Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: IX Número: 3. Artículo no.:12 Período: 1ro de mayo al 31 de agosto del 2022.

TÍTULO: La paradoja de la seguridad informática durante la pandemia. ¿Son más vulnerables los alumnos de tecnologías de la información?

AUTORES:

1. Est. Felipe Baltazar Maldonado Ortiz.
2. Dr. Ramón Ventura Roque Hernández.
3. Dr. Rolando Salazar Hernández.
4. Máster. Yuritzi Llamas Mangin.

RESUMEN: La seguridad es un área de la informática cuya importancia ha crecido durante la pandemia por COVID-19. Este estudio se realizó con el objetivo de comparar los niveles de seguridad informática de los alumnos de la Licenciatura en Administración y de la Licenciatura en Tecnologías de la Información a través del análisis de sus percepciones, usos y hábitos. Se utilizó un diseño cuantitativo y transversal. Participaron 321 estudiantes de ambas carreras. Se encontró que todos pueden mejorar su seguridad; sin embargo, los alumnos de tecnologías son quienes podrían ser más vulnerables, pues se involucraron en actividades riesgosas y fueron víctimas cibernéticas con mayor frecuencia; así la capacitación, la concientización y los programas universitarios de apoyo se deben impulsar constantemente.

PALABRAS CLAVES: seguridad informática, estudiantes universitarios, educación superior, pandemia, ciberseguridad.

TITLE: The paradox of computer security during the pandemic. Are information technology students more vulnerable?

AUTHORS:

1. Stud. Felipe Baltazar Maldonado Ortiz.
2. PhD. Ramón Ventura Roque Hernández.
3. PhD. Adán López Mendoza.
4. Master. Yuritzi Llamas Mangin.

ABSTRACT: Security is an area of computing that has grown in importance during the COVID-19 pandemic. This study was carried out with the objective of comparing the levels of computer security of the students of the Bachelor of Administration and the Bachelor of Information Technologies through the analysis of their perceptions, uses and habits. A quantitative and cross-sectional design was used. 321 students from both careers participated. It was found that everyone can improve their security; however, technology students are the ones who could be more vulnerable, since they were involved in risky activities and were cyber victims more frequently; thus, training, awareness and university support programs must be constantly promoted.

KEY WORDS: computer security, university students, higher education, pandemic, cybersecurity.

INTRODUCCIÓN.

La seguridad es un área de la informática que ha tenido una creciente importancia en los últimos años. A partir de la aparición del SARS-COV2 y debido a las restricciones por el confinamiento, muchas de las actividades que antes se realizaban presencialmente se han tenido que realizar por medios electrónicos. Esta migración de la presencialidad a medios digitales ha implicado un incremento de riesgos en el área de seguridad informática.

El número de delitos informáticos aumenta cada vez más y los usuarios parecen estar cada vez más expuestos. Surge entonces una pregunta ¿Cómo es el nivel de seguridad informática de los usuarios de los sistemas? No es fácil abordar esta pregunta pues tiene muchas dimensiones y aristas. En un primer acercamiento para encontrar esta respuesta en el contexto universitario, este trabajo se realizó con los objetivos de caracterizar y comparar los niveles de seguridad informática de los alumnos de la licenciatura en administración y de la licenciatura en tecnologías de la información a través del análisis de sus percepciones, usos y hábitos. Se eligieron estas dos carreras con el propósito de comparar un programa académico que posee un perfil completamente tecnológico con otro afín, pero sin esta acentuación.

DESARROLLO.

Antecedentes.

Tiempo atrás, la seguridad informática era un tema primordial especialmente para las empresas, ya que eran quienes estaban más propensas a sufrir ataques cibernéticos. Hoy en día, la seguridad informática es un tema relevante no solo para las empresas sino para todos los usuarios de sistemas de información, pues cualquiera corre el riesgo de ser blanco de ataques cibernéticos, lo que puede ocasionar grandes pérdidas (Parkinson et al., 2021), ya sean económicas, de datos personales, identidad, o de reputación. Esto ha sido motivado por la creciente presencia de los sistemas y dispositivos inteligentes en casi todas las áreas de la cotidianidad. Se estima que hasta el año 2020 había más de 4.2 billones de estos dispositivos funcionando y accediendo a internet en el mundo (Alzubaidi, 2021).

