecnológica. En uno de cada 36 dispositivos móviles, se instalaron aplicaciones de alto riesgo, de modo que son las aplicaciones de herramientas (39,1 %), estilo de vida (14,9 %) y entretenimiento (7,3 %) las que encabezan el *ranking* de las principales categorías en las que se aloja código malicioso; además, las infecciones con *ransomware* en móviles crecieron un 33 % respecto de 2017. En el mismo año, los delitos informáticos más comunes fueron la estafa (compraventa por internet), *malware*, suplantación de identidad, *phishing*, *vishing*, amenazas a través de redes, *smishing*, publicación no autorizada de imágenes o videos, injuria y calumnia en redes sociales, sextorsión, ingeniería social, *cyberbullying*, carta nigeriana, *defacement*, *ransomware*, *skimming*, *grooming*, *spoofing*, *turinet* y DoS (por sus siglas en inglés). De los anteriores, los tres primeros delitos, según las denuncias, son el *malware* con 1943 casos, seguido de la suplantación de identidad con 1277 casos y, en el tercer puesto, el *vishing* con 1271 casos (Symantec, 2019).

Ahora bien, es importante mencionar que, como cualquier otro ciudadano, el policía profesional o incluso los estudiantes del programa Técnico Profesional en Servicio de Policía que se imparte en la Escuela de Policía Simón Bolívar (ESBOL) (Tuluá, Valle del Cauca) están expuestos a diferentes modalidades de crímenes en el ámbito informático. Por eso, en esta unidad académica se imparte la cátedra Tecnologías Aplicadas al Servicio de Policía, que, dentro de su contenido programático, en la unidad 2, incluye temas referentes a la seguridad de la información.

Este artículo tuvo como propósito realizar una revisión sobre las prácticas de seguridad de la información aplicadas o instanciadas por el personal del Nivel Ejecutivo de la Policía Nacional de Colombia, para poder caracterizar algunas prácticas que pudieran ser etiquetadas como "buenas" y "malas", y recomendar algunas estrategias para la consolidación de las buenas prácticas y la minimización de aquellas que fueron etiquetadas como malas o negativas.

Finalmente, el artículo se estructura de la siguiente manera: primero, se presentan trabajos que sustentaron la investigación desde el punto de vista conceptual, luego la metodología de la investigación, más adelante los resultados y la discusión, y, por último, las conclusiones.

Trabajos relacionados

A continuación, se reseñan los principales documentos de referencia que sirvieron para la planificación y el desarrollo de la investigación, particularmente desde el componente metodológico en la medida en que cada trabajo revisado sirvió para la identificación de diferentes variables y, por tanto, la formulación de las diferentes preguntas que fueron incluidas en el instrumento de recolección de información. La tabla 1 presenta el insumo utilizado para

la identificación de cada una de las variables estudiadas durante la investigación.

Metodología

Según el problema expuesto y la revisión de la literatura, se planteó una investigación aplicada con enfoques cuantitativos y cualitativos; el primero para facilitar la generalización de resultados a toda la base de la Policía Nacional y el segundo para de poder responder a los problemas con propuestas desde la misma institución policial. La investigación se desarrolló en tres fases: la fase de diseño de los instrumentos de recolección de información, la fase de aplicación de los instrumentos y la fase de análisis de la información recolectada.

La figura 1 sintetiza el marco metodológico utilizado.

Fase de diseño

Se construyó un instrumento de recolección de información compuesto por cinco variables y treinta subvariables; para ello, fue necesario revisar instrumentos de investigaciones similares y realizar un proceso de consolidación como variable dependiente la seguridad de información aplicada por estudiantes y profesionales adjuntos a la ESBOL. De igual modo, se procedió a realizar la validación de este instrumento por medio de la realización de una prueba piloto con nueve estudiantes del programa Técnico Profesional en Servicio de Policía. Durante el ejercicio de pilotaje, se señalaron con mayor nivel de ocurrencia dos preguntas del instrumento, que fueron ajustadas para el cuestionario definitivo. Finalmente, durante el análisis de los resultados, fue posible calcular un alfa de Cronbach del 84 %, lo cual permitió establecer que el cuestionario es consistente internamente y es útil para poblaciones mucho mayores. El diseño estadístico y el cuestionario completo están disponibles en un repositorio público.[1]

