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: V Número: 3 Artículo no.: 55 Período: 1ro de mayo al 31 de agosto del 2018.

TÍTULO: Preliminares para diseñar un plan de capacitación y concientización en seguridad informática: Diferenciando los conocimientos, hábitos y percepciones de los usuarios de distintas edades.

AUTORES:

1. Dr. Ramón Ventura Roque Hernández.

2. Dra. Frida Carmina Caballero Rico.

3. Lic. Abraham Rogelio del Carmen de la Peña.

RESUMEN: Este artículo presenta una investigación que comparó los conocimientos, hábitos y percepciones en seguridad informática entre personas menores de 35 años y personas de 35 años o más para determinar sus requerimientos para un plan de capacitación y concientización. Se encuestó a 71 usuarios no profesionales de sistemas informáticos. Se aplicaron pruebas t y $Jí^2$ para buscar diferencias. Los jóvenes percibieron tener mayor conocimiento de informática, virus y seguridad; también reportaron tener buenas contraseñas pero poca preocupación ante el robo de información. Los jóvenes registraron una alta probabilidad para instalar software ilegal en sus computadoras, contrariamente a los mayores. Se concluye que es importante promover la capacitación y la concientización en ambos grupos tomando en cuenta sus necesidades particulares.

PALABRAS CLAVES: seguridad informática, Educación, usuarios, hábitos, percepciones.

TITLE: Preliminaries to design a plan of training and awareness in cyber-security: Differentiating knowledge, habits and perceptions of users of different ages.

AUTHORS:

1. Dr. Ramón Ventura Roque Hernández.

2. Dra. Frida Carmina Caballero Rico.

3. Lic. Abraham Rogelio del Carmen de la Peña.

ABSTRACT: This paper presents a research that compared knowledge, habits, and perceptions about information security between people younger than 35 years and people 35 years or older. This comparison was performed to elicit their requirements for a training and awareness program. 71 non-professional users of computer systems were surveyed. T and Chi-squared tests were performed to establish significant differences. Young people perceived they were more knowledgeable in Information Systems, Virus and Cyber-Security. They also had better passwords and a low level of concern about information theft. Young people were more likely to install illegal software in their computers than older people. We conclude that it is important to promote training and awareness in both groups taking into consideration their particular needs.

KEY WORDS: information security, Education, users, habits, perceptions.

INTRODUCCIÓN.

La seguridad informática, sin duda, es un tema de actualidad debido a la constante interacción de las personas con la tecnología, a los crecientes riesgos que implica la despreocupación en su uso y al desconocimiento de buenas prácticas de prevención y defensa. La investigación sobre hábitos, costumbres y percepciones sobre seguridad informática es necesaria para determinar riesgos

potenciales, prever cursos de acción para evitarlos y tomar decisiones orientadas a la disminución de riesgos e incidentes para los usuarios finales.

El presente trabajo tuvo por objetivo comparar los conocimientos, percepciones, hábitos y prácticas de la seguridad informática en dos grupos de personas: los jóvenes (menores de 35 años) y los mayores (35 años o más) para determinar si existen diferencias y en qué consisten. Este conocimiento permitiría conocer las fortalezas y debilidades de cada grupo y determinar si es necesario un solo plan de capacitación y concientización en seguridad informática orientado al público en general, o bien, si existen evidencias que sugieran realizar dos concreciones para atender las necesidades particulares de cada uno de estos grupos. Se eligió la edad de 35 años para dividir a la población de estudio debido a que el reporte de la Asociación de Internet (Infotec, 2017) indica que en México, la mayoría de los usuarios son menores de 35 años (72%) y solo el 28% son mayores de 35 años. Esto indica que la edad podría ser un factor relevante en el estudio de la informática y su seguridad, y por lo tanto, la capacitación y concientización de estos dos grupos de personas podría requerir una acentuación distinta.

Este artículo está organizado de la siguiente manera: primero se encuentran los antecedentes que incluyen los aspectos de seguridad informática relevantes para esta investigación y los trabajos previos reportados en la literatura. Posteriormente, se describe la metodología seguida para este estudio. Luego se presentan los resultados obtenidos y su discusión. Finalmente, se resumen las principales conclusiones de este artículo así como los trabajos futuros propuestos para continuar esta investigación.

DESARROLLO.

Antecedentes.

Aspectos de seguridad informática relevantes para este trabajo.

