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

Estudio de caso

Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá

Information Security Practices in Times of Pandemic. Case Universidad del Valle, Tuluá campus

Práticas de segurança da informação em tempos de pandemia. Caso Universidade del Valle, campus Tuluá

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

[a]https://orcid.org/0000-0002-6849-1278 Profesor asociado e investigador, Universidad del Valle, Tuluá, Colombia
[b]https://orcid.org/0000-0001-6359-3104 Profesor auxiliar e investigador, Universidad del Valle, Tuluá, Colombia
[c]https://orcid.org/0000-0002-4056-6565 Policía Nacional de Colombia, Bogotá D. C. Colombia

- Fecha de recepción: 2021-04-27
- Fecha concepto de evaluación: 2021-06-04
- Fecha de aprobación: 2021-07-08
https://doi.org/10.22335/rlct.v13i3.1446

Para citar este artículo/To reference this article/Para citar este artigo: Estrada-Esponda, R. D., Unás-Gómez, J. L., & Flórez-Rincón, O. E. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. Revista Logos Ciencia & Tecnología, 13(3), 98-110. https://doi.org/10.22335/rlct.v13i3.1446

RESUMEN

La pandemia generada por el COVID-19 implicó estrategias de confinamiento masivo como respuesta pública de emergencia en el marco de derecho de policía para combatir el nivel de contagios. Adicionalmente, dicha situación coyuntural implicó cambiar las distintas formas de interacción social (virtual) en torno a temas como la educación, la atención en salud y el empleo. De manera directamente proporcional, la delincuencia aprovechó la situación virtual para intensificar delitos electrónicos como el phishing, las fake news y en general actividades como inyección de malware. El propósito de la investigación fue identificar las prácticas de seguridad de la información en una comunidad universitaria por medio de una encuesta, bajo un enfoque de investigación mixto que consideró entre otras variables la pandemia como precursora de nuevos hábitos de higiene digital. Entre los resultados más representativos se destaca que tanto los profesores como estudiantes tienen un aceptable conocimiento sobre seguridad de la información, pese a no recibir capacitación significativa por entidades gubernamentales. Finalmente, se concluye que los esfuerzos institucionales para combatir ese tipo de delitos no han sido suficientes y por tanto se está en mora de generar estrategias de sensibilización para promover una mejor higiene digital.

Palabras claves: Ingeniería social**,** seguridad de datos, seguridad en internet, seguridad, phishing.

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

ABSTRACT

The pandemic generated by COVID-19 implied massive confinement strategies as an emergency public response within the framework of the police law to combat the level of contagion. Additionally, this situation implied changing the different forms of social interaction such as education, health care and employment. In a directly proportional way, crime took advantage of the situation to intensify electronic crimes such as phishing, fake news and, in general, activities such as malware injection. The purpose of the research was to identify information security practices in a university community by means of a survey, under a mixed research approach that considered, among other variables, the pandemic as a precursor of new digital hygiene habits. Among the most representative results, it is highlighted that both professors and students have an acceptable knowledge of information security, despite not receiving significant training by governmental entities such as the National Police. Finally, it is concluded that institutional efforts to combat this type of crime have not been sufficient and therefore there is a lack of awareness strategies to promote better digital hygiene.

Keywords: Data privacy, security, internet security, phishing, social engineering.

RESUMO

A pandemia gerada pelo COVID-19 envolveu estratégias de confinamento em massa como uma resposta de emergência pública dentro da estrutura da lei policial para combater o nível de contágio. Além disso, essa situação conjuntural implicou uma mudança nas diferentes formas de interação social (virtual) em torno de questões como educação, saúde e emprego. De forma diretamente proporcional, a delinquência aproveitou a situação virtual para intensificar os crimes eletrônicos como phishing, fake news e atividades gerais como injeção de malware. O objetivo da pesquisa foi identificar as práticas de segurança da informação em uma comunidade universitária por meio de uma enquete, sob uma abordagem de pesquisa mista que considerou, entre outras variáveis, a pandemia como precursora de novos hábitos de higiene digital. Dentre os resultados mais representativos, destaca-se que tanto professores quanto alunos possuem conhecimentos aceitáveis sobre segurança da informação, apesar de não receberem treinamento significativo de órgãos governamentais. Finalmente, conclui-se que os esforços institucionais para combater este tipo de crime não têm sido suficientes e, portanto, está em atraso gerar estratégias de conscientização para promover uma melhor higiene digital.

Palavras-chaves: Engenharia social, segurança de dados, segurança na internet, segurança, phishing.

Los ciberataques y en general las vulnerabilidades relacionadas con la seguridad de la información se han hecho cada vez más comunes, en la medida que la informatización de la sociedad se consolida en los diferentes territorios mundiales. A mayor nivel de exposición en entornos digitales también es mayor el nivel de riesgo al que se exponen los diferentes usuarios de aplicaciones y sistemas empresariales. Ahora, en tiempos de la pandemia generada por el COVID-19 el uso de las tecnologías de la información y la comunicación ha aumentado de forma significativa, y de hecho en PwC (2020) se menciona que por dicha pandemia han aumentado las probabilidades de ser víctimas de diversos tipos de ciberataques. Incluso, para el caso específico de Bogotá se evidenció que durante la pandemia las actividades delictivas relacionadas con seguridad informática pasaron de 33 a 41 modalidades de ciberataques (Castellanos Vega, 2019). Sin embargo, precisamente el estado de emergencia generado por la pandemia también ha motivado el desarrollo de estrategias para proteger a los usuarios de las diferentes redes, sean personales o corporativas. En relación a ello, Deloitte (2020) reseña cómo las organizaciones y los gobiernos se han enfocado en proteger la seguridad de los ciudadanos, colaboradores y clientes en tiempos de pandemia. También es necesario señalar que dichos ataques o vulnerabilidades no son coyunturales; según UNISYS (2019), para el año 2019 Colombia ocupó el segundo puesto, déspues de Filipinas, en el nivel de preocupación experimentado por sus ciudadanos en temas referentes a la seguridad digital. Para el año 2020 la misma corporación señala, aunque de manera general, que el 41 % de los encuestados manifiesta inquietudes por la seguridad

de los datos mientras trabajan remotamente y el 43 % se preocupa por la educación de sus hijos en tiempos de pandemia (UNISYS, 2020).