Fase de aplicación

Consistió en la aplicación del instrumento descrito en la fase anterior. Vale la pena aclarar que, conforme al diseño estadístico, el propósito era aplicar el instrumento a 28 policías profesionales adjuntos a la ESBOL y a 174 estudiantes del programa técnico; sin embargo, gracias a la diligencia de su personal, para el caso de estudiantes, el cuestionario pudo ser aplicado a 468 personas, casi la totalidad de personal de ese rango, lo cual, sin duda, mejoró la generalización. Desde el punto de vista de confidencia-

1 https://drive.google.com/drive/folders/1KyzlWw2O_jtOTj0l6FxAn74J4TIwRFTG

Tabla 1. Revisión literatura: identificación de variables

Trabajo	Referencias	Variables	Preguntas
"Making passwords secure and usable"	Adams, Sasse y Lunt (1997)	• Seguridad en contraseña	24,25,30
Buenas prácticas en seguridad informática	Mieres (2009)	• Seguridad en redes P2P • Seguridad en mensajería instantánea • Seguridad en redes sociales • Protección a correos electrónicos • Seguridad en la navegación • Actualización de sistemas operativas y aplicaciones	13,21,3,6,7,11,24
"La seguridad en las competencias digitales de los *millennials*"	Castillejos, Torres y Lagunes (2016)	• Protección de dispositivos • Protección de datos personales	26,9,10,12
"Conceivable security risks and authentication techniques for smart devices: A comparative evaluation of security practices"	Muzammal, Shah, Zhang y Yang (2016)	• Protección de datos en dispositivos inteligentes • Seguridad en contraseña	24,25,30,26 y 29
"Why do some people manage phishing e-mails better than others?"	Pattinson, Jerram, Parsons, McCormac, y Butavicius, (2012)	• Familiaridad con computadoras • Seguridad en correo electrónico • *phishing*	1,3,11,24 y 20
"Power to the people? The evolving recognition of human aspects of security"	Furnell y Clarke (2012)	• Uso de antivirus • Autenticación • Factores humanos	23,24,25,26,27,28
"Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios"	Hernández, Ventura y Juárez (2018)	• Conocimientos sobre seguridad	16,17,18,19,20
"Self-efficacy in information security: Its influence on end users' information security practice behavior"	Rhee, Kim y Ryu (2009)	• Alfabetización informática	1,2,3,9,10,11,12,14,23,24,25,26,27

Figura 1. Proceso metodológico.

lidad, no fue necesario realizar ningún comité ético en la medida en que las respuestas de todos los individuos fueron anónimas. En cuanto a la ubicación espacial, la prueba piloto se realizó en las instalaciones de la Universidad del Valle, sede Tuluá, mientras que el test definitivo se aplicó por medio de Google Forms.

Fase de análisis

Se procedió a tabular y analizar 496 respuestas de estudiantes del programa técnico y profesionales adjuntos a la ESBOL. En este proceso, fue posible generar una discusión relacionada con cada una de las variables objeto de estudio. Paralelamente, y desde una dimensión documental, se revisó el plan de estudios del programa Técnico Profesional en Servicio de Policía, con énfasis en las asignaturas Ambientes Educativos Saludables, Tecnologías Aplicadas al Servicio de Policía y Seguridad Integral. Finalmente, una vez realizada la tabulación de información y la revisión documental, se plantearon algunas conclusiones según las debilidades identificadas en cuanto a seguridad de la información.

Resultados

Según el trabajo de campo realizado, fue posible identificar que, para el caso de los policías profesionales adjuntos a la ESBO, el mayor número se concentra en los intendentes, con un 39,29 %, seguido de los patrulleros con un 32,14 %, subintendentes con un 21,43 % y, en una misma frecuencia, en los comisarios y subcomisarios con un 3,57. %. La figura 2 detalla esta información.