Desde 2020, la sociedad ha vivido cambios radicales en todas las actividades diarias debido a la aparición y avance de la pandemia por SARS-COV2 (Haleem et al., 2020). De un momento a otro, las personas comenzaron a trabajar desde sus hogares para prevenir los contagios.

Por otra parte, los estudiantes y maestros también migraron sus actividades escolares hacia la modalidad virtual (Gillis y Krull, 2020), ya que los medios electrónicos fueron el escenario de tantas actividades en este tiempo de contingencia; la ciberseguridad adquirió una importancia todavía más decisiva. Los ciber delincuentes incrementaron sus ataques y han aprovechado toda oportunidad para entrometerse, robar información, o simplemente molestar; por ejemplo, durante la pandemia ha sido popular aprovecharse de las vulnerabilidades de los sistemas para realizar video conferencias. Tal es el caso de los ataques denominados Zoombombing, que suceden cuando personas que no fueron invitadas ingresan sin autorización a una vídeo conferencia para robar datos, o diseminar información falsa, grosera o inapropiada (Ospina-Díaz y Sanabria-Rangel, 2020), solo por mencionar uno de estos ciber delitos (Mohanty et al., 2022). Por otra parte, también la suplantación de identidad, los fraudes y los chantajes cibernéticos se han incrementado en los últimos meses.

Durante la pandemia y antes de ella, las contraseñas de texto han sido un medio popular para implementar restricciones y accesos selectivos (Kim et al., 2021); sin embargo, las contraseñas deben crearse con características que garanticen su robustez; es decir, que dificulten el acceso a los intrusos. Además, el uso, los hábitos y la conciencia de las personas con respecto a sus contraseñas son elementos también muy importantes para lograr una verdadera seguridad (Buil-Gil et al., 2020).

En este orden de ideas, los seres humanos -usuarios- son un elemento vulnerable en cualquier estrategia de protección informática; es por esa razón, que la seguridad informática es un tema que debe abordarse y fortalecerse desde el entorno universitario (Stanciu y Tinca, 2016) con una perspectiva multi dimensional.

En los siguientes apartados de este artículo se presentan primero, los detalles metodológicos del trabajo; posteriormente, los principales hallazgos y su discusión, y finalmente, se abordan las conclusiones y recomendaciones.

Metodología.

Población y muestra.

La población de estudio consistió en los alumnos inscritos en una universidad pública del noreste de México en la carrera de Licenciatura en Administración (729) y en la Licenciatura en Tecnologías de la Información (222). Con la herramienta en línea NetQuest (NetQuest, 2021) se hizo un cálculo de la muestra para tener 90% de confianza, una heterogeneidad del 50% y un margen de error del 5%. Con estos parámetros, se obtuvo una muestra de 198 alumnos de la carrera de Administración y 123 de la carrera de Tecnologías de la información; esto quiere decir, que al encuestar a los 321 alumnos, las variables medidas estarían en un intervalo de $\pm$ 5% respecto a los datos observados en las encuestas.

Procedimiento.

La investigación inició con una búsqueda bibliográfica orientada a conocer más sobre la seguridad informática, las percepciones sobre ella, los hábitos de los usuarios, y de manera particular, el uso de las contraseñas.

Todo eso se tomó en consideración para diseñar un cuestionario para recolectar datos entre los participantes. El cuestionario tenía el propósito de conocer algunos aspectos concretos sobre conductas, hábitos y percepciones de los usuarios de sistemas de cómputo. El cuestionario pasó por varias etapas de refinamiento, en donde participaron tres expertos, se condujo una prueba piloto y se ajustó la redacción de las preguntas. El cuestionario se implementó en un formulario de Google Forms, cuyo hipervínculo se compartió con los alumnos de los distintos grupos.

La participación fue anónima, voluntaria y no remunerada. Todos los participantes dieron su consentimiento para ser parte del estudio. Se les garantizó el anonimato y la privacidad de sus respuestas individuales.

Análisis de datos.

El análisis de datos se realizó con el software JASP (JASP, 2021) y consistió en la obtención de estadísticos descriptivos, así como en la aplicación de pruebas de Shapiro Wilk, Mann-Whitney y Xi Cuadrado. Las pruebas de Shapiro-Wilk mostraron que las respuestas no tenían distribución normal, por lo que se optó por utilizar estadística no paramétrica (Siegel y Castellan, 2015). De esta manera, las pruebas de diferencias de Mann-Whitney se aplicaron a las respuestas de tipo ordinal y las pruebas Xi Cuadrado se aplicaron a las categóricas.