Código malicioso.

El término "código malicioso" se refiere a programas que han sido desarrollados para realizar acciones desfavorables para los usuarios. Este tipo de programas pueden causar la destrucción de datos, el uso no autorizado de recursos computacionales y el robo de información. Se puede distinguir entre virus, spyware y troyanos, por su naturaleza y conducta. Los virus son programas capaces de modificar otros programas, causar inconvenientes al usuario y reproducirse fácilmente para infectar otros equipos. Los programas spyware no se autoreproducen, pero funcionan como espías y ladrones de información sensible del usuario, quien regularmente no se da cuenta de su presencia. Los troyanos son programas que aparentan ser inofensivos y útiles, pero en realidad tienen una intención secundaria negativa: la de enviar información a otros equipos y abrir un hueco en las barreras de seguridad para que una persona externa sin autorización tome el control del sistema. Muchas personas tienen equipos de cómputo infectados con virus troyanos y pueden estar así durante meses o años sin darse cuenta (Rhodes-Ousley, 2013); por eso, es importante que los sistemas de cómputo cuenten con protección actualizada contra todo tipo de código malicioso.

Instalación de software.

Instalar software de aplicación en los equipos de cómputo es una actividad cotidiana; sin embargo, no todo el software se puede instalar libre o gratuitamente. Muchos de los programas comerciales más populares imponen restricciones tales como el pago de tarifas o un limitado número de instalaciones. La copia no autorizada de programas de cómputo, así como su uso en condiciones distintas a la que se especifica en la licencia, son actividades ilegales que encuentran en Internet un medio ideal de promoción (Velandia, Gallego, & Coca, 2016). La instalación de software no

autorizado conduce a riesgos de seguridad informática principalmente asociados a código malicioso agregado que puede provocar pérdidas de información y vulnerabilidades en los sistemas. En un estudio conducido por Gantz y sus colaboradores (Gantz, y otros, 2015), se logró determinar que el software ilegal y la presencia de código malicioso poseen una fuerte correlación estadística positiva; esto quiere decir, que al aumentar el índice de programas ilegales instalados, la presencia de código malicioso también aumenta.

Contraseñas.

La identificación y autenticación de los usuarios son la base de los servicios que se ofrecen a través de Internet. Las contraseñas son el sistema de autenticación preferido en internet por ser flexibles y de bajo costo (Miguel Pérez, 2015). Keszthelyi (Keszthelyi, 2013) menciona que seleccionar y usar buenas contraseñas es de importancia crítica, especialmente en la era de crímenes cibernéticos en la que nos encontramos. Para las buenas contraseñas, la longitud es una característica importante, incluso más que la inclusión de letras, números y caracteres especiales que ha sido erróneamente difundida. De cualquier manera, se deben evitar combinaciones que sean fácilmente deducibles por otras personas, como por ejemplo, fechas, matrículas y nombres. No es recomendable utilizar la misma contraseña en diferentes servicios de Internet ni compartirla con otras personas por ningún medio. También es una buena práctica cambiarla regularmente. En su trabajo, Keszthelyi resalta que la educación teórica y práctica en seguridad informática es necesaria para evitar que las nuevas generaciones hereden las consecuencias de los problemas cibernéticos actuales.

Respaldos de información.

Los datos de un sistema informático son un elemento muy sensible que puede provocar graves pérdidas para cualquier usuario. Los respaldos son las copias de seguridad de los datos que hacen

posible su restauración completa en caso de alguna contingencia. Estas copias se deben guardar en un lugar distinto al que se encuentran los datos originales. El procedimiento es sencillo y económico; sin embargo, muchas personas no lo realizan regularmente (Palmgren, 2017). La frecuencia para realizar respaldos varía según la tasa de modificaciones de los datos; pueden hacerse diariamente o una vez a la semana; sin embargo, si los datos sufren muchos cambios, los respaldos deberían realizarse más frecuentemente.

Estudios previos.