Por otra parte, el 99 % de los individuos evaluados, tanto profesionales como estudiantes, son de sexo masculino, esto es explicable en la medida en que en la ESBO no hay oferta académica para mujeres, ya que otros centros se ocupan de ello. En cuanto al origen de procedencia, el

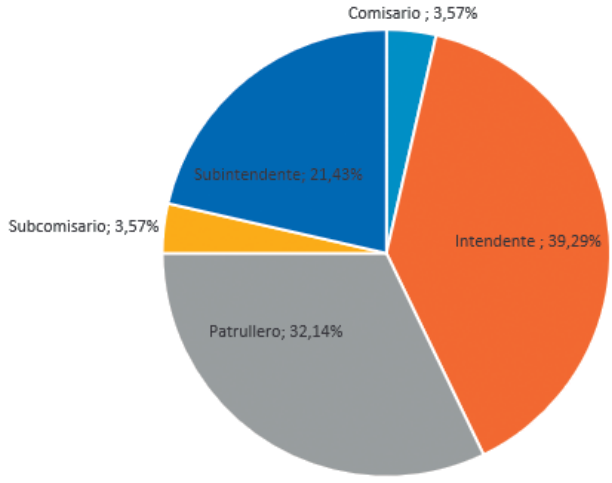

Figura 2. Distribución de profesionales por rango.

44,02 % de los estudiantes provienen del departamento de Nariño, el 32,69 % del departamento del Valle del Cauca, el 13,25 % del departamento del Cauca y el resto de otros departamentos, no solo del suroccidente colombiano, sino también de todo el país.

En relación con la formación académica, el 96,79 % de los estudiantes tienen estudios de secundaria, el 0,43 % estudios de primaria y solo el 2,78 % estudios profesionales. Para el caso de profesionales, la distribución por formación académica cambia significativamente; así pues, el 52,63 % acreditan estudios de secundaria, el 23,68 % estudios profesionales, el 10,53 % estudios de maestría, el 10,53 % estudios de especialización y solo el 2,63 % estudios de primaria. En relación con la edad, se encuentra que el individuo más joven tiene 18 años, mientras que el individuo con más edad alcanza los 50 años. El promedio general de edad es de 31 años, sin embargo, para estudiantes el promedio es de 23 años, mientras que para profesionales asciende a 37 años. Finalmente, respecto de la antigüedad del personal, el 91 % de ellos llevan cuatro o menos años en la ESBO. Lo señalado busca caracterizar,

en algún grado, al personal de la ESBO, para introducir el análisis de variables que a continuación se presentan.

Alfabetización informática

En cuanto a la variable de *Alfabetización informática*, se observa que el conocimiento que dicen tener tanto estudiantes como policías profesionales no es consistente entre regiones. Así es que, por ejemplo, en el departamento de Nariño, el 32,06 % de los individuos manifiestan tener conocimientos buenos sobre las nuevas tecnologías, mientras que en el departamento del Cauca solo el 8,30 % manifestaron lo mismo.

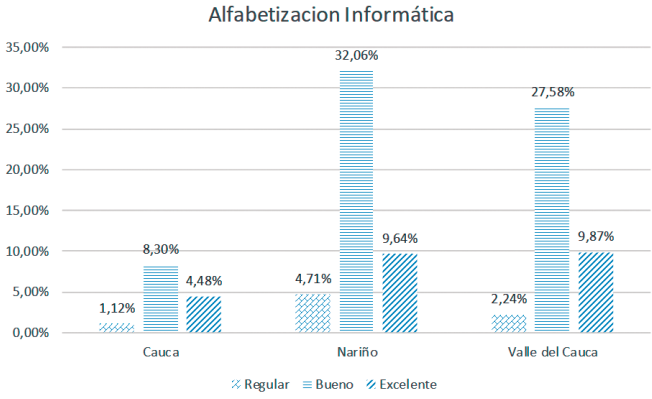

Figura 3. Alfabetización informática por departamento de origen.

Del mismo modo, durante una revisión documental fue posible estudiar el *pensum* del programa Técnico Profesional en Servicios de Policía, en el que se encontró que en el primer periodo del nivel básico deben cursar la asignatura Tecnologías Aplicadas al Servicio de Policía. Este curso está dividido en tres unidades; la segunda unidad trata sobre seguridad de la información que a su vez se divide en conceptos básicos sobre seguridad de la información (a), protección en la red (b) y redes sociales (c). Como parte de la revisión, fue posible calcular el promedio de calificaciones cuantitativas a un grupo de 49 estudiantes de una misma compañía para el periodo marzo-septiembre de 2019. La tabla 2 contiene el promedio por cada sección.