Precisamente, ese nivel de preocupación derivado de fenómenos reales de inseguridad ciudadana en las redes ha motivado estudios sobre el nivel de preparación de las personas en aspectos relacionados con la seguridad de la información y la seguridad informática, siendo un ejemplo de ello el trabajo presentado por Estrada-Esponda et al. (2019), en el cual se estudiaron 19 variables en un establecimiento de formación policial, hallándose como principal resultado que a pesar de que en dicho establecimiento se incluyen temáticas a nivel de currículo asociadas con la seguridad de la información, los resultados en la medición de los niveles de seguridad informática no son adecuados ni para los estudiantes ni para los profesionales que allí laboran.

Si bien es cierto que estudios como el reseñado anteriormente constituyen un precedente para motivar su replicación en contextos organizacionales, académicos y gubernamentales, entre otros, es igualmente cierto que por la actual pandemia de COVID-19 dichos estudios deben ser priorizados, para poder establecer de manera concreta el estado actual de la seguridad de la información y las posibles estrategias para poder contrarrestar los efectos de los ataques. En ese sentido, Interpol (2020) señala que "entre enero y el 24 de abril de 2020 se detectaron 907.000 correos basura, 737 incidentes de tipo malware, y 48.000 URL maliciosas, todos ellos relacionados con la COVID-19" (p.4).

Algunos ejemplos de dichos ataques o vulnerabilidades durante la emergencia resaltan cómo los ambientes e-learning, donde se maneja información reservada o confidencial, están expuestos a troyanos, spyware, acceso no autorizado o a la alteración parcial o total de la información que se almacena estos sistemas. Sin embargo, la implementación de buenas prácticas de seguridad de la información aplicada por instituciones que regularmente soportan e-learning ha significado un éxito para la gestión académica de forma remota (Monges Olmedo & Jiménez Chaves, 2020).

En términos de percepción también resulta interesante poder evaluar cómo ha sido la afectación de la emergencia sanitaria generada por la pandemia en el ámbito académico; en este contexto específico, Machuca-Rubio y Cabrera-Duffaut (2020) indagan sobre la percepción de los padres de familia de los estudiantes de una institución educativa de Ecuador, por medio de un instrumento de recolección de información en línea que permitió identificar que la mayoría de padres de familia no aplica controles de seguridad de información o de seguridad informática, y además no perciben que la misma institución proponga espacios para tratar temas de protección frente a los peligros a los que los estudiantes están expuestos en internet.

Por otro lado, pese a los procesos de vacunación masiva que se realizan a nivel mundial, el COVID-19 sigue siendo una problemática global que abona el terreno para que los ciberdelincuentes aumenten su presencia, aprovechando las vulnerabilidades relacionadas con el teletrabajo, así como también de los procesos de enseñanza mediados por la tecnología, al punto que dichos delincuentes consolidan sus actividades delictivas y generan modus operandi mucho más complejos y sofisticados que atentan contra la seguridad de la información y la seguridad informática (Interpol, 2020).

En ese sentido, replicar estudios como los realizados por Estrada-Esponda et al. (2019) permite fomentar estrategias institucionales para contrarrestar en algún grado esas nuevas amenazas que ponen en riesgo la seguridad ciudadana en términos digitales. Así pues, la pregunta que deriva de la anterior exposición está en función de determinar: ¿Cuál es el nivel de preparación de los miembros de una comunidad académica en relación con la seguridad de la información en tiempos de pandemia?

El artículo continúa con la reseña de estudios que sirvieron para favorecer el trabajo de campo realizado, y luego se procede con el análisis de las variables de investigación, así como con su discusión. Por último, se presentan las conclusiones y posibles proyecciones sobre trabajos futuros.

Metodología

Con base en la problemática expuesta y la revisión de la literatura que se realizó, se planteó una investigación aplicada con enfoques cuantitativos y cualitativos, primero con la finalidad de facilitar la generalización de resultados a toda la comunidad académica de la Universidad del Valle, sede Tuluá, y segundo con el propósito de poder responder a problemáticas que bien pueden ser estructurales o coyunturales, con base en la nuevas dinámicas de enseñanza y aprendizaje motivadas por la pandemia del COVID-19.

El tamaño de la muestra fue calculado a partir de un muestreo aleatorio simple con un método estratificado, con un nivel de confianza definido del 95 % y un error del 5 %. De este modo, con base en una población total de 1847 individuos la muestra representativa se determinó en 319 personas. La investigación tuvo las siguientes fases:

- **Fase de diseño**: Se construyó el instrumento de recolección de información, compuesto por 5 variables y 32 subvariables, además de que se incluyeron preguntas misceláneas para fortalecer el análisis de los resultados. No fue necesario solicitar un consentimiento informado, ya que el instrumento se respondió de manera anónima. Sin embargo, se añadió una política de tratamiento de datos conforme a la Ley 1581 de 2012, como parte del instrumento.

Para esta elaboración fue necesario revisar instrumentos de investigaciones similares y realizar un proceso de consolidación, teniendo como variable dependiente la seguridad informática aplicada por estudiantes y profesores vinculados a la Universidad de Valle, sede Tuluá. De igual modo, se procedió a realizar la validación de dicho instrumento por medio de la realización de una prueba piloto con 43 estudiantes de los programas académicos de Ingeniería de Sistemas y Tecnología en Sistemas de Información. Durante este ejercicio de pilotaje se comentaron con mayor nivel de ocurrencia las escalas de valoración de un par de preguntas, las cuales fueron ajustadas para el cuestionario definitivo, que incluyó a 338 individuos adicionales, para obtener un total de 381 respuestas. Finalmente, durante el análisis de los resultados en esta fase fue posible calcular un alfa de Cronbach de 75 %, 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 durante el periodo 02/02/2021-01/03/2021; vale la pena aclarar que, conforme al diseño estadístico, el propósito era aplicar el instrumento inicialmente a 287 estudiantes de pregrado, 16 de posgrado y 16 profesores. El instrumento fue difundido vía Google Forms y promocionado por redes sociales y bases de datos de la Universidad del Valle, sede Tuluá.