De acuerdo al estudio de Infotec (Infotec, 2017), existen 70 millones de internautas en México contabilizados hasta el 2016. El 72% de ellos se ubican entre 34 años o menos y el 28% tienen 35 años o más. El 52% de los internautas en México se encuentran conectados a Internet todo el día. En cuanto a las actividades en línea, el 83% de los mexicanos usa Internet para acceder a redes sociales y el 78% para enviar o recibir correos electrónicos. Estas cifras indican que un gran número de personas enfrentan constantemente riesgos de seguridad tan solo en nuestro país, y que dos de sus principales actividades en Internet requieren obligadamente el uso de contraseñas. Esto lo confirma una publicación del Senado de la República Mexicana (Senado de la República Mexicana, 2016), que explica que las amenazas latentes en seguridad informática han derivado en fraudes o delitos efectuados a través de redes sociales a 37 de cada 100 personas en este país.

En un estudio realizado por Kaspersky Lab (Kaspersky Lab, 2017), se compararon las actitudes y acciones de los usuarios jóvenes y los usuarios mayores. Se encontró que los usuarios de mayor edad son más cautos en relación a la seguridad informática; sin embargo, no son tan hábiles para detectar estafas o amenazas. De acuerdo a los resultados de este estudio, los jóvenes instalan software y bajan archivos con impaciencia y son menos cautelosos al descargar contenido; de esta manera, los jóvenes no se enteran con detalle de las condiciones de los programas que instalan y

tienen altas probabilidades de convertirse en víctimas de ataques de seguridad pues exhiben comportamientos poco prudentes. En este estudio, se expone, que el 57% de los usuarios menores de 24 años fueron afectados en el año 2015 en comparación con el 34% de los usuarios mayores. De los afectados, el 17% de los mayores no entendió la manera en la que sucedió, en comparación con solo el 10% de los jóvenes. En ese estudio, se concluye, que los usuarios de edad avanzada no toman tantos riesgos con su información personal; sin embargo, no tienen la suficiente perspicacia para identificar las amenazas cibernéticas.

En una investigación realizada por CSID (CSID, 2012), se encontró que el 61% de los usuarios reutiliza contraseñas en varios sitios web y el 44% cambia sus contraseñas una sola vez al año como máximo. A pesar de estos hechos, el 89% se siente seguro con sus hábitos de seguridad actuales y el 21% reportó haber tenido, al menos, una cuenta en línea comprometida. También se halló que las contraseñas se reutilizan más entre personas de 18 a 24 años y que la contraseña promedio contiene entre 8 y 10 caracteres. La empresa investigadora recomendó educar a los usuarios sobre las consecuencias de los malos hábitos en el área de seguridad informática.

En un estudio conducido por Ranghetti y su equipo (Ranghetti, Jaeger, F. A., & Milnitsky, 2012), se encontró que lo usuarios más jóvenes tienden a tener contraseñas de más longitud que los usuarios de mayor edad. La investigación que hizo Bonneau (Bonneau, 2012) con 70 millones de cuentas de Yahoo reveló que las mejores contraseñas las poseen personas de mayor edad, y en general, la mayoría de los usuarios tienen contraseñas débiles fácilmente deducibles.

En el trabajo de Fernández-Alemán y sus compañeros (Fernández-Alemán, y otros, 2015), se resalta que las contraseñas son fundamentales para los sistemas de información y se menciona que aproximadamente el 90% de las brechas de seguridad en el año 2012 fueron debidas a una contraseña débil, o utilizada en más de un sitio, de acuerdo a un estudio conducido por Verizon. En el trabajo realizado por ellos, se detectó que el 62.2% de los participantes tenía contraseñas

débiles que eran demasiado cortas o incluían nombres, información personal o fechas importantes fáciles de adivinar.

Metodología.

Participantes y muestreo.

En esta investigación se contó con la participación de 71 personas que utilizan, por lo menos, un equipo de cómputo de escritorio, portátil o móvil. Ninguno de ellos era especialista en sistemas computacionales, informática o alguna área afín, pero todos utilizaban la computadora e Internet diariamente para sus actividades laborales o personales. Los participantes no recibieron ninguna remuneración por contestar a las preguntas del cuestionario. El muestreo fue no probabilístico. La selección de personas se realizó en lugares públicos en la ciudad de Nuevo Laredo, Tamaulipas, México de manera aleatoria, y en todos los casos se solicitó la aprobación voluntaria para participar en esta investigación.

La media de la edad total de los participantes fue de 34.97 años con una desviación estándar de 11.27. El grupo de jóvenes estuvo integrado por 37 participantes, y el grupo de mayores por 34. Los detalles de la muestra se encuentran en la Tabla 1.

Tabla 1. Participantes en el estudio.

