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.:26 Período: 1ro de mayo al 31 de agosto del 2022.

TÍTULO: Hábitos y percepciones sobre Seguridad Informática en estudiantes universitarios pertenecientes a las generaciones Y, Z: Un estudio comparativo de dos universidades públicas en México.

AUTORES:

1. Dr. Adán López Mendoza.
2. Dr. Ramón Ventura Roque Hernández.
3. Dra. Ma. Teresa Prieto Quezada.
4. Dr. Rolando Salazar Hernández.

RESUMEN: El presente estudio tiene como objetivo determinar cuáles son las similitudes y diferencias respecto a los hábitos y percepciones de seguridad informática de los estudiantes universitarios pertenecientes a las generaciones Y, Z. El estudio se realizó en dos universidades públicas. La investigación es de corte cuantitativo-comparativo, y se enfocó en estudiantes de la carrera de Tecnologías de la Información. Para el análisis de los datos, se utilizó el programa Jamovi y SPSS versión 24. Los resultados arrojan que los estudiantes muestran diferencias significativas, principalmente en lo relacionado con la autopercepción que tienen con respecto a sus conocimientos sobre informática, seguridad informática, virus, robo de identidad, etc.

PALABRAS CLAVES: ciberseguridad, tecnología, educación superior.

TITLE: Habits and perceptions about Computer Security in university students belonging to generations Y, Z: A comparative study of two public universities in Mexico.

AUTHORS:

1. PhD. Adán López Mendoza.
2. PhD. Ramón Ventura Roque Hernández.
3. PhD. Ma. Teresa Prieto Quezada.
4. PhD. Rolando Salazar Hernández.

ABSTRACT: The objective of this study is to determine what are the similarities and differences regarding the habits and perceptions of computer security of university students belonging to generations Y, Z. The study was carried out in two public universities. The research is quantitative-comparative and focused on students of the Information Technology career. For the analysis of the data, the Jamovi and SPSS version 24 programs were used. The results show that the students show significant differences, mainly in relation to the self-perception they have regarding their knowledge about computers, computer security, viruses, theft of identity, etc.

KEY WORDS: cybersecurity, technology, higher education.

INTRODUCCIÓN.

La seguridad informática es un tema que ha cobrado gran importancia en los últimos años, ya que los dispositivos de comunicación y conectividad se han multiplicado de manera exponencial (Venter et al., 2019), y como consecuencia, lo mismo ha sucedido con los riesgos a los que están expuestos los usuarios de todas las edades. Esto es preocupante, ya que existen usuarios de sistemas informáticos desde menos de 6 años, hasta mayores de 80. La presente investigación centra su atención en dos generaciones de las que existen actualmente: Y, Z, de acuerdo con la clasificación de (Baysal, 2014). En la tabla 1 se muestran las generaciones y años de nacimiento incluidos.

Tabla 1. Generaciones y rangos de edades.

Generación	**Año de nacimiento**
Tradicionalista o Silencio	1900-1945
Baby Boomers	1946-1964
X	1965-1979
Y (Millenials)	1980-1994
Z (Internet o Cristal)	1995-

Fuente: Baysal Berkup (2014).

Una de las principales actividades humanas es la socialización. Este proceso de interactuar con otros suele ser tan habitual para todos, que hoy se encuentra estrechamente entrelazado con la tecnología cotidiana. Es así, como actualmente la mayoría de las comunicaciones se establecen por medios electrónicos. Tomando en cuenta que los estudiantes universitarios realizan gran parte de sus interacciones a través de dispositivos como teléfonos inteligentes, computadoras y tabletas, resulta pertinente analizar cómo perciben ellos la seguridad informática, qué hábitos tienen, y a qué riesgos se enfrentan, quizá de manera inadvertida.

Al respecto, Parsons et al., (2017) comenta que en repetidas ocasiones se ha señalado a las personas como “la primera línea de defensa” contra diferentes amenazas a la seguridad de la información. En ese sentido, es conveniente realizar investigaciones de este corte para estar en condiciones de conocer las percepciones de los usuarios y sus principales hábitos relacionados con la seguridad informática. De esta manera, se podrán identificar vulnerabilidades y sugerir actividades para reforzar las actitudes y aptitudes de los usuarios con el objetivo final de aumentar la ciber-resiliencia.