- **Fase de análisis:** Se procedió a tabular y analizar, con un enfoque univariado, 381 respuestas de estudiantes y profesores de la comunidad académica de la Universidad del Valle, sede Tuluá, proceso durante el cual fue posible generar una discusión relacionada con cada una de las variables objeto de estudio.

Finalmente, la tabla 1 reseña los principales documentos de referencia que sirvieron para la planificación y el desarrollo de la investigación, particularmente desde el componente metodológico, que además fueron consultados en repositorios o bases de datos académicas.

1 https://drive.google.com/drive/folders/1htbc2xvkhho0JI4DoFvCVP7lAW0fu9hR

Tabla 1
Revisión de la literatura: identificación de variables

Trabajo	Referencias	Variable(s)	Preguntas
• Making passwords secure and usable	Adams et al. (1997)	• Seguridad en contraseñas	24, 25, 30
• Buenas prácticas en seguridad informática	Mieres. (2009)	• Seguridad en redes sociales • Seguridad en redes P2P • Seguridad en mensajería instantánea • Seguridad en redes sociales • Protección a correos electrónicos • Seguridad en la navegación • Actualización de sistemas operativos y aplicaciones	13, 21, 3, 6, 7, 11, 24
• La seguridad en las competencias digitales de los *millennials*	Castillejos et al.(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 et al.(2016)	• Protección de datos personales • Protección de datos en dispositivos inteligentes • Seguridad en contraseñas	24, 25, 30, 26 y 29

Trabajo	Referencias	Variable(s)	Preguntas
• Why do some people manage phishing e-mails better than others?	Pattinson et al.(2012)	• Familiaridad con computadoras • Seguridad en correos electrónicos • 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	Roque Hernández y Juárez Ibarra. (2018)	• Conocimientos sobre seguridad	16, 17, 18, 19, 20
• Self-efficacy in information security: Its influence on end users' information security practice behavior	Rhee et al.(2009)	• Alfabetización informática	1, 2, 3, 9, 10, 11, 12, 14, 23, 24, 25, 26, 27
• Ciberdelincuencia: Efectos de la COVID-19 (COVID-19 • Seguridad de la información en tiempos de COVID-19	(Interpol, 2020; PwC, 2020)	• Seguridad de la información en tiempos de pandemia	29, 30, 31, 32, 33, 34, 35

Nota: Elaborado a partir de Estrada-Esponda et al. (2019)

Resultados y discusión

Con base en el trabajo de campo realizado se logró encuestar a 381 personas (37 % de sexo femenino y 63 % de sexo masculino), realizando diversas caracterizaciones de la población objeto de estudio. De los encuestados, 335 son estudiantes de pregrado, 37 pertenecen al estamento docente y 9 adelantan estudios de posgrado, lo cual evidencia que se realizaron las encuestas previstas según el diseño estadístico. Los encuestados se dividen en 4 áreas del conocimiento, así: 25.7 % corresponden a la Facultad de Ciencias de la Administración, 4.2 % a Humanidades, 60.4 % pertenecen al área de Ingeniería y el 9.7 % son docentes. En cuanto a la distribución de las edades, se encuentra que para los estudiantes el promedio de edad es de 21.5 años y para los docentes es de 43 años; haciendo una diferenciación entre los estudiantes de pregrado y posgrado, los promedios de edad son de 21.1 años para los primeros y 38.1 para los segundos. Las edades de los encuestados se han agrupado de la siguiente manera: grupo 1, de 16 a 26 años; grupo 2, de 27 a 37 años; además de un tercer grupo en el que se encuentran los mayores de 37 años. El porcentaje de distribución por los respectivos grupos etarios es: grupo 1, 84 %; grupo 2, 7.6 %; y grupo 3, 8.4 %.

Respecto a la alfabetización informática, el 90 % (343) de los encuestados manifiesta tener un nivel entre excelente (115) y bueno (228), mientras que el restante 10 % (38 individuos) considera que su alfabetización informática es regular.

En cuanto al tiempo de uso de equipos de cómputo o dispositivos tecnológicos (smartphones, tablets, lectores, etc.), se tiene que el 93.44 % de los encuestados lleva usando este tipo de dispositivos por más de 4 años, mientras que solo un 6.56 % los ha usado entre 2 y 4 años.

En el análisis de la última variable de alfabetización informática, que indaga sobre los años de uso de internet, se pudo evidenciar que el 92.39 % usa este recurso desde hace más de 4 años, seguido de un 6.56 % cuyo tiempo de uso está entre los 2 y 4 años, y por último un 1.05 % que solo lleva usando internet entre 1 y 2 años.

Luego del ejercicio de caracterización se indagó entre los individuos con respecto a cinco grupos de variables, incluyendo un grupo asociado a la pandemia generada por el COVID-19, además de algunas preguntas misceláneas. A continuación, se presentan los respectivos resultados:

Familiaridad con las computadoras

Para el estudio de este aspecto se realizaron 6 preguntas, con una valoración de 1 a 5, encontrándose promedios globales que indican que existe una alta familiaridad con las computadoras por parte de todos los encuestados, con una tendencia mayor en docentes que en estudiantes, en tanto el promedio global obtenido fue de 4.4 para docentes y 4.0 para estudiantes. La tabla 2 también evidencia que el componente de acceso a internet es el que mayor valoración presenta, con un promedio general de 4.77 (4.89 para profesores y 4.65 para estudian-

tes), mientras que el componente de más bajo puntaje en este aspecto es el que hace referencia a las compras por internet, el cual obtuvo un promedio general de 2.78 (3.14 para profesores y 2.42 para estudiantes), lo que evidencia que aún existe temor y recelo para la realización de compras y transacciones financieras utilizando estos medios digitales. La tabla 2 deja ver igualmente que son los estudiantes quienes ligeramente utilizan más las redes sociales (Facebook, Instagram, YouTube, Twitter y WhatsApp) frente a los docentes, obteniendo los primeros una calificación de 4.34 versus 4.16 para los segundos.