Tabla 2. Calificaciones asignatura Tecnologías Aplicadas al Servicio de Policía

Sección	Promedio
Conceptos básicos sobre seguridad de la información	4,3
Protección en la red	4,0
Redes sociales	4,1
Promedio general	4,1

El promedio general permite señalar que, según el criterio profesoral, los estudiantes tienen un buen desempeño desde el punto de vista de la asignatura Tecnologías Aplicadas al Servicio de Policía. Por otra parte, también fue posible revisar el perfil profesional y académico para dirigir el curso en mención, allí se evidenció que la ESBO como centro de formación requiere para este curso un profesional del área de ingeniería de sistemas, telemática o afines. De igual modo, señala que preferiblemente cuente con certificación ISO 27001:2013 e ISO 27001:2005, y de manera opcional con un curso sobre *hacking* ético.

Familiaridad con las computadoras o dispositivos

Para la variable *Familiaridad con las computadoras o dispositivos*, se usó como referencia para las escalas de valoración a Deloitte (2017). Sin embargo, se añadió la última opción "Eventualmente", para no excluir a personas que usan dispositivos no tan frecuentemente. De igual modo, se eliminó del procesamiento la pregunta "¿Con qué frecuencia accede a internet?", porque las demás preguntas exponen directamente esta frecuencia.

En cuanto a policías profesionales, el 47,37 % de ellos cada día usa dispositivos tecnológicos, mientras que los estudiantes en esa misma frecuencia alcanzan el 54,70 %. Lo anterior coincide con el aumento del uso de estas tecnologías según lo mencionado en acápites anteriores. Por otro lado, se encuentra que tanto policías como estudiantes usan estas tecnologías en mayor grado para comunicarse por medio de redes sociales tales como *Facebook*, *Instagram*, *Twitter* y *WhatsApp*. Paralelamente, causa curiosidad que, para la pregunta sobre la frecuencia de compras en línea, para el caso de profesionales, el 42,11 % de ellos indiquen que cada día realiza ese tipo de transacciones; quizá para esta subvariable se debió utilizar otro tipo de escala de valoración, ya que una persona natural a menos que tenga una actividad económica especial, no realiza tal número de transacciones. De hecho, en *Portafolio* (2019) se menciona "que solo el 39 % de las transacciones se realizaron a través de dispositivos móviles el año pasado". Además, Deloitte (2017) señala que el 62 % de los usuarios con dispositivo móviles no lo usan para comprar en línea, lo cual coincide con el 63,46 % de estudiantes del programa técnico que eventualmente compran por dispositivos tecnológicos. La tabla 3 expone los resultados tanto para policías profesionales (P) como estudiantes (E).

Conocimientos sobre seguridad

La tabla 4 evidencia cómo tanto para profesionales como para estudiantes el promedio general sobre conocimientos

Tabla 3. Resultado variable Familiaridad computadoras o dispositivos en porcentajes por profesionales (P) y estudiantes (E)

Pregunta	Cada día		Cada 3 h		Cada hora		Cada 30 min		Cada 15 min		Cada 5 min		Eventual-mente	
	P	E	P	E	P	E	P	E	P	E	P	E	P	E
¿Con qué frecuencia usa una computadora o dispositivos tecnológicos en las siguientes ubicaciones? (hogar, trabajo, universidad)	47,37	54,70	7,79	10,90	18,42	8,55	5,26	3,21	5,26	1,71	7,89	0,43	7,89	20,51
¿Con qué frecuencia accede a su correo electrónico desde las siguientes ubicaciones? (hogar, trabajo, universidad, otras computadoras públicas o privadas)	57,89	58,76	18,4	7,69	10,5	3,85	5,26	1,50	2,63	1,50	0	0,21	5,26	26,50
¿Con qué frecuencia se involucra en las siguientes actividades informáticas? (procesamiento de textos, uso de hojas de cálculo, diseño de presentaciones, edición multimedia y juegos)	50,00	37,18	10,53	7,05	10,53	4,27	2,63	2,15	0	1,50	5,26	1,07	21,05	46,79
¿Con qué frecuencia utiliza las siguientes aplicaciones? (Facebook, Instagram, Twitter y WhatsApp)	55,26	40,38	15,79	7,48	10,53	5,56	5,26	2,56	0	0,64	2,63	0,43	10,53	42,95
¿Con qué frecuencia utiliza las siguientes aplicaciones? (PayPal, eBay, Amazon, Mercado Libre, Linio y en general compras en línea)	42,11	29,49	10,53	2,14	2,63	2,35	2,63	0,64	0	1,28	0	0,64	42,11	63,46
Promedio variable	49,11	45,30	12,70	6,13	12,72	5,52	3,95	2,25	1,75	1,36	4,39	0,61	15,35	37,50