	Jóvenes (menos de 35 años)	**Mayores (35 años o más)**	**Total**
Hombres	24	18	42
Mujeres	13	16	29
Total	37	34	71

Instrumento.

Como instrumento de recolección de datos se utilizó un cuestionario con 20 preguntas, aplicado impreso en dos hojas de papel tamaño carta a cada uno de los participantes. Las preguntas fueron contestadas directamente en las hojas de papel. La Tabla 2 presenta las preguntas del cuestionario, sus valores posibles de respuesta y los identificadores que se usaron en este trabajo.

Tabla 2. Instrumento de recolección de datos.

Identificador	Pregunta	Valores posibles de respuesta
P1	¿Qué tanto conoce de informática?	0 a 10
P2	¿Qué tanto conoce sobre la seguridad informática?	0 a 10
P3	¿Qué tanto conoce sobre virus informáticos?	0 a 10
P4	¿Qué tan probable es que instale en su computadora un programa que no es original?	0 a 10
P5	¿Cuántas veces ha sido usted víctima de un robo de identidad en los últimos doce meses?	0 a 10
P6	¿Ha comprado antivirus originales en los últimos doce meses?	SI / NO
P7	¿Ha utilizado antivirus que son gratis por un periodo de tiempo?	SI / NO
P8	¿Qué tanto le preocupa que su información personal pueda ser robada al utilizar internet?	0 a 10
P9	¿Cuántas películas de Internet ha visto en los últimos 30 días?	0 a 10
P10	¿Cuántos respaldos de información personal ha realizado en los últimos 30 días?	0 a 10
P11	¿Cuántas veces ha visitado una institución especializada en la protección de los datos personales en los últimos 12 meses?	0 a 10
P12	En los últimos doce meses ¿Cuántas veces ha utilizado los conocimientos de algún especialista para que le asesore en el área de seguridad informática?	0 a 10
P13	¿Qué medio utiliza más para realizar transacciones bancarias?	Computadora de escritorio / Computadora portátil /Celular / Tablet / Otros
P14	¿Qué medio utiliza más para revisar su correo?	Computadora de escritorio / Computadora portátil /Celular / Tablet / Otros
P15	¿Cuántas cuentas activas de correo electrónico revisa usted diariamente?	0 a 10
P16	¿Qué tan probable es que en una contraseña usted establezca fechas importantes, como por ejemplo cumpleaños o aniversarios?	0 a 10
P17	¿Qué tan probable es que usted comparta alguna de sus contraseñas con otra persona?	0 a 10
P18	¿Con qué proveedor tiene usted la cuenta de correo electrónico que más utiliza?	Hotmail / Yahoo! / Gmail / Outlook
P19	¿Cuántos caracteres en total (longitud) tiene la contraseña de la cuenta de correo electrónico que usted más utiliza?	1 a 19
P20	¿Cuántos caracteres especiales tiene la contraseña de la cuenta de correo electrónico que usted más utiliza (por ejemplo: ¡”#$%&/()=?¡°¨*) ?	1 a 19

Análisis de datos.

Una vez que las respuestas fueron recabadas, éstas se capturaron en el software estadístico SPSS versión 22. Ahí se condujeron procedimientos preliminares para asegurar que los datos estaban completos y reflejaban correctamente las respuestas expresadas en papel por los participantes. Posteriormente, se procedió a la formación de dos grupos: uno con los participantes con edad menor a 35 y otro con los participantes con 35 años o más. Posteriormente, se plantearon hipótesis de diferencias entre jóvenes y mayores para cada una de las preguntas.

Con la finalidad de decidir si se podían establecer diferencias entre los grupos y de acuerdo a lo expuesto por Zikmund (Zikmund, Barry, Carr, & Griffin, 2013), se realizaron dos tipos de pruebas: para las preguntas cuya respuesta era numérica (preguntas números 1-5, 8-12, 15-17, 19-20) se condujeron pruebas t para grupos independientes. Para las preguntas cuya respuesta era categórica (preguntas 6, 7, 13, 14, 18) se realizaron pruebas $Jí^2$, buscando diferencias entre las distribuciones de las posibles respuestas debidas a la edad. Se trabajó con un 95% de confianza, por lo que un PValor menor que .05 fue indicador de diferencias estadísticas significativas. Finalmente se reflexionó y se concluyó sobre los resultados encontrados.

Resultados.