Esto, debido a que la ciberseguridad es un tema de creciente preocupación en los usuarios regulares de sistemas informáticos que continuamente se ven vulnerados.

El presente artículo expone los resultados de un estudio realizado con el objetivo de determinar el efecto de la generación (Y o Z) y del contexto -representado por dos instituciones mexicanas de educación superior distintas y geográficamente distantes- sobre las percepciones y hábitos en seguridad informática de los estudiantes universitarios. En los siguientes apartados se presentan, primero los antecedentes del tema, y posteriormente, la metodología, los resultados, su discusión, y finalmente, las conclusiones y líneas de trabajo futuro.

DESARROLLO.

Generaciones.

Existe una vasta literatura sobre las generaciones X, Y, Z a las cuales pertenecen adultos, jóvenes y niños. Cada uno de estos grupos son descritos ampliamente desde diferentes perspectivas como condiciones económicas, cambios sociales y desarrollos históricos significativos (Betz, 2019; Dida et al., 2021). Por primera vez en la historia contemporánea se tienen seis generaciones de personas diferentes haciendo uso de la tecnología; además de las tres generaciones mencionadas, se tienen dos anteriores que son conocidas como generación del silencio o tradicionalista y los “Baby Boomers” (Jiri, 2016).

Las personas pertenecientes a las primeras cinco generaciones de acuerdo con Baysal, (2014) se mostraron en la tabla 1; sin embargo, cabe mencionar que de acuerdo con una clasificación más reciente existe otra generación denominada *Alpha* para los nacidos posteriormente al año 2012 (Galbusera, 2020; Instituto Economía Digital, 2017).

Ferreiro (2006) señala que el concepto *generación* puede ser entendido como “conjunto de personas que comparten características distintivas según uno o varios criterios y que producen comportamientos similares”. Cada una de estas generaciones presenta características únicas de los

contextos en los que se han desarrollado; por ejemplo, la generación X presenta un mayor nivel de educación que las anteriores, pero es menor si se compara con las generaciones posteriores (Y -Millenials- y Z -Internet-). Es necesario aclarar, que existe una amplia gama de características que distinguen las diferentes generaciones, pero de ninguna manera se puede asumir que si una persona nació en el año de 1985, él o ella presentará la mayoría de las características que identifican a la generación Y, o que una persona que nació en los años de 1960, y que por lo tanto, pertenece a la generación Baby Boomers, será menos sofisticado tecnológicamente que una persona que pertenece a la Generación X o Y (Jirí, 2016).

Seguridad Informática.

La seguridad informática se ha investigado en diferentes contextos; por ejemplo, desde organizaciones privadas, instituciones públicas y universidades, hasta equipos de desarrollo de software. Shahim (2021) afirma, que en sus primeros años, la computación estaba centrada principalmente en diseño, desarrollo, mantenimiento y administración de la infraestructura de los centros de datos. En ese tiempo, la seguridad de los datos estaba más administrada por personal tipo *staff*. En la actualidad, eso ha cambiado, pues muchas empresas cuentan con su propio departamento y políticas sobre la seguridad de los datos. Además, hoy en día, la seguridad informática se tiene en alta prioridad, ya que tanto las personas como las empresas se encuentran más expuestas que nunca a riesgos y amenazas cibernéticas (Wang et al., 2020).