en seguridad es medio. Por otra parte, hay una coincidencia desde el punto de vista del desconocimiento de fraude en la modalidad de *phishing*, con una representación de profesionales del 36,84 % y de estudiantes del 32,91 %. Lo anterior permite señalar cómo desde el programa técnico de formación hay oportunidades de mejora respecto de la capacitación específica para prevenir estafas de esta naturaleza a su personal adjunto y, por supuesto, a los estudiantes. De igual modo, el hecho de tener en promedio un conocimiento medio sobre seguridad y a la vez estar expuesto a diversas tecnologías, como bien se señaló en la revisión de la variable *Familiaridad computadoras o dispositivos*, deja entrever la imperativa necesidad de fortalecer las habilidades de prevención en los diferentes actores de la comunidad académica de la ESBOL.

Prácticas de seguridad: aspectos tecnológicos

En la tabla 5, se puede apreciar que un 49,13 % y un 50,36 % de profesionales (P) y estudiantes (E), respectivamente, presentan buenas prácticas en cuanto a la conciencia

Tabla 4. Resultado variable Conocimientos sobre seguridad en porcentajes por profesionales (P) y estudiantes (E)

Pregunta	Deficiente		Medio		Satisfactorio		Muy Bueno		Excelente	
	P	E	P	E	P	E	P	E	P	E
¿Qué nivel de seguridad aplica en sus actividades de cómputo diarias?	5,26	1,92	31,58	22,01	31,58	28,42	13,16	32,91	18,42	14,74
¿Qué nivel de conocimientos tiene sobre seguridad?	5,26	1,71	42,11	26,28	26,32	29,06	18,42	32,05	7,89	10,90
¿Qué tan claras tiene las diferencias entre *hacker* y *cracker*?	26,32	9,40	34,21	32,92	18,42	23,92	10,53	22,44	10,53	11,32
¿Qué tan claras tiene las diferencias entre gusano, troyano y *spyware*?	26,32	16,24	31,58	32,05	26,32	20,73	7,89	20,51	7,89	10,47
¿Qué tanto sabe de *phishing*?	36,84	32,91	28,95	31,41	15,79	17,09	13,16	12,18	5,26	6,41
Promedio variable	20,00	12,44	33,69	28,93	23,69	23,84	12,63	24,02	10,00	10,77

Tabla 5. Resultado variable Aspectos tecnológicos en porcentajes por profesionales (P) y estudiantes (E)

Pregunta	Sí		No		No sé si lo utilizo		No sé a qué se refiere	
	P	E	P	E	P	E	P	E
¿Utiliza actualmente antivirus en su computadora?	78,95	84,83	10,53	11,54	10,53	3,42	0	0,21
¿Utiliza actualmente *software antispyware* en su computadora?	47,37	53,42	28,95	32,48	21,05	12,18	2,63	1,92
¿Utiliza actualmente una función de filtrado de *spam* en el correo electrónico?	47,37	50,64	31,58	35,90	18,42	11,54	2,63	1,92
¿Utiliza una herramienta o función de bloqueo de ventanas emergentes en su computadora?	52,63	53,63	34,21	39,74	10,53	5,98	2,63	0,64
¿Utiliza alguna forma de función de cifrado inalámbrico en su conexión inalámbrica?	36,84	33,55	39,74	55,77	18,42	7,05	5,26	3,63
¿Utiliza un *fire wall* en sus dispositivos o en su red interna?	31,58	26,07	44,74	54,49	23,68	12,18	0	7,26
Promedio variable	49,13	50,36	31,63	38,32	17,11	8,73	2,19	2,60