Para las comparaciones se tomaron en cuenta las respuestas recabadas en ambos programas académicos: Licenciatura en Administración y Licenciatura en Tecnologías de la Información. Para todas las comparaciones, se utilizó un nivel de confianza del 90%.

Resultados.

Los resultados de las pruebas de diferencias entre los alumnos de Administración y los de Tecnologías de la Información sobre sus percepciones en seguridad informática se muestran en la Tabla 1. Las diferencias sobre usos de las contraseñas se presentan en la Tabla 2. Finalmente, en la Tabla 3 se encuentran los resultados de las comparaciones en las preguntas dicotómicas del cuestionario.

Tabla 1. Resultados de las pruebas de diferencias Mann-Whitney entre alumnos de Administración y de Tecnologías sobre sus percepciones en seguridad informática.

Planteamiento	Licenciatura en Administración Mediana (R.I.)	Licenciatura en Tecnologías de la información Mediana (R.I.)	W	p	Tamaño del efecto (Correlación Rango-Biserial)
¿Qué tanto conoces sobre seguridad informática?	5(3)	6(3)	10954.00	0.126	-0.100
¿Qué tan importante consideras que es la seguridad informática en tiempos de pandemia?	10(1)	10(1)	13237.00	0.135	0.087

¿Qué tan importante consideras que es contar con un antivirus instalado en tiempos de pandemia?	10(1.75)	9(2)	14348.00	0.003 *	0.178
¿Qué tan seguro te sentías en las clases en línea durante la pandemia?	7(4)	7(3)	12588.00	0.608	0.034
¿Qué tan probable es que abras un archivo adjunto de un correo de un contacto desconocido?	1(3)	1(3)	11967.50	0.774	-0.017
¿Qué tan probable es que abras un artículo de Facebook de una fuente desconocida?	2(4)	2(4)	11998.50	0.818	-0.015

Fuente: elaboración propia.

Tabla 2. Resultados de las pruebas de diferencias Mann-Whitney entre alumnos de Administración y de Tecnologías sobre usos y costumbres de los usuarios con sus contraseñas.

Planteamiento	Licenciatura en Administración Mediana (R.I.)	Licenciatura en Tecnologías de la información Mediana (R.I.)	W	p	Tamaño del efecto (Correlación Rango-Biserial)
¿De cuántos caracteres en total es tu contraseña para ingresar a MSTEAMS?	9(2)	8(2)	12824.00	0.408	0.053
¿Cuántas mayúsculas tiene tu contraseña para ingresar a MSTEAMS?	1(1)	1(2)	10867.00	0.093 *	-0.108
¿Cuántos caracteres especiales tiene tu contraseña para ingresar a MSTEAMS?	1(2)	1(3)	12160.50	0.984	-0.001
¿Qué tan probable es que comparta su contraseña de MSTEAMS con otras personas?	1(1)	1(2)	11467.00	0.311	-0.058
¿De cuántos caracteres en total es tu contraseña para ingresar a FACEBOOK?	10(4)	10(4)	12023.50	0.849	-0.013
¿Cuántas mayúsculas tiene tu contraseña para ingresar a FACEBOOK?	1(1)	1(2)	11527.00	0.391	-0.053
¿Cuántos caracteres especiales tiene tu contraseña para ingresar a FACEBOOK?	1.5(2.75)	2(3)	11633.00	0.494	-0.045

¿Qué tan probable es que compartas contraseñas a través de redes sociales?	1(0)	1(0)	11625.50	0.276	-0.045
¿Qué tan probable es que utilices la misma contraseña en más de un sitio?	4(7)	3(6)	13163.50	0.214	0.081

Fuente: elaboración propia.

Tabla 3. Resultados de las pruebas Xi^2 de diferencias para las preguntas dicotómicas.