Los estadísticos descriptivos y los resultados de las pruebas t de las preguntas del cuestionario con escala numérica se encuentran en la

Tabla *3*. Los datos descriptivos para las preguntas del cuestionario cuya respuesta es categórica se muestran las Tablas 4, 5, 6, 7 y 8.

Tabla 3 Datos descriptivos y resultados de las pruebas t para las preguntas cuya respuesta tiene escala numérica.

Pregunta	**Jóvenes**		**Mayores**		**Resultado prueba t**		
	Media	**Desv. Std.**	**Media**	**Desv. Std.**	**P Valor**	**t**	**gl**
P1. ¿Qué tanto conoce de informática?	7.25	1.87	5	2.42	.000	4.63	69
P2. ¿Qué tanto conoce sobre la seguridad informática?	6.69	2.30	4.75	2.57	.001	3.47	68
P3. ¿Qué tanto conoce sobre virus informáticos?	6.67	2.29	4.41	2.60	.000	4.10	69
P4. ¿Qué tan probable es que instale en su computadora un programa que no es original?	7.58	2.37	4.72	2.89	.000	4.70	69
P5. ¿Cuántas veces ha sido usted víctima de un robo de identidad en los últimos doce meses?	1.03	2.32	.72	1.88	.482	.70	69
P8. ¿Qué tanto le preocupa que su información personal pueda ser robada al utilizar internet?	5.83	3.88	8.06	2.87	.007	-2.77	65.5
P9. ¿Cuántas películas en Internet ha visto en los últimos 30 días?	4.56	3.90	3.38	3.95	.178	1.36	68
P10. ¿Cuántos respaldos de información personal ha realizado en los últimos 30 días?	2.22	2.66	1.09	2.17	.055	1.95	68
P11. ¿Cuántas veces ha visitado una institución especializada en la protección de los datos personales en los últimos 12 meses?	0.22	0.68	0.50	1.21	.262	-1.13	48.9
P12. En los últimos doce meses ¿Cuántas veces ha utilizado los conocimientos de algún especialista para que le asesore en el área de seguridad informática?	0.39	1.40	0.91	1.57	.159	-1.42	68
P15. ¿Cuántas cuentas activas de correo electrónico revisa usted diariamente?	2.06	1.17	2.50	2.56	.40	-.83	43.55
P16. ¿Qué tan probable es que en una contraseña usted establezca fechas importantes, como por ejemplo cumpleaños o aniversarios?	2.14	3.38	4.44	3.82	.014	-2.52	68

P17. ¿Qué tan probable es que usted comparta alguna de sus contraseñas con otra persona?	2.08	2.98	2.44	3.00	.698	-.390	67
P19. ¿Cuántos caracteres en total (longitud) tiene la contraseña de la cuenta de correo electrónico que usted más utiliza?	9.39	2.87	7.94	3.28	.038	2.11	68
P20. ¿Cuántos caracteres especiales tiene la contraseña de la cuenta de correo electrónico que usted más utiliza (por ejemplo: ¡”#$%&/()=?¡°¨*) ?	1.89	2.62	1.16	2.01	.205	1.27	68

Tabla 4 Frecuencias para la pregunta P6 ¿Ha comprado antivirus originales en los últimos 12 meses? ($Jí^2$ = .003, gl=1, pValor =.95).

	Jóvenes	**Mayores**
Sí	10 (27%)	9 (26.5%)
No	27 (73%)	25 (7.5%)

Tabla 5 Frecuencias para la pregunta P7 ¿Ha utilizado antivirus de prueba? ($Jí^2$ = .226, gl=1, pValor =.63).

	Jóvenes	**Mayores**
Sí	30 (81.1%)	26 (76.5%)
No	7 (18.9%)	8 (23.5%)

Tabla 6 Frecuencias para la pregunta P13 ¿Qué medio utiliza más para realizar transacciones bancarias? ($Jí^2$ = 5.81, gl=3, pValor =.12).

	Jóvenes	**Mayores**
Computadora de escritorio	10 (27%)	13 (38.2%)
Computadora portátil	7 (18.9%)	4 (11.8%)
Celular	8 (24.3%)	2 (5.9%)
Otros	11 (29.7%)	14 (41.2%)

Tabla 7 Frecuencias para la pregunta P14 ¿Qué medio utiliza más para revisar su correo electrónico? ($Jí^2$ = 1.10, gl=2, pValor =.57).