del manejo de la seguridad. Sin embargo, al confrontar estos datos versus el *pensum* académico de la ESBOL donde se ve un módulo de seguridad de la información, se observa que solo la mitad de los estudiantes tienen conciencia sobre la seguridad informática, lo cual invita a realizar un análisis sobre qué sucede con la otra mitad del estudiantado y, por supuesto, con el personal profesional adjunto al centro de formación. Lo anterior para dotar de herramientas a todo el personal en la medida en que el 47,83 % de todos los individuos que participaron de esta investigación manifestaron que los datos que almacenan en sus dispositivos tienen una sensibilidad alta o muy alta, y el 30,63 % utiliza conexiones directas tipo *peer-to-peer* para intercambiar archivos tales como películas y juegos.

Prácticas de seguridad: comportamiento de cuidado consciente de seguridad

En la tabla 6, se encuentra un porcentaje aceptable del 39,5 % para profesionales (P) y del 38,7 % para estudiantes (E) sobre el comportamiento consciente de la seguridad informática; sin embargo, en la misma tabla, se pueden ver resultados que pueden considerarse como preocupantes, debido a que el 4,11 % de los profesionales y el 30,13 % de los estudiantes nunca revisan si un sitio cifra los datos que son transferidos a través de él. Situación que, al igual que en la tabla anterior, merece ser analizada usando como referencia el módulo de seguridad de la información que se imparte en la ESBOL.

Discusión

Como bien se señaló los resultados, actualmente en la ESBOL el 91 % de los individuos llevan cuatro años o menos en ella, es decir, que se formaron bajo un *pensum* que incluye la asignatura Tecnologías Aplicadas al Servicio de Policía. Por lo anterior, las discusiones respecto de los resultados claramente pueden comparar a estudiantes y a policías profesionales egresados relativamente hace poco tiempo, en la medida en que este *pensum* está vigente desde 2015 y que esta asignatura incluye algunas unidades referentes a la seguridad de la información.

Paralelamente, poder cursar estas unidades debería brindar una buena conciencia sobre la seguridad de la información personal, sin embargo, los resultados de las tablas 4 y 5 llaman la atención, puesto que para los estudiantes estos resultados en promedio no son buenos, lo cual podría generar una evaluación en la forma como se aborda este curso y cómo los estudiantes están aprendiendo las técnicas enseñadas. De igual modo, para los profesionales, los promedios, desde el punto de vista de conocimientos de seguridad y seguridad aplicada tampoco son los mejores, lo cual implica que también se deberían promover programas de fortalecimiento o recapacitación en seguridad de la información para este personal.

Por otra parte, se puede deducir que tanto los computadores o en general cualquier dispositivo es usado indistintamente por estudiantes o policías profesionales, lo cual deja claro que cualquiera de ellos está expuesto a los riesgos que supone el uso de este tipo de tecnologías y, por tanto, es menester de la ESBOL como centro de formación continuar incluyendo en su currículo asignaturas relacionadas con la seguridad de la información.

En cuanto a capacitaciones al personal profesional en asuntos referentes a la seguridad de la información,

Tabla 6. Resultado variable Comportamiento de cuidado consciente de seguridad en porcentajes por profesionales (P) y estudiantes (E)

Pregunta	Nunca		Casi nunca		Algunas veces		Casi siempre		Siempre	
	P	E	P	E	P	E	P	E	P	E
¿Almacena información confidencial como datos financieros y registros médicos en su computadora?	34,21	40,81	34,21	20,30	21,05	24,15	2,63	8,33	7,89	6,41
¿Envía información confidencial como números de cuenta, contraseñas y número de seguro social por correo electrónico?	65,79	61,11	23,68	20,51	10,53	13,46	0	2,99	0	1,92
¿Utiliza las mismas contraseñas para diferentes cuentas en línea?	34,21	44,44	28,95	18,80	28,95	22,01	0	10,68	7,89	4,06
Al enviar su información personal en internet, ¿comprueba si el sitio cifra los datos transferidos?	42,11	30,13	31,58	22,86	13,16	20,30	5,26	11,32	7,89	15,38
¿Comparte su computadora con otras personas?	42,11	38,46	31,58	25,21	23,68	25,85	0	8,33	2,63	2,14
¿Utiliza una contraseña que es difícil de adivinar, como una combinación de mayúsculas y minúsculas, símbolos y números?	18,42	17,31	15,79	11,54	26,32	13,89	15,79	19,23	23,68	38,03
Promedio variable	39,5	38,7	27,6	19,8	20,62	19,94	4,21	10,15	8,3	11,32