Planteamiento	Licenciatura en Administración Mediana (R.I.)		Licenciatura en Tecnologías de la información Mediana (R.I.)		Xi^2	p	V de Cramer
	No	Sí	No	Sí			
¿Cambiaste tu contraseña de MSTEAMS durante la contingencia?	158 (162)	40 (35)	106 (101)	17 (21)	2.11	0.146	0.081
¿Cambiaste tu contraseña de FACEBOOK durante la contingencia?	121 (117)	77 (80)	70 (73)	53 (49)	0.556	0.456	0.042
¿Conoces cómo cambiar la contraseña de tu modem?	86 (68)	112 (129)	25 (42)	98 (80)	17.91	<.001*	0.236
¿Cambiaste la contraseña de tu modem durante la contingencia?	157 (146)	41 (51)	81 (91)	42 (31)	7.148	0.008*	0.149
¿Has compartido alguna información personal durante la contingencia?	119 (115)	79 (82)	68 (71)	55 (51)	0.724	0.395	0.047
¿Has agregado contactos desconocidos en tus redes sociales?	128 (119)	70 (78)	65 (73)	58 (49)	4.407	0.036*	0.117
¿Tuviste algún antivirus instalado en tu computadora durante la contingencia?	81 (78)	117 (119)	46 (48)	77 (74)	0.391	0.532	0.035
¿Tu antivirus contaba con licencia?	89 (90)	109 (107)	58 (56)	65 (66)	0.149	0.700	0.022
¿Instalaste algún software pirata durante la contingencia?	179 (162)	19 (35)	85 (101)	38 (21)	25.566	<.001*	0.271
¿Realizaste compras en línea durante la contingencia?	92 (84)	106 (113)	45 (52)	78 (70)	3.027	0.082*	0.097

¿Realizaste pagos con tarjeta bancaria durante la contingencia?	113 (107)	85 (90)	61 (66)	62 (56)	1.709	0.191	0.073
¿Fuiste víctima de algún incidente de seguridad durante esta contingencia?	194 (188)	4 (9)	111 (116)	12 (6)	9.587	0.002*	0.173
Además de tomar clases ¿Realizaste alguna otra actividad en línea?	144 (138)	54 (59)	81 (86)	42 (36)	1.710	0.191	0.073

Fuente: elaboración propia.

Discusión de los resultados.

En las percepciones en seguridad informática solamente se encontró una diferencia significativa relacionada con la importancia de contar con un antivirus instalado. Los alumnos de Administración lo consideraron más importante que los de Tecnologías de la Información.

Acerca del uso de contraseñas, solamente se encontró divergencia en el número de letras mayúsculas que tiene la contraseña para ingresar a la plataforma de MSTEAMS. Se observó que esta desigualdad está relacionada con la mayor variación que presentan las respuestas de los alumnos de Tecnologías.

En las preguntas categóricas, como era esperado, se encontró que los alumnos de Tecnologías no solo conocían mejor el procedimiento de cambiar la contraseña de su modem, sino que en realidad la cambiaron con mayor frecuencia (34%) que los de Administración (20%) durante la pandemia.

Se encontró que los alumnos de Tecnologías fueron más propensos a agregar contactos desconocidos en sus redes sociales (47%), así como a instalar programas ilegales en sus computadoras (30%) y a realizar compras en línea durante la pandemia (63%) que los alumnos de Administración (35%, 9% y 53%, respectivamente). Cabe destacar, que también fueron los alumnos de Tecnologías quienes resultaron víctimas de incidentes de seguridad informática durante la pandemia con mayor frecuencia (9%) que los de Administración (2%).

Los resultados indican que a pesar de que los conocimientos sobre seguridad informática y la percepción de su importancia no son significativamente diferentes en los dos programas académicos analizados, los alumnos de Tecnologías son quienes han tenido mayores conductas riesgosas. Además, entre los alumnos de Tecnologías se detectó un posible mayor riesgo debido a la menor importancia percibida sobre los antivirus y a la mayor variabilidad en la seguridad de las contraseñas que utilizan.

CONCLUSIONES.

La seguridad es un área de la informática que ha tenido una creciente importancia en los últimos años. Debido a las restricciones por el confinamiento, muchas de las actividades que antes se realizaban presencialmente, a partir de la pandemia por COVID-19, se han tenido que realizar por medios electrónicos. Esta migración de actividades a medios digitales ha implicado un incremento de riesgos de seguridad informática.

El presente estudio reveló, que si bien tanto los alumnos de Administración como los de Tecnologías pueden mejorar sus niveles de seguridad; son los estudiantes con acentuación en Tecnología quienes podrían ser más vulnerables; esto debido a que se involucraron en actividades riesgosas y reportaron haber sido víctimas cibernéticas con mayor frecuencia.