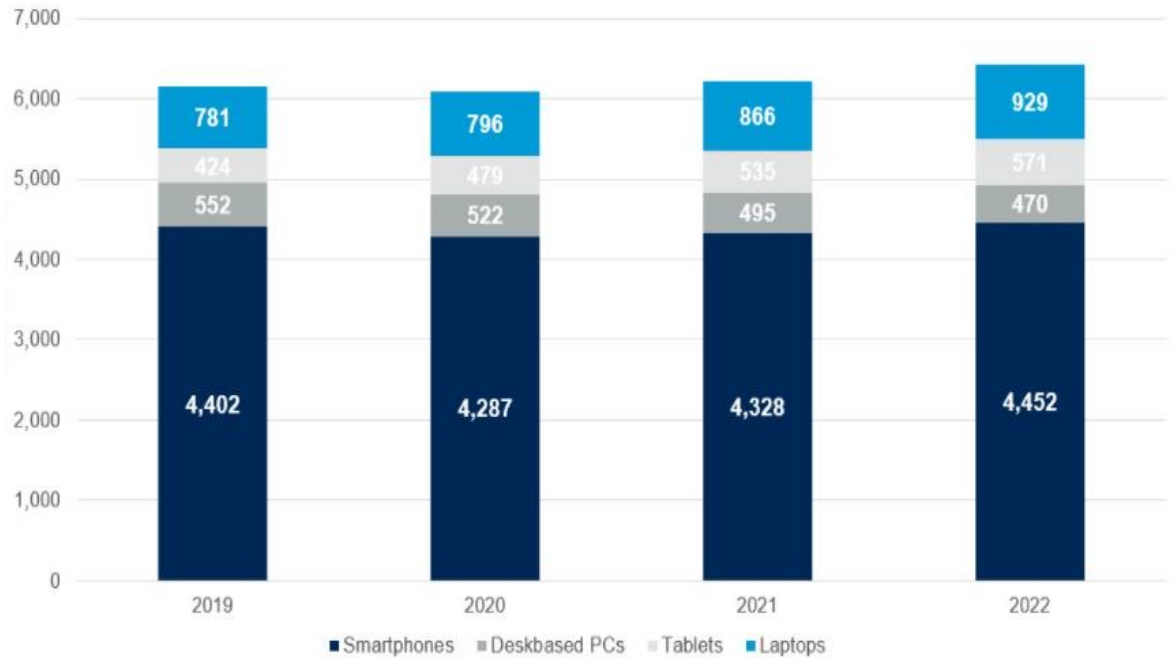
Kashif et al. (2018) define ciberseguridad como: “el conjunto de reglas, complementos tecnológicos, procesos y procedimientos para proteger los datos electrónicos, redes de computadoras y programas computacionales de cualquier ataque o acceso no autorizado”. Por su parte, Vogel, (2016) menciona que *ciberseguridad* es un concepto general para la piratería, espionaje, fraude y ataques a la infraestructura crítica, por lo que ahora se identifica como llave para la seguridad nacional. En su

estudio, Wang et al., (2020) añade que la ciberseguridad está compuesta por todas las tecnologías y prácticas para proteger los datos, las computadoras y los sistemas de redes.

Dispositivos conectados en 2021.

Desde hace varios años, el uso de los dispositivos conectados a internet ha ido en crecimiento constante. De acuerdo con Gartner.Com (2021), en el presente año 2021, se tendrán conectados a internet 6.2 billones de dispositivos electrónicos entre teléfonos celulares, tabletas, computadoras de escritorio y computadoras portátiles (ver figura 1). Se espera que se utilicen 125 millones más de tabletas y computadoras portátiles que en el año 2020; mientras que las computadoras de escritorio muestran una clara tendencia a la baja, ya que se espera que en el año 2022 se utilicen 470 millones de 522 utilizados en el 2020; es decir, una diferencia de 52 millones de computadoras de escritorio menos.

Figura 1. Dispositivos conectados a la red 2019-2022 (miles de unidades).



Fuente: Gartner.Com (Abril, 2021).

De acuerdo con el 17° Estudio sobre los Hábitos de los Usuarios de Internet en México 2021, actualmente en nuestro país existen 86.8 millones de usuarios de internet en edades de 6 años en delante, lo que representa el 76.3% de la población (Asociación de Internet Mx, 2021) que utiliza desde computadoras de escritorio, laptops, tabletas, teléfonos inteligentes, hasta consolas de videojuegos. De la totalidad de usuarios, un 15.8% tienen entre 18 y 24 años -que son la mayoría de las edades en las que se encuentran los estudiantes universitarios (Gen Z)-, estos estudiantes en pocos años pasarán a ser parte del mercado laboral.

Los otros dos grupos de edades de usuarios de internet que se encuentran por encima de este grupo son los que van en el rango de edad de 35-44 años con un 17.3%, mientras que el porcentaje más alto corresponde a las personas que van de los 25 a 34 años con un 20.2% (Asociación de Internet Mx, 2021). Con respecto al género, el mencionado estudio muestra que un 49.2% de los participantes son hombres y un 50.8% son mujeres, lo cual significa que prácticamente la mitad de los usuarios en México son hombres y la otra mitad son mujeres. Otro dato interesante y de cierta manera un tanto obvio -por el confinamiento debido a la pandemia- es que en el último año, la mayoría de los usuarios se conectaron a internet desde casa; el porcentaje de este lugar de conexión fue del 90%. Así mismo, se menciona en la investigación, que un 73% de los usuarios de internet han utilizado plataformas de videollamadas en el último año.