podría considerarse que estas capacitaciones deben considerar el origen de los participantes, en la medida en que, como bien lo señala la figura 3, las habilidades o los conocimientos en esta materia parecen estar determinados por la región de procedencia de las personas.

En relación con los docentes a cargo del curso, aunque son efectivos en la capacitación de tecnologías y plataformas tecnologías que posee la Policía Nacional para soportar el servicio de seguridad a la ciudadanía, podría considerarse también programas de actualización constante en temáticas como la norma ISO 27001 y cursos de *hacking* ético, para soportar específicamente las sesiones referentes a la seguridad de la información. En otro caso, los requisitos en cuanto a estos perfeccionamientos no deberían ser opcionales en el perfil docente sino clasificatorios. Con eso podrían mejorarse los indicadores para futuras cohortes en la ESBOL.

Finalmente, solo considerar personal profesional del nivel ejecutivo y a estudiantes aspirantes a rangos de este nivel podría ser una oportunidad para replicar este estudio no solo en individuos con estas características. Por el contrario, podría considerarse personal del rango de oficiales o suboficiales, y de este modo mapear por completo las debilidades y fortalezas en materia de seguridad de la información de toda la Policía Nacional de Colombia.

Conclusiones

Se puede evidenciar cómo, a pesar de que en el programa Técnico Profesional en Servicios de Policía se abordan asuntos relacionados con la seguridad de la información, los promedios en cuestiones referentes a la conciencia de la seguridad informática no son buenos ni para estudiantes ni para profesionales; dado lo anterior, estos resultados son preocupantes, ya que, como se puede evidenciar en la tabla 3, la familiaridad y el uso de computadores o dispositivos electrónicos es permanente en estudiantes y profesionales. Además, contrastando esta información a la luz de los datos suministrados al inicio de este artículo, en el que se hace evidente el incremento en las diferentes modalidades de incidentes de seguridad informática, es bastante probable que profesionales de policía o estudiantes adscritos a la ESBOL puedan estar involucrados en algún incidente de esta naturaleza.

Por otro lado, gracias al enfoque metodológico usado en esta investigación, es totalmente viable poder, en primera instancia, desde la inferencia estadística, deducir las fortalezas y debilidades en el ámbito de la seguridad de la información de los policías profesionales adjuntos a los diferentes centros de formación y, por supuesto, de los estudiantes de estos centros. Sin embargo, en atención a que en los 14 centros de formación (excepto de la ESBOL) pertenecientes a la Dirección Nacional de Escuelas (DINAE) se forma a jóvenes de diferentes departamentos del país y, por tanto, con diferentes costumbres y culturas dominantes, sería necesario replicar este estudio para mapear por completo las prácticas desde el punto de vista de seguridad de la información de la base de la Policía Nacional de Colombia, es decir, de su nivel ejecutivo en todos sus rangos. Lo anterior se justifica en la medida en que, para el caso de la ESBOL, que tiene como cobertura gran

parte del suroccidente del país (Valle, Cauca y Nariño), la variable sobre alfabetización informática obtuvo valores dispersos en sus diferentes categorías, según la figura 3.

En cuanto a la información existente sobre la actualidad tecnológica, por ejemplo, la encontrada en Deloitte (2017), es necesario recomendar que no basta con mapear las tendencias desde el punto de vista de consumo de diferentes tecnologías, sino que son necesarias iniciativas como las de Deloitte de incluir en sus informes aspectos sobre prácticas de seguridad aplicadas por los consumidores de estas tecnologías.