Tabla 2
Familiaridad con las computadoras

Pregunta	Profesor	Estudiante
¿Con qué frecuencia usa una computadora o dispositivos tecnológicos en las siguientes ubicaciones: hogar, trabajo, universidad?	4.84	4.60
¿Con qué frecuencia accede a internet?	4.89	4.65
¿Con qué frecuencia accede a su correo electrónico desde las siguientes ubicaciones: hogar, trabajo, universidad, otras computadoras públicas o privadas?	4.76	4.16
¿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?	4.57	3.84
¿Con qué frecuencia utiliza las siguientes aplicaciones: Facebook, Instagram, YouTube, Twitter y Whatsapp?	4.16	4.34
¿Con qué frecuencia utiliza las siguientes aplicaciones: PayPal, eBay, Amazon, Mercado Libre, Linio y en general compras en línea?	3.14	2.42
Promedio general	4.4	4.0

Conocimientos sobre seguridad

En este punto, el instrumento incluyó 7 preguntas, cuyas respuestas eran de carácter cualitativo; sin embargo, para facilitar el análisis de las respuestas, se les dio una valoración cuantitativa en una escala tipo Likert de 1 a 5. El estudio pretendió identificar cuáles eran los conocimientos en materia de seguridad informática que poseían los encuestados, encontrándose en general resultados muy similares, pues el puntaje global para docentes fue de 2.4, mientras los estudiantes se encuentran solo un punto decimal por encima, con 2.5. Estos datos resultan preocupantes, pues tanto en los resultados globales como en los específicos de cada ítem indagado, ninguno de los dos grupos obtuvo una media satisfactoria que superara el valor de 3, encontrándose que la respuesta mejor calificada para ambos grupos fue: ¿Qué nivel de seguridad aplica en sus actividades de computo diarias?, en donde la valoración para ambos grupos fue de 2.9, mientas que las valoraciones más bajas se tuvieron en torno a la pregunta: ¿Qué tanto sabe de ransomware, DDoS, dominios maliciosos, malware de recolección de datos y desinformación o fake news?, y en la calificación de las habilidades y conocimientos para defenderse o contrarrestar los mismos temas, además del phishing o las estafas por internet, con una calificación de 2.1 para cada ítem. La tabla 3 presenta los resultados globales por cada pregunta de este aspecto de conocimientos sobre seguridad.

Tabla 3
Conocimientos sobre seguridad

Pregunta	Profesor	Estudiante
¿Qué nivel de seguridad aplica en sus actividades de computo diarias?	2.9	2.9
¿Qué nivel de conocimientos tiene sobre seguridad?	2.6	2.7
¿Qué tan claras tiene las diferencias entre hacker y cracker?	2.5	2.7
¿Qué tan claras tiene las diferencias entre gusano, troyano y spyware?	2.4	2.5
¿Qué tanto sabe de phishing?	2.3	2.2
¿Qué tanto sabe de ransomware, DDoS, dominios maliciosos, malware de recolección de datos y desinformación o fake news?	2.1	2.4
¿En general qué tan buenos son sus conocimientos para defenderse o contrarrestar los siguientes temas: 1. Phishing y estafas por internet; 2. Ransomware; 3. DDoS; 4. Dominios maliciosos; 5. Malware de recolección de datos; 6. Desinformación o fake news?	2.1	2.3
Promedio general	2.4	2.5

Prácticas de seguridad

Este punto de evaluación se dividió en dos clases, el primero denominado Aspectos tecnológicos, que hace referencia a las posibles herramientas que podría utilizar el encuestado, y el segundo de Comportamiento de cuidado consciente de seguridad, donde se pretende analizar la actuación y el comportamiento del encuestado en su vida digital cotidiana.

Prácticas de seguridad: Aspectos tecnológicos

Aquí se logró evidenciar que tanto profesores como estudiantes utilizan en un alto porcentaje (76.6% en prome-

dio) alguna herramienta de seguridad tipo antivirus. En el mismo ítem, un 14.2 % de ambos grupos reporta que no usa antivirus, mientras que el restante 9.2 % no sabe si lo usa o no está al tanto de qué se le está hablando. Respecto a las herramientas de protección de filtrado de tráfico de red (tipo Firewall), para el equipo personal o red doméstica las cifras muestran poco interés o desconocimiento en este tema, pues solo un 33.6 % lo usa, un 34.4 % no lo usa, y un 32 % no sabe si lo usa o no está al tanto de qué se le está hablando. La tabla 4 refleja los resultados detallados.

Tabla 4
Prácticas de seguridad – Aspectos tecnológicos. Profesores vs. estudiantes

Pregunta		Profesores	Estudiantes
¿Utiliza actualmente antivirus en su computadora?	• No	14.2	14.2
	• No sé a qué se refiere	0.8	0.6
	• No sé si lo utilizo	8.7	8.4
	• Sí	76.4	76.7
¿Utiliza actualmente software anti-spyware en su computadora?	• No	36	36
	• No sé a qué se refiere	3.9	3.5
	• No sé si lo utilizo	33.1	34.9
	• Sí	27	25.6
¿Utiliza actualmente una función de filtrado de spam en el correo electrónico?	• No	25.2	26.2
	• No sé a qué se refiere	1.6	1.2
	• No sé si lo utilizo	16.5	15.7
	• Sí	56.7	57
¿Utiliza una herramienta o función de bloqueo de ventanas emergentes en su computadora?	• No	22.3	23
	• No sé a qué se refiere	1.8	1.5
	• No sé si lo utilizo	9.7	9
	• Sí	66.1	66.6
¿Utiliza alguna forma de función de cifrado inalámbrico en su conexión inalámbrica?	• No	44.6	46.2
	• No sé a qué se refiere	3.7	3.2
	• No sé si lo utilizo	26	25.9
	• Sí	25.7	24.7
¿Utiliza un *Firewall* en sus dispositivos o en su red doméstica?	• No	34.1	34.6
	• No sé a qué se refiere	5	4.9
	• No sé si lo wutilizo	27.3	26.7
	• Sí	33.6	33.7

Posteriormente se analizaron las mismas respuestas, pero dividiendo los grupos entre los que pertenecen a los programas del núcleo básico de Ingeniería de Sistemas, Telemáticas y afines, según la clasificación del SNIES (Ingeniería de Sistemas, Tecnología en Sistemas de Información y Tecnología en Desarrollo de Software), versus los demás programas académicos, encontrándose una variación importante, pues se evidenció en los primeros un mayor conocimiento de los aspectos tecnológicos indagados; es así como las preguntas cuyas respuestas reflejan desconocimiento (No sé a qué se refiere y No sé si lo utilizo) disminuyeron significativamente sus porcentajes, mientras que las respuestas que reflejan seguridad (Sí o No) aumentaron en gran medida sus porcentajes. En la tabla 5 se reseñan estos resultados.