	Jóvenes	**Mayores**
Computadora de escritorio	17 (45.9%)	18 (52.9%)
Computadora portátil	8 (21.6%)	6 (17.6%)
Celular	12 (32.4%)	7 (20.6%)

Tabla 8 Frecuencias para la pregunta P18 ¿Cuál es el proveedor de la cuenta de correo electrónico que más utiliza? ($Jí^2$ = 7.99, gl=4, pValor =.09).

	Jóvenes	**Mayores**
Hotmail	15 (40.5%)	18 (52.9%)
Yahoo	2 (5.4%)	4 (11.8%)
Gmail	17 (45.9%)	6 (17.6%)
Outlook	3 (8.1%)	3 (8.8%)
Otro	0 (0%)	2 (5.9%)

Solamente en las preguntas con los siguientes indicadores: P1, P2, P3, P4, P8, P16, P19 se encontraron diferencias estadísticas significativas a través de pruebas t (Ver Tabla 9). En el resto de las preguntas no hubo diferencias estadísticas significativas con pruebas t ni con $Jí^2$.

Tabla 9 Preguntas en las que se encontraron diferencias estadísticas significativas.

Identificador	**Pregunta**
P1	¿Qué tanto conoce sobre informática en general?
P2	¿Qué tanto conoce sobre seguridad informática?
P3	¿Qué tanto conoce sobre virus informáticos?
P4	¿Qué tan probable es que instale un programa que no es original?
P8	¿Qué tanto le preocupa que su información pueda ser robada en internet?
P16	¿Qué tan probable es que en una contraseña usted incluya fechas importantes como por ejemplo, cumpleaños o aniversarios?
P19	¿Cuántos caracteres en total tiene la contraseña de la cuenta de correo que más utiliza?

Los resultados significativos se presentan a continuación:

P1. Conocimiento sobre informática.

Sí se encontraron diferencias estadísticas significativas entre los participantes jóvenes y los participantes de mayor edad (t(69)=4.63, pValor= .000). Los jóvenes reportaron tener más conocimiento (media=7.30, desviación estándar=1.86) que los mayores (media=4.97 desviación estándar=2.35).

P2. Conocimiento sobre seguridad informática.

Se encontraron diferencias estadísticas significativas entre los participantes jóvenes y los participantes con más edad (t(68)=3.45, pValor= .001). Los jóvenes reportaron tener más

conocimiento (media=6.73, desviación estándar=2.28) que los mayores (media=4.73 desviación estándar=2.54).

P3. Conocimiento sobre virus informáticos.

Se encontraron diferencias estadísticas significativas entre los participantes jóvenes y los participantes de mayor edad (t(69)=4.10, pValor= .000). Los jóvenes reportaron tener más conocimiento (media=6.73, desviación estándar=2.29) que los mayores (media=4.38 desviación estándar =2.52).

P4. Probabilidad de instalar software pirata.

Se encontraron diferencias estadísticas significativas entre los participantes jóvenes y los participantes con más edad (t(69)=4.70, pValor= .000). Es más probable que los jóvenes instalen programas que no son originales en sus computadoras (media=7.54, desviación estándar =2.35) que los participantes de mayor edad (media=4.65 desviación estándar =2.82).

P8. Preocupación sobre el robo de su información.

Se encontraron diferencias estadísticas significativas entre los participantes jóvenes y los participantes con más edad (t(65.55)=-2.77, pValor= .007). Los participantes de mayor edad dijeron estar más preocupados acerca del robo de su información por internet (media=8.18, desviación estándar =2.82) que los jóvenes (media=5.95 desviación estándar =3.89).

P16. Probabilidad de incluir fechas importantes en las contraseñas.

Se encontraron diferencias estadísticas significativas entre los participantes jóvenes y los participantes con más edad (t(68)=-2.52, pValor= .014). Los participantes de mayor edad tendrían más probabilidad de establecer contraseñas que incluyan fechas importantes (media=4.30, desviación estándar =3.84) que los jóvenes (media=2.14 desviación estándar =3.33).

P19. Longitud de las contraseñas en el correo electrónico.

Se encontraron diferencias estadísticas significativas entre los participantes jóvenes y los participantes con más edad (t(68)=2.11, pValor= .038). Los participantes jóvenes utilizan contraseñas más grandes en sus cuentas de correo electrónico principales (media=9.49, desviación estándar =2.89) que los participantes de mayor edad (media=7.94 desviación estándar =3.23).