Aunque este fue un estudio cuyo ámbito se circunscribió a una sola facultad universitaria, brinda un panorama fértil para continuar investigando sobre esta misma línea. Es recomendable fortalecer los conocimientos, las habilidades y los valores de los estudiantes con el objetivo de mejorar su seguridad en el uso de los sistemas informáticos. En este sentido, la capacitación, la concientización y la creación de programas institucionales permanentes son elementos clave que se deben impulsar en el contexto universitario.

REFERENCIAS BIBLIOGRÁFICAS.

1. Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(1), e06016. https://doi.org/10.1016/j.heliyon.2021.e06016
2. Buil-Gil, D., Lord, N., & Barrett, E. (2020). The Dynamics of Business, Cybersecurity and Cyber-victimization: Foregrounding the Internal Guardian in Prevention. *Victims & Offenders*, *16*(3), 286–315. https://doi.org/10.31235/osf.io/nd6xg
3. Gillis, A., & Krull, L. M. (2020). COVID-19 Remote Learning Transition in Spring 2020: Class Structures, Student Perceptions, and Inequality in College Courses. *Teaching Sociology*, 1–17. https://doi.org/10.1177/0092055X20954263
4. Haleem, A., Javaid, M., & Vaisha, R. (2020). Effects of COVID-19 pandemic in daily life. *Current Medicine Research and Practice*, *10*(January), 78–79.
5. JASP. (2021). *JASP*. https://jasp-stats.org/
6. Kim, P., Lee, Y., Hong, Y. S., & Kwon, T. (2021). A password meter without password exposure. *Sensors (Switzerland)*, *21*(2), 1–25. https://doi.org/10.3390/s21020345
7. Mohanty, M., Jena, R., & Singh, P. (2022). Can Zoom video conferencing tool be misused for real-time cybercrime? *WIREs Forensic Science*, *4*(1), 1–6. https://doi.org/10.1002/wfs2.1419
8. NetQuest. (2021). *Calculadora de la muestra NETQUEST*. Www.Netquest.Com.
9. Ospina-Díaz, M. R., & Sanabria-Rangel, P. E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad*, *62*(2), 199–217.
10. Parkinson, S., Khan, S., Crampton, A., Xu, Q., Xie, W., Liu, N., & Dakin, K. (2021). Password policy characteristics and keystroke biometric authentication. *IET Biometrics*, *July 2020*, 163–178. https://doi.org/10.1049/bme2.12017

11. Siegel, S., & Castellan, N. J. (2015). *Estadística no paramétrica aplicada a las ciencias de la conducta*. Trillas.
12. Stanciu, V., & Tinca, A. (2016). Students' awareness on information security between own perception and reality-an empirical study. *Accounting and Management Information Systems, 15*(1), 112–130.

DATOS DE LOS AUTORES.

1. **Felipe Baltazar Maldonado Ortiz.** Es estudiante de Licenciatura en Tecnologías de la Información en la Facultad de Comercio, Administración y Ciencias Sociales de Nuevo Laredo, Tamaulipas, México. Participó en el verano de investigación DELFIN. Correo electrónico: felipeortiz105@gmail.com
2. **Ramón Ventura Roque Hernández.** Es Doctor en Ingeniería Telemática y Doctor en Educación. Actualmente es profesor investigador de tiempo completo en la Facultad de Comercio, Administración y Ciencias Sociales de la Universidad Autónoma de Tamaulipas, México. Correo electrónico: rvhernandez@uat.edu.mx
3. **Rolando Salazar Hernández.** Es Doctor en Tecnologías Multimedia. Actualmente es profesor investigador de tiempo completo en la Facultad de Comercio, Administración y Ciencias Sociales de la Universidad Autónoma de Tamaulipas, México. Correo electrónico: rsalazar@docentes.uat.edu.mx
4. **Yuritzi Llamas Mangin.** Es Maestra en Administración Integral del Ambiente. Actualmente es docente de tiempo completo en la Facultad de Comercio, Administración y Ciencias Sociales de la Universidad Autónoma de Tamaulipas, México. Correo electrónico: yuritzi.llamas@docentes.uat.edu.mx

RECIBIDO: 7 de marzo del 2022. **APROBADO:** 27 de abril del 2022**.**