Tabla 5
Prácticas de seguridad – Aspectos tecnológicos - Programas de sistemas vs. otros programas

Pregunta		Otras	Sistemas
¿Utiliza actualmente antivirus en su computadora?	• No	10.5	18.2
	• No sé a qué se refiere	1	0.5
	• No sé si lo utilizo	15.7	1.1
	• Sí	72.8	80.2
¿Utiliza actualmente software anti-spyware en su computadora?	• No	28.3	44.4
	• No sé a qué se refiere	5.2	2.7
	• No sé si lo utilizo	47.6	17.6
	• Sí	18.8	35.3
¿Utiliza actualmente una función de filtrado de spam en el correo electrónico?	• No	20.4	29.9
	• No sé a qué se refiere	2.6	0.5
	• No sé si lo utilizo	27.2	5.9
	• Sí	49.7	63.6
¿Utiliza una herramienta o función de bloqueo de ventanas emergentes en su computadora?	• No	27.7	16.6
	• No sé a qué se refiere	2.1	1.6
	• No sé si lo utilizo	17.3	1.6
	• Sí	52.9	80.2
¿Utiliza alguna forma de función de cifrado inalámbrico en su conexión inalámbrica?	• No	37.7	51.9
	• No sé a qué se refiere	5.8	1.1
	• No sé si lo utilizo	35.6	16
	• Sí	20.9	31
¿Utiliza un Firewall en sus dispositivos o en su red doméstica?	• No	35.6	33.2
	• No sé a qué se refiere	6.8	2.7
	• No sé si lo utilizo	40.8	13.4
	• Sí	16.8	50.8

Prácticas de seguridad: Comportamiento de cuidado consciente de seguridad

La consciencia y la actuación cotidiana de la vida digital de los encuestados se midió con base en 6 preguntas, encontrándose contrastes en las diferentes respuestas, al obtener en algunos buenos promedios en la actuación, mientras que en otras estos promedios bajaron significativamente, de lo cual se concluye que no existe consistencia en el comportamiento consciente de la seguridad digital (tabla 6). Por ejemplo, el 80.5 % de los encuestados nunca o casi nunca comparten números de cuenta, contraseñas y número de seguro social por correo electrónico, lo cual anticipa un buen comportamiento digital; sin embargo, para la pregunta: ¿Utiliza las mismas contraseñas para diferentes cuentas en línea?, se evidencia que el 66.4 % de los encuestados apela a este tipo de práctica, lo cual no es consistente con el buen comportamiento digital que aseguran tener, lo que a su vez implica un problema de desconocimiento, y por tanto una oportunidad para establecer planes de capacitación en prácticas de comportamiento digital.

Tabla 6
Prácticas de seguridad – Comportamiento de cuidado consciente de seguridad

Pregunta	Escala	Total
¿Almacena información confidencial, como datos financieros y registros médicos, en su computadora?	Nunca Casi nunca Algunas veces Casi siempre Siempre	23.4 % 34.9 % 24.7 % 11.8 % 5.2 %
¿Envía información confidencial (como números de cuenta, contraseñas y número de seguro social) por correo electrónico?	Nunca Casi nunca Algunas veces Casi siempre Siempre	57.7 % 22.8 % 12.9 % 5.2 % 1.3 %
¿Utiliza las mismas contraseñas para diferentes cuentas en línea?	Nunca Casi nunca Algunas veces Casi siempre Siempre	17.1 % 16.5 % 37.8 % 20.2 % 8.4 %
Al enviar su información personal en internet, ¿comprueba si el sitio cifra los datos transferidos?	Nunca Casi nunca Algunas veces Casi siempre Siempre	25.5 % 24.4 % 25.2 % 13.4 % 11.5 %
¿Comparte su computadora con otras personas?	Nunca Casi nunca Algunas veces Casi siempre Siempre	39.6 % 30.7 % 17.1 % 8.7 % 3.9 %
¿Utiliza una contraseña que es muy difícil de adivinar, como una combinación de mayúsculas y minúsculas, símbolos y números?	Nunca Casi nunca Algunas veces Casi siempre Siempre	10.2 % 12.1 % 25.5 % 25.2 % 27.0 %

Seguridad informática en tiempos de pandemia

En esta componente solo se encuentra un ítem cuyos extremos de respuestas son bastante similares, y es el referido a si la persona ha recibido recientemente información falsa (fake news) o información conspirativa sobre la pandemia, de modo que el 47.8 % de los encuestados asegura no haber recibido ninguna notica falsa o información conspirativa al respecto, mientras que un 43.3 % sí afirman haber recibido este tipo de información.

Del total de encuestados, un 19.9 % tuvo que realizar tareas o trabajos desde su casa a través de VPN, mientras que un 68.5 % no se vio obligado a desplegar este tipo de infraestructuras o trabajar sobre las mismas, resaltando además que un significativo 11.5 % no responde o no sabe si le tocó trabajar sobre estas tecnologías. También, un 2.4 % fue víctima de robo de información a través de software que aparentaba contener archivos con medidas para prevenir el COVID-19. Un poco más del 90 % manifiesta no haber sido suplantado en plataformas de reuniones sincrónicas como Zoom, Google Meet u otra similar, ni tampoco en las plataformas ofrecidas por su institución educativa. A su vez, el 88 % afirma no haber sido testigo de suplantación o sabotaje en reuniones sincrónicas a través de plataformas tipo Google Meet, Zoom, etc.; sin embargo, un 8.1 % sí fue testigo de este tipo de suplantación o sabotaje en estas reuniones. Por último, una cifra bastante alta, el 81.1 % de la muestra manifestó que no visitó dominios en internet que estuviesen asociados con las palabras coronavirus o COVID-19 que resultaran ser finalmente falsos o que su actividad interna fuera la de realizar actividades malintencionadas. La tabla 7 presenta los resultados detallados.