Discusión.

Se encontró que las personas jóvenes perciben tener más conocimientos técnicos en el área de informática y seguridad que las personas mayores. También se observó que los jóvenes utilizan contraseñas de mayor longitud y es menos probable que usen fechas importantes para construirlas; sin embargo, se encontró un posible riesgo entre los usuarios jóvenes: ellos no se preocupan tanto por el posible robo de su información y toman el riesgo de instalar en sus computadoras software que no es original. Esta falta de preocupación, combinada con el exceso de confianza, hace a los jóvenes una población vulnerable y blanco perfecto para muchas amenazas informáticas en la actualidad. Por otra parte, las personas de mayor edad también son vulnerables debido al desconocimiento que tienen de estos temas. Coincidimos con Keszthelyi (Keszthelyi, 2013) y CSID (CSID, 2012) en que es importante promover la capacitación y la concientización sobre seguridad informática. Además, nosotros pensamos que esta capacitación debe hacerse entre jóvenes y personas de mayor edad a través de dos perfiles con una base común, pero acentuando aspectos diferenciados de acuerdo a las necesidades particulares de cada grupo.

Nuestros resultados concuerdan con el reporte de Kaspersky Lab (Kaspersky Lab, 2017) pues encontramos que los usuarios de mayor edad tienen una preocupación mayor por su información y una baja percepción sobre sus conocimientos informáticos; quizás por estas razones ellos tendrían

más cautela con la seguridad de sus datos, pero carecían de habilidad técnica para lidiar con las amenazas que enfrentan. También, de la misma manera que el reporte de Kaspersky, en nuestro trabajo encontramos que los jóvenes tienen una alta probabilidad de instalar software ilegal en sus equipos.

También nuestros hallazgos son similares a los de CSID (CSID, 2012), en cuanto a la longitud de las contraseñas. Ellos reportan entre 8 y 10 caracteres en promedio. En nuestro trabajo, las contraseñas de los jóvenes tienen en promedio 9.39 caracteres y las de los mayores, 7.94 caracteres.

Nuestros resultados también coinciden con los de Ranghetti y su equipo (Ranghetti, Jaeger, F. A., & Milnitsky, 2012), pues encontramos que los usuarios más jóvenes suelen tener contraseñas de más longitud que los usuarios de mayor edad; sin embargo, discrepan con los de Bonneau (Bonneau, 2012) quien reporta lo opuesto. Esto puede ser debido a que Bonneau estudió las contraseñas de un solo proveedor de correo electrónico y nosotros no impusimos esa restricción. Otras diferencias con ese trabajo son que nuestro tamaño de la muestra es reducido y que nuestros participantes pertenecen a una sola ubicación geográfica, siendo estas las limitaciones del estudio que presentamos.

La interpretación de nuestros principales resultados se muestra en la Tabla 10.

Tabla 10 Resumen e interpretación de los resultados obtenidos en esta investigación.

Identificador	**Pregunta**	**Interpretación**
P1	¿Qué tanto conoce sobre informática en general?	Los jóvenes perciben tener un mayor conocimiento sobre informática.
P2	¿Qué tanto conoce sobre seguridad informática?	Los jóvenes perciben tener un mayor conocimiento sobre seguridad informática.
P3	¿Qué tanto conoce sobre virus informáticos?	Los jóvenes perciben tener un mayor conocimiento sobre virus informáticos.
P4	¿Qué tan probable es que instale un programa que no es original?	Es más probable que los jóvenes instalen programas que no son originales en sus computadoras.
P8	¿Qué tanto le preocupa que su información pueda ser robada en	Las personas mayores muestran una mayor preocupación sobre el robo de su

	internet?	información.
P16	¿Qué tan probable es que en una contraseña usted incluya fechas importantes como por ejemplo, cumpleaños o aniversarios?	Es más probable que las personas de mayor edad incluyan fechas importantes en sus contraseñas.
P19	¿Cuántos caracteres en total tiene la contraseña de la cuenta de correo que más utiliza?	Los jóvenes utilizan contraseñas de mayor longitud.

CONCLUSIONES.