Por todos es conocido que constantemente se incrementa el número de dispositivos conectados a internet, los cuales son de mucha utilidad para realizar las diferentes actividades de las personas; ya sean de trabajo, estudio, ocio, entre otras; es decir, con el crecimiento de los usuarios y los equipos conectados a la red, se aumenta el riesgo de alguna amenaza. Si bien es cierto que existen organizaciones con todo un equipo especializado en ciberseguridad, también existen muchos usuarios con poco o nulo conocimiento sobre el tema, lo cual los vuelve más vulnerables. Para tratar

de prevenir esto, la ciberseguridad juega un papel fundamental para ayudar a la sociedad, a las organizaciones gubernamentales y a las universidades (Kashif et al., 2018; Parsons et al., 2017)

North y Pascoe (2016) mencionan, que la ciberseguridad es un tema de creciente preocupación, especialmente para las empresas del sector privado, pues son quienes con mayor frecuencia son víctimas de costosos ataques informáticos. En su trabajo, resaltan la importancia de concebir la seguridad como un tema de interés para toda la organización y no solo para el departamento de tecnología. Por otro lado, tenemos que en muchas ocasiones los incidentes de seguridad informática se deben a errores humanos. Esto se señala en el reporte elaborado por *IBM Global Technology Services* en el año 2014 (Parsons et al., 2017), cuyos autores identifican a los seres humanos como el eslabón más débil de la cadena de seguridad; por esta razón, es importante el estudio de los hábitos y percepciones, como una forma de anticiparse a las incidencias críticas de seguridad.

En el trabajo realizado por Roque y Juárez (2018), mencionan algunos de los riesgos que se corren al estar conectados a internet; entre los que se encuentran: *hackers*, *crackers*, gusanos, troyanos, *spyware*, *phishing*. Por su parte (Castaño et al., 2021; Gratian et al., 2018) mencionan que uno de los principales ataques en internet es el *phishing*, ya que solo en el último cuarto del año 2020 se alcanzaron a detectar cerca de 225,000 casos (Anti-Phishing Working Group (APWP) citado por Castaño et. al., 2021).

Estudiantes Universitarios y la Seguridad Informática.

Las universidades están conscientes de la necesidad de incluir en los programas de licenciatura junto con el grado, las habilidades necesarias en cuestiones de ciberseguridad para cuando el estudiante ingrese al mercado laboral, ya que si bien es cierto que los graduados poseen un conocimiento sólido en cuestiones teóricas al egresar, carecen de experiencia y de confianza para integrarse a dicho mercado (Johnson, 2019). Por su parte, van Schaik et al. (2017) añade, que es poco probable que la

falta de conocimiento y precaución de los estudiantes desaparezcan cuando se incorporen de manera profesional a su área de trabajo.

Los riesgos informáticos a los que se exponen las personas de acuerdo con Gratian et al., (2018) se pueden considerar en cinco diferentes categorías: éticos, financieros, salud-seguridad, recreación y social. De los riesgos mencionados a los que más están expuestos los jóvenes estudiantes universitarios son a los riesgos éticos, de salud-seguridad, recreación, y social, ya que la mayoría de ellos no realizan operaciones financieras en línea.

Dentro de las habilidades que las empresas están solicitando en los especialistas del área de las tecnologías de la información se encuentran las relacionadas con la ciberseguridad, dentro de las que se mencionan: habilidad para mantener sistemas de información seguros y protegidos de intrusiones e intentos de robo de propiedad intelectual, neutralizar los *hackers, malware, virus, phishing,* y denegar servicios de ataque de dominio (Vogel, 2016). Esto lo pueden ver los estudiantes como una ventana de oportunidad para quienes piensen especializarse en el área de la seguridad informática, ya que de acuerdo con una encuesta realizada por la empresa Raytheon Technologies, se muestra un crecimiento de 3.5 veces más rápido para los especialistas del área de la ciberseguridad que el resto del mercado laboral de las TI, y un crecimiento 12 veces más rápido del total del mercado laboral (Vogel, 2016).