Tabla 7
Seguridad informática en tiempos de pandemia

Pregunta	Respuesta	Porcentaje
¿Ha recibido recientemente información falsa (*fake news*) o información conspirativa sobre la pandemia?	No No sabe / No responde Sí	47.8 % 8.9 % 43.3 %
¿Fue víctima de robo de información por software maliciosos que parecían o aparentaban ser archivos que contenían medidas para prevenir el COVID-19?	No No sabe / No responde Sí	94.5 % 3.1 % 2.4 %
¿Ha visitado o visitó dominios de internet asociados con la palabra COVID-19 o coronavirus, que resultaron ser falsos y su único propósito tenía que ver con actividades malintencionadas?	No No sabe / No responde Sí	81.1 % 4.7 % 14.2 %

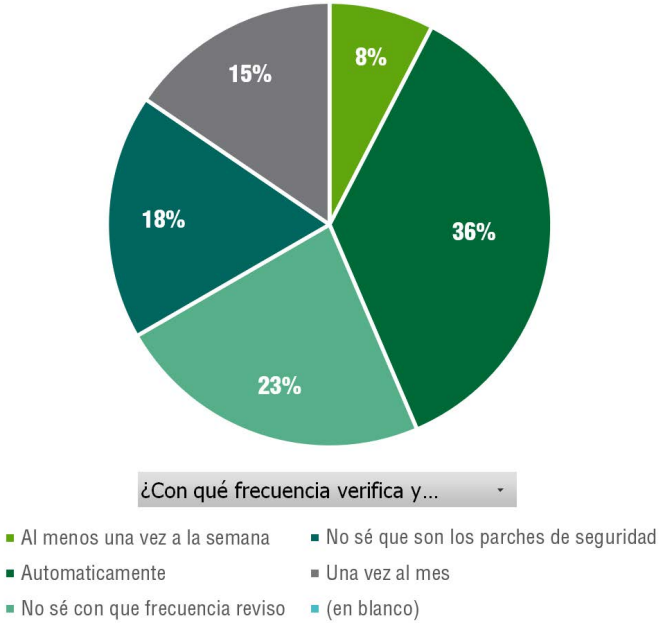
Pregunta	Respuesta	Porcentaje
¿Fue suplantado en plataformas virtuales de conectividad sincrónica, como Zoom, Google Meet u otra?	No No sabe / No responde Sí	92.7 % 3.9 % 3.4 %
¿Fue suplantado en plataformas *e-learning* ofrecidas por su universidad en relación con actividades académicas no sincrónicas?	No No sabe / No responde Sí	94.0 % 4.7 % 1.3 %
¿Fue testigo de ingresos no autorizados a sesiones de trabajo sincrónicas que afectaron el desarrollo de dichas sesiones?	No No sabe / No responde Sí	88.2 % 3.7 % 8.1 %
A raíz de la pandemia del COVID-19, ¿ha tenido que realizar teletrabajo a través de una VPN?	No No sabe / No responde Sí	68.5 % 11.5 % 19.9 %

Aspectos misceláneos

El 77 % de los encuestados manifiesta que el uso que le dan a su correo electrónico institucional es para uso netamente académico, seguido de un 11.8 % que lo usan para actividades académicas, laborales y personales.

En cuanto a los parches de seguridad y/o actualizaciones automáticas, realizando un agrupamiento entre quienes lo hacen de manera automática, semanal o mensual, el 59.1 % lleva a cabo esta tarea, frente a un 23.1 % que no sabe con qué frecuencia se realiza este proceso en sus equipos y un restante 17.8 % que manifiesta no tener conocimiento sobre este aspecto. La figura 1 resume dicha situación.

Figura 1
Aplicación de parches y actualizaciones de seguridad



En lo que refiere al intercambio o descarga de archivos por medio de conexiones peer-to-peer (P2P), el 50.5 % de la muestra manifiesta que no realiza esta actividad, un 25.4 % sí lo hace, mientras que el restante 24.1 % no sabe a qué se refiere esta actividad.

En cuanto al uso de plataformas o aplicaciones para descargar o compartir software, la dependencia que más realiza esta actividad es la Facultad de Ingeniería, con un 20.9 %, en contraste con la Facultad de Humanidades, que con un 0.3 % es el grupo de encuestados que menos la realiza. La tabla 8 presenta los resultados detallados.

Tabla 8
Uso de plataformas o aplicaciones para descargar o compartir software

Facultad	Respuesta	Porcentaje
Administración	No No sé a qué hace referencia ese tipo intercambio de archivos Sí	12.4 % 9.5 % 3.4 %
Humanidades	No No sé a qué hace referencia ese tipo intercambio de archivos Sí	1.6 % 2.4 % 0.3 %
Ingeniería	No No sé a qué hace referencia ese tipo intercambio de archivos Sí	30.4 % 9.3 % 20.9 %
Profesor	No No sé a qué hace referencia ese tipo intercambio de archivos Sí	6.1 % 2.9 % 0.8 %

En cuanto a la importancia y/o sensibilidad de los datos almacenados en los dispositivos (móvil, laptop, etc.) de los individuos encuestados, un 86.7 % de ellos califica dicha sensibilidad como moderada y alta, lo cual contrasta frente a un 13.3 % que considera baja o muy baja la información que almacena en sus dispositivos. La figura 2 presenta dicha situación.

Un aspecto muy importante a la hora de enfrentar fallas, ataques informáticos, catástrofes, entre otras circunstancias, es la realización de copias de seguridad, aspecto en el cual los encuestados se dividen en cuatro grupos, con porcentajes muy similares entre ellos, cuando se les indagó: ¿Cuándo fue la última vez que hizo una copia de seguridad de archivos importantes? La figura 3 refleja dichos grupos.