En este artículo se presentó un estudio que abordó la seguridad informática con una perspectiva de edad. Se ilustraron las diferencias encontradas entre conocimientos, hábitos y percepciones de los participantes jóvenes y los más mayores, y quedó en evidencia, que ambos grupos tienen sus fortalezas y debilidades en el área de la seguridad informática y que ambos deberían ser parte de un programa de capacitación y concientización orientado a atender sus necesidades particulares. Como trabajo futuro, se plantea aumentar el tamaño de la muestra, estudiar estos y otros aspectos de la seguridad informática a la luz de las generaciones X, Y, Z definidas en la literatura a partir de la edad de los participantes y desarrollar perfiles concretos de capacitación y concientización. También se propone abordar el tema central de este trabajo desde una perspectiva que incluya entrevistas personales y estudios de casos.

REFERENCIAS BIBLIOGRÁFICAS:

1. Bonneau, J. (2012). The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. 2012 IEEE Symposium on Security and Privacy (SP) (págs. 1-10). San Francisco, CA, USA: IEEE.
2. CSID. (2012). Consumer Survey: Password Habits. Estados Unidos: CSID.

3. Fernández-Alemán, J., Sánchez-Henarejos, A., García-Amicís, V., Toval, A., Sánchez-García, A., & Hernández-Hernández, I. (2015). Estudio sobre la importancia y la seguridad de uso de las contraseñas en el ámbito laboral sanitario. Gaceta Sanitaria, 74-76.
4. Gantz, J. F., Vavra, T., Lim, V., Soper, P., Smith, L., & Minton, S. (2015). El software sin licencia y las amenazas a la seguridad informática. Estados Unidos: BSA.
5. Infotec. (2017). Treceavo Estudio sobre los hábitos de los usuarios de internet en México 2017 de la asociación de Internet MX. Ciudad de México: Infotec.
6. Kaspersky Lab. (26 de octubre de 2017). Kaspersky Lab. Obtenido de Kaspersky Lab: https://latam.kaspersky.com/about/press-releases/2016_los-consumidores-mayores-de-edad-son-mas-cuidadosos-en-linea-pero-menos-diestros-en-cuanto-a-los-peligros
7. Keszthelyi, A. (2013). About Passwords. Acta Polytechnica Hungarica, 99-118.
8. Miguel Pérez, J. C. (2015). Protección de datos y seguridad de la información. México: Ra-Ma.
9. Palmgren, K. (2017). Respaldo y recuperación. Ciudad de México: UNAM CERT.
10. Ranghetti, D., Jaeger, A., F. A., C., & Milnitsky, L. (2012). Passwords Usage and Human Memory Limitations: A Survey across Age and Educational Background. Plos One, 1-7.
11. Rhodes-Ousley, M. (2013). Information Security - The Complete Reference. EU: McGraw-Hill.
12. Senado de la República Mexicana. (2016). Hábitos de los usuarios de internet y redes sociales en México, 2016. Visor Ciudadano.
13. Velandia, J., Gallego, M., & Coca, A. (2016). Análisis de la piratería de software en Colombia. Sexta Conferencia de Directores de Tecnología de Información, TICAL 2016. Gestión de las TICs para la Investigación y la Colaboración. Buenos Aires, Argentina.
14. Zikmund, W., Barry, B., Carr, J., & Griffin, M. (2013). Business Research Methods. Mason, Ohio, Estados Unidos: Cengage Learning.

DATOS DE LOS AUTORES:

1. **Ramón Ventura Roque Hernández**. Es Doctor en Ingeniería Telemática por la Universidad de Vigo, España y Doctor en Educación por la Universidad José Martí de Latinoamérica, México. Actualmente, es Profesor Investigador de la Universidad Autónoma de Tamaulipas, México en la Facultad de Comercio, Administración y Ciencias Sociales de Nuevo Laredo, Tamaulipas. Correo electrónico: rvHernandez@uat.edu.mx

2. **Frida Carmina Caballero Rico**. Es Doctora en Educación Internacional por la Universidad Autónoma de Tamaulipas, México. Actualmente es Profesora y Directora de Investigación de esa misma institución. Correo electrónico: FCaballer@uat.edu.mx

3. **Abraham Rogelio del Carmen de la Peña**. Es Licenciado en Informática y candidato al grado de Maestro en Administración de Negocios por la Universidad Autónoma de Tamaulipas, México. Correo electrónico: rogeliodelcarmen@gmail.com

RECIBIDO: 18 de enero del 2018. **APROBADO:** 21 de febrero del 2018**.**