De acuerdo con el reporte *Cybersecurity Professionals Stand Up to a Pandemic Cybersecurity Workforce 2020* elaborado por la Asociación (ISC2, 2020), en ciberseguridad trabajan una amplia gama de profesionistas de diferentes edades y con diferentes niveles de educación. En dicho reporte mencionan que la mayoría de los profesionales que trabajan en esta área son hombres (77%). Del total de los que respondieron esa encuesta, la mayoría pertenecen a la generación Y (Millenials), ya que representan un 44%, le sigue la generación X con un 39%, posteriormente se encuentran los pertenecientes a la generación *boomers* con un 13%, y finalmente, empiezan a ingresar a esta área

los profesionistas de la generación Z, quienes representan solamente el 1% (ISC2, 2020); así mismo, en el estudio se menciona que los grados académicos que tiene la mayoría de los profesionistas del área son: licenciatura con un 41%, seguidos de los que poseen un grado de maestría, estos representan el 35%, en el nivel técnico se encuentran un 8%, y con un doctorado o postdoctorado un 3% de los profesionistas que trabajan en el área de la ciberseguridad. Lo anterior nos brinda un panorama actualizado del perfil de los profesionistas que se desempeñan en el área de la ciberseguridad.

Con el confinamiento por la COVID-19, personas de todas las edades se han visto en la necesidad de utilizar un mayor número de aplicaciones para realizar videollamadas, ya sea por cuestiones de trabajo, de estudio, para reuniones familiares o de amigos. Esto ha elevado el uso de los dispositivos electrónicos de comunicación, y con ello, la exposición a las amenazas cibernéticas mencionadas con anterioridad. En este sentido, las generaciones más afectadas fueron la Z y los Millenials (Y), ya que como suspendieron sus reuniones sociales y citas presenciales, tuvieron que adoptar novedosas formas tecnológicas de socialización, y como lo confirma Kaspersky Labs (2021), estos dos son los grupos de edad más propensos a incursionar en innovaciones y en tecnología.

Método.

Participantes.

Los participantes fueron estudiantes de la carrera universitaria de Licenciatura en Tecnologías de la Información de dos universidades públicas estatales de México, una del centro del país, la Universidad de Guadalajara (UdeG), Centro Universitario de Ciencias Económico-Administrativas (CUCEA), y otra del noreste mexicano, la Universidad Autónoma de Tamaulipas (UAT), Facultad de Comercio, Administración y Ciencias Sociales Nuevo Laredo (FCACS). Se contó con la participación de 62 alumnos de la universidad del centro y con 62 de la universidad del noreste. Los

alumnos son de los diferentes semestres que cursan la carrera a nivel licenciatura. Todos estaban inscritos en el semestre de primavera del año 2018 y fueron elegidos al azar.

Tabla 2. Estudiantes encuestados.

	Gen Y	Gen Z	Total
UAT	**31** *H=24, M= 7	**31** H= 16, M= 15	62
UdeG	**31** H= 22, M= 9	**31** H= 24, M= 7	62
Total	**62**	**62**	124

*H= Hombres M=Mujeres. Fuente: Elaboración propia.

Instrumento.

Para la recolección de datos, se utilizó el cuestionario que se muestra en la Tabla 3. Los reactivos se presentaron a los estudiantes con una escala de respuestas del 1 al 10, con excepción de las preguntas 14 y 15, que tuvieron una escala del 1 al 20. Este instrumento pasó por etapas de refinamiento, en donde intervinieron expertos de las áreas de seguridad informática y de educación. El cuestionario se ha aplicado previamente por los autores en otros estudios.

Tabla 3. Instrumento de recolección de datos.

ID	Pregunta
1	¿Qué tanto conoce de informática?
2	¿Qué tanto conoce sobre seguridad informática?
3	¿Qué tanto conoce sobre virus informáticos?
4	¿Qué tan probable es que usted instale en su computadora un programa que no es original?
5	¿Cuántas veces ha sido usted víctima de robo de identidad en los últimos doce meses?