Figura 2
Valoración de la información almacenada en los dispositivos

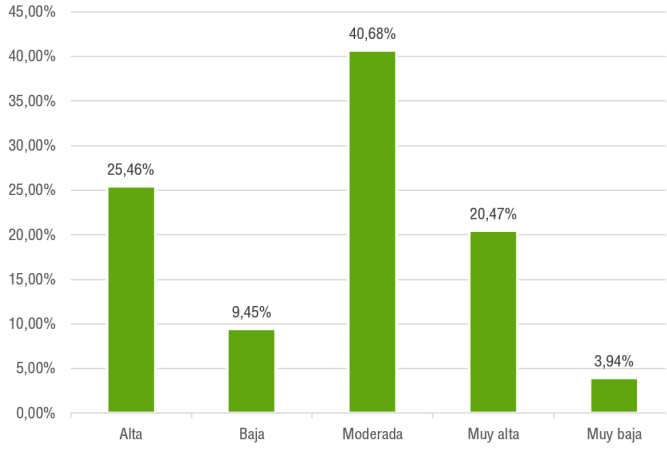
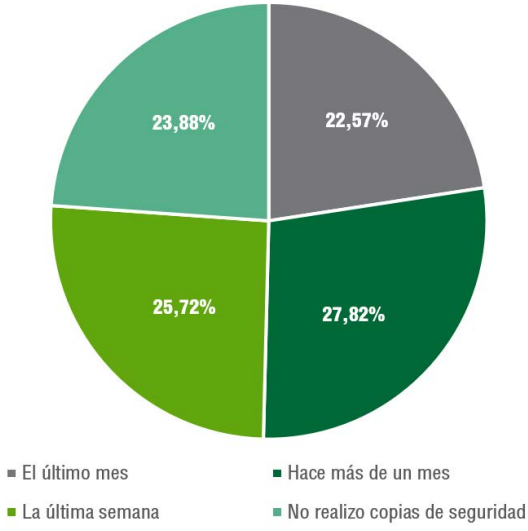


Figura 3
Realización de copias de seguridad



Ante la eventualidad de la pandemia vivida a nivel mundial, el 49.34 % de los encuestados revela que no ha recibido información de prevención contra delitos informáticos por parte de ninguna institución, seguido de un 29.42 % que manifiesta sí haber recibido información de este tipo por parte de una institución académica, y un 6.86 % por parte de la Policía Nacional; el resto reporta porcentajes aún más bajos (tabla 9). Sin embargo, llama la atención que la Policía Nacional, como institución encargada de la seguridad ciudadana, no encabece este tipo de campañas.

En cuanto a la formación y/o higiene digital, un 36.30 % no se entrena o recibe información al respecto, lo cual se traduce en una oportunidad para ejecutar campañas de sensibilización que mejoren la higiene digital de dichos individuos. Por otra parte, el 27.61 % se entrena por medio de instituciones educativas como las universidades, un 27.76 % lo hace de manera autónoma, un 3.70 % lo hace en su lugar de trabajo, y hay dos grupos que lo realizan por medio de compañeros o a manera de hobby. La tabla 10 refleja todas las categorías.

Tabla 9
Información de delitos informáticos

Institución	Porcentaje
De ninguna institución	49.34 %
De una institución académica	29.42 %
De la Policía Nacional	6.86 %
De una entidad financiera	6.19 %
De una empresa de seguridad o de TI	5.97 %
De las Fuerzas Militares	0.88 %
Semilleros de la universidad	0.44 %
Amigos y familiares	0.22 %
Autodidacta	0.22 %
Universidad	0.22 %
Videos de YouTube	0.22 %

Tabla 10
Entrenamiento en seguridad informática

Institución	Porcentaje
No se entrena sobre temas de seguridad	36.30 %
En la universidad	27.61 %
De forma autónoma por interés personal	26.74 %
En un grupo independiente por hobby	4.78 %
En el trabajo	3.70 %
Cursos por el Sena de seguridad web	0.65 %
Compañeros	0.22 %

Un 78 % de los encuestados manifiesta no conocer lo que es un doble factor de autenticación, mientras que solo el 22 % de los mismos sí sabe lo que es este método. Adicionalmente, estos individuos indicaron cuál es la herramienta o método de doble factor de autenticación que utilizan, los cuales se señalan en la tabla 11. Sin embargo, para este 78 % de personas que no conoce métodos de doble autenticación también aplicarían campañas de sensibilización, para evitar el hackeo de cuentas y los delitos que ello implica.

Ante los correos electrónicos sospechosos, un 69.81 % de los encuestados opta por borrarlos, mientras que un 17.63 % utiliza algún tipo de herramienta para validar el

correo o su contenido, un 7.25 % abre dicho correo, un 2.42 % simplemente no los abre y, por último, un 2.90 % actúa de diferentes maneras, como, por ejemplo, marcándolo como spam, o nunca le llegan ese tipo de correos. La tabla 12 presenta los datos detallados.

Tabla 11
Herramientas o métodos de doble autenticación

Método	Porcentaje
SMS	50.60 %
APP móvil	13.25 %
E-mail	12.05 %
Token	8.43 %
Biométrico	7.23 %
Latch	2.41 %
SteamGuard	2.41 %
AMF	1.20 %
Preguntas secretas	1.20 %
Voz	1.20 %

Tabla 12
Actuación frente a correo electrónico sospechoso

Actuación	Porcentaje
Lo borra	69.81 %
Usa alguna herramienta de seguridad para validar el correo o su contenido	17.63 %
Lo abre	7.25 %
No lo abre	2.42 %
Otras actuaciones	2.90 %

Conclusiones

Hay evidencia empírica que demuestra que con la pandemia del COVID-19 los incidentes en términos de la seguridad de la información aumentaron sustancialmente. Sin embargo, para la comunidad académica observada no se puede señalar que dicho incremento sea igual de significativo, en la medida que no se observaron de forma masiva vulneraciones a actividades académicas como reuniones sincrónicas o trabajos asincrónicos, lo cual permite entender que el nivel de preparación de la comunidad académica de la Universidad del Valle, sede Tuluá, en relación con la seguridad de la información en tiempos de pandemia, es bueno, pese a que casi un 37 % de ellos no recibió ningún tipo de formación al respecto. Esto podría estar relacionado con que el incremento se presenta en mayor medida en situaciones transaccionales asociadas con el sector financiero, y de hecho en PwC (2020) se enfatiza precisamente que en el corto plazo se deben resolver los temas financieros en aspectos relativos a la ciberseguridad.