Finalmente, aunque en la sección de discusión se planteó un trabajo futuro desde el punto de vista de replicar el estudio a todas las escuelas de policía del país, podría resultar interesante realizar este ejercicios en instituciones de educación superior (IES) por fuera del régimen policial, siempre y cuando se considere, en primera instancia, la necesidad de mapear en la futura población objeto de estudio información sobre alfabetización informática, cultura digital y, en general, elementos que determinan las buenas o malas prácticas en el ámbito de la seguridad de la información.

Agradecimientos

Agradecemos el apoyo de todo el personal de la Escuela de Policía Simón Bolívar por su diligencia a la hora de responder el cuestionario enviado por medio digital. De igual modo, al Programa Interinstitucional para el Fortalecimiento de la Investigación y el Posgrado del Pacífico por facilitar la movilidad internacional de la estudiante Mariela Medina Morales, quien contribuyó con el trabajo de campo necesario para este trabajo. Finalmente, a la estudiante Laura Romero del programa de Ingeniería de Sistemas de la Universidad del Valle, sede Tuluá, por su ayuda como monitora de la investigación.

Conflictos de interés

Todos los autores de este artículo manifestamos que no existe ningún conflicto de interés ni conflictos éticos.

Referencias

Adams, A., Sasse, M. A. & Lunt, P. (1997). Making passwords secure and usable. En H. Thimbleby, B. O'Conaill y P. J. Thomas (Eds.), *People and computers XII* (pp. 1-19). Londres, RU: Springer. http://dx.doi.org/10.1007/978-1-4471-3601-9_1

Castillejos López, B., Torres Gastelú, C. A. y Lagunes Domínguez, A. (2016). La seguridad en las competencias digitales de los millennials. *Apertura*, *8*(2), 54-69.

Deloitte. (2017). Consumo móvil en Colombia: los móviles prueban ser indispensables en un mundo "siempre" conectado. Recuperado de https://www2.deloitte.com/content/dam/Deloitte/co/Documents/technology-media-telecommunications/Consumo %20movil(VF1).pdf

Durán Santos, A. U. (2019). *Contexto del ciber crimen en Colombia*. Centro Cibernético Policial. Recuperado de https://docplayer.es/125813772-Centro-cibernetico-policial.html

El Tiempo. (2017, septiembre 27). *A diario se registran 542.465 ataques informáticos en Colombia*. Recuperado de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370

Furnell, S. & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983-988. http://dx.doi.org/10.1016/j.cose.2012.08.004

Hernández, R., Ventura, R. y Juárez Ibarra, C. M. (2018). Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios. *PAAKAT: Revista de Tecnología y Sociedad*, *8*(14). http://dx.doi.org/10.18381/pk.a8n14.318

Mieres, J. (2009). *Buenas prácticas en seguridad informática*. ESET Latinoamérica. Recuperado de https://www.welivesecurity.com/wp-content/uploads/2014/01/buenas_practicas_seguridad_informatica.pdf

Muzammal, S. M., Shah, M. A., Zhang, S. J. & Yang, H. J. (2016). Conceivable security risks and authentication techniques for smart devices: A comparative evaluation of security practices. *International Journal of Automation and Computing*, *13*(4), 350-363. http://dx.doi.org/10.1007/s11633-016-1011-5

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*, *20*(1), 18-28. http://dx.doi.org/10.1108/09685221211219173

Porras Niño, F. H. (2018). *Sistemas de gestión de la seguridad de la información* (Universitat Oberta de Catalunya, Cataluña, España). Recuperado de http://openaccess.uoc.edu/webapps/o2/handle/10609/81125

Portafolio. (2019, marzo 26). Colombianos hacen sus compras en internet desde el computador. Recuperado de https://

www.portafolio.co/negocios/colombianos-prefieren-el-computador-para-hacer-compras-*on line*-527870

Rhee, H. S., Kim, C. & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816-826. http://dx.doi.org/10.1016/j.cose.2009.05.008

Symantec. (2019). *Informe sobre las amenazas para la seguridad en internet 2019*. Recuperado de https://www.symantec.com/es/es/security-center/threat-report

Unisys. (2019). *Índice de Seguridad de Unisys™ en Colombia*. Recuperado de https://www.unisys.com/unisys-security-index/colombia