6	¿Qué tanto le preocupa que su información pueda ser robada?
7	¿Cuántas películas en Internet ha visto en los últimos 30 días?
8	¿Cuántos respaldos de información personal ha realizado en los últimos 30 días?
9	¿Cuántas veces ha visitado una institución especializada en la protección de datos en los últimos 12 meses?
10	¿Cuántas veces ha utilizado los conocimientos de alguien especializado para que le asesore en el área de informática?
11	¿Cuántas cuentas activas de correo electrónico revisa usted diariamente?
12	¿Qué tan probable es que en una contraseña usted incluya fechas importantes como cumpleaños o aniversarios?
13	¿Qué tan probable es que usted comparta alguna contraseña con otra persona?
14	¿De cuántos caracteres en total es la contraseña de la cuenta de correo que usted más utiliza?
15	¿Cuántos caracteres especiales tiene la contraseña de la cuenta de correo electrónico que usted utiliza más?
16	¿Qué tan probable es que usted use la misma contraseña en dos o más páginas web?
17	¿Qué tan probable es que usted cambie la contraseña de su correo una vez al mes?
18	¿Qué tan respetuoso se considera de las reglas de los sistemas de información de su institución?

Fuente: Elaboración propia.

Análisis de datos.

El análisis de datos se realizó con el paquete estadístico Jamovi. Primero se obtuvieron los estadísticos descriptivos media y desviación estándar de los datos agrupados por generación, por institución, y por ambos factores. También se realizaron pruebas de Shapiro-Wilk, las cuales

indicaron que no existía distribución normal en las respuestas recabadas. Por esa razón, se decidió utilizar la prueba Schreirer-Ray-Hare, que es una alternativa para el Anova de dos vías. Con esta prueba no paramétrica se obtuvieron valores de significancia (P valores) para analizar el efecto de cada factor (generación e institución) y el efecto de ambos simultáneamente sobre las respuestas de los participantes. Se utilizó un 95% de confianza en todos los casos, por lo que se consideraron efectos estadísticamente significativos cuando se encontraron PValores inferiores a .05.

Resultados.

Los resultados de las pruebas Schreirer-Ray-Hare, que fueron estadísticamente significativos, se presentan en la Tabla 4.

Tabla 4. Principales resultados estadísticamente significativos.

Pregunta Número	**Redacción**	**Diferencia encontrada**	**Resultado de la prueba**	**Conclusión**	**Estadísticos Descriptivos**
1	¿Qué tanto conoce de informática?	Por generación	H=9.87, p=0.001	Gen Y conoce más que la Gen Z	Gen Y (m=7.79, ds=1.57 Gen Z (m=6.84, ds=1.80)
2	¿Qué tanto conoce sobre seguridad informática?	Interacción	H=4.59, p=0.032	Gen Y conoce más que la Gen Z	Gen Y (m=7.13, ds=1.69) Gen Z (m=6.00, ds=2.14)
3	¿Qué tanto conoce sobre virus informáticos?	Por Generación	H=6.86, p=0.008	Gen Y conoce más que la Gen Z	Gen Y (m=7.10, ds=2) Gen Z (m=6.08, ds=2.18)
3	¿Qué tanto conoce sobre virus informáticos?	Interacción	H=6.24 p=0.01	UAT Y puntuaciones más altas, UAT Z puntuaciones más bajas	UAT Y(m=7.45, ds=1.88) UAT Z(m=5.45, ds=2.13)
4	¿Qué tan probable es que usted instale en su computadora un programa que no es original?	Por generación	H=6.98 p=0.008	UAT Y puntuaciones más altas UAT Z puntuaciones más bajas	Gen Y (m=7.02, ds=2.91) Gen Z (m=6.02, ds=2.43)

5	¿Cuántas veces ha sido usted víctima de robo de identidad en los últimos doce meses?	Por Institución	H=7.27 p=0.006	UAT puntuaciones más altas UdeG puntuaciones más bajas.	UAT(m=0.871, ds=2.38) UdeG (m=.032, ds=0.178)
9	¿Cuántas veces ha visitado una institución especializada?	Por Generación	H=8.51 p=0.003	Gen Y visitó más instituciones que Gen Z	Gen Y (m=1.16, ds=2.35) Gen Z (m=0.339, ds=1.32)
13	¿Qué tan probable es que usted comparta alguna contraseña con otra persona?	Por Institución	H=6.02 p=0.014	UdeG puntuaciones más altas, UAT puntuaciones más bajas.	UAT(m=1.77, ds=2.38) UdeG (m=1.97, ds=1.62)

Fuente: Elaboración propia

Discusión.

En el presente estudio, se observó que la mayoría de los estudiantes de