Ahora bien, pese a que las afectaciones en educación no fueron significativas comparadas con situaciones del sector financiero, se observa que sí hubo algunos incidentes, por ejemplo con herramientas de trabajo sincrónico como Zoom, de manera que de forma no autorizada terceros accedían a las reuniones con propósitos de sabotearlas, situación que se reseña incluso en Harán (2020). Sin embargo, para el caso de la Universidad del Valle, sede Tuluá, la plataforma usada para tales reuniones fue mayoritariamente Google Meet, por medio de cuentas institucionales, lo cual hacía más seguras dichas sesiones académicas.

Por otro lado, fue posible identificar que los hábitos de higiene digital son mayores en estudiantes de las áreas TI, y por ello los resultados muestran cómo los estudiantes de la Escuela de Ingeniería de Sistemas y Computación, además de que conceptualmente tienen mayor claridad, en la práctica asumen actividades más responsables frente a las vulnerabilidades de una sociedad digitalizada, comparados por ejemplo con estudiantes de la Facultad de Ciencias de la Administración o de otras facultades.

En cuanto a las campañas o estrategias de sensibilización, se observa que su número no es significativamente importante, y, de hecho, casi el 50 % de los individuos respondieron que no recibieron nunca recomendaciones en relación con la seguridad de la información en tiempos donde perduran las noticias falsas y en general campañas de desinformación o conspiración. Por otro lado, solo un 6.86 % de los individuos respondieron que la Policía Nacional compartió prácticas o estrategias en temas de seguridad de la información, lo cual es relativamente poco, asumiendo la actual situación coyuntural del COVID-19, y lleva a pensar que, en condiciones normales, la difusión de dichas prácticas por parte de la institución policial es mínima.

En la misma dirección, con base en los resultados presentados, podría resultar pertinente que la Policía Nacional, a través de la Dirección de Seguridad Ciudadana, junto con el CSIRT-PONAL, el Centro Cibernético Policial o el Observatorio del Cibercrimen de la Dirección de Investigación Criminal, pudiera intensificar, de forma articulada con las instituciones educativas y entidades privadas en

general, campañas de prevención de delitos informáticos para sensibilizar a los usuarios, no solo en tiempos de pandemia, sino de forma más continua y estructurada.

Como una limitante, se reseña que el método de muestro fue por conveniencia y en ese sentido, replicar este estudio bajo un enfoque probabilístico con enfoques bivariados se traduce en un trabajo futuro.

Finalmente, se observan oportunidades de trabajo futuro sobre la medición real y quizás más objetiva respecto al nivel de preparación de los ciudadanos en términos de seguridad de la información, en la medida en que se encontraron algunas respuestas no consistentes que llamaron la atención, y que de paso invitan, por ejemplo, a no solo preguntar, sino también validar por medio de escenarios controlados de ataque cibernético, para evaluar el comportamiento de dichos ciudadanos y contrastarlo con sus respectivas respuestas.

Referencias

Adams, A., Sasse, M., & Lunt, P. (1997). Making Passwords Secure and Usable. En H. Thimbleby, B. O'Conaill & P. J. Thomas (eds.), *People and Computers XII* pp. 1-19. https://doi.org/10.1007/978-1-4471-3601-9_1

Castellanos Vega, C. J. (2019). Modalidades de cibercrimen en tiempos de pandemia Covid-19 en Bogotá (Colombia). http://hdl.handle.net/10654/37304

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

Deloitte. (2020). *Consideraciones de ciberseguridad en medio de una pandemia global*. https://www2.deloitte.com/co/es/pages/risk/articles/consideraciones-de-ciberseguridad-en-una-pandemia-global.html

Estrada-Esponda, R. D., Unás-Gómez, J. L., & 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. https://doi.org/10.22335/rlct.v12i1.1050

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

Harán, J. M. (2020). Zoom: problemas de seguridad y privacidad en la popular herramienta para videoconferencias. *welivesecurity by ESET*. https://www.welivesecurity.com/la-es/2020/03/30/zoom-problemas-seguridad-privacidad-popular-herramienta-videoconferencias/

Interpol. (2020). *Ciberdelincuencia: Efectos de la COVID-19*. Secretaría General de la Interpol. https://www.interpol.int/es/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_SP.pdf

Machuca-Rubio, J. B., & Cabrera-Duffaut, A. (2020). Percepción de la exposición en seguridad informática de los niños y adolescentes durante la pandemia COVID-19. *Polo del Conocimiento*, 5(1), 37-51.

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

Monges Olmedo, M. R., & Jiménez Chaves, V. E. (2020). Seguridad de la información en plataformas de e-learning en tiempos de pandemia COVID-19. *Revista UNIDA Científica*, 4(1), 1-27. http://revistacientifica.unida.edu.py/publicaciones/index.php/cientifica/article/view/9

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. https://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? I*nformation Management & Computer Security*, 20(1), 18-28. https://doi.org/10.1108/09685221211219173

PwC. (2020). *Seguridad de la información en tiempos de COVID-19*. pwc.com/co. https://www.pwc.com/co/es/pwc-times/Seguridad-informacion-tiempos-COVID-19.html

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

Roque Hernández, R. V., & Juárez Ibarra, C. M. (2018). Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios.

PAAKAT: *Revista de Tecnología y Sociedad*, 8(14), 00005. https://doi.org/10.32870/pk.a8n14.318

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

UNISYS. (2020). 2020 *Unisys Security Index™*. https://www.unisys.com/unisys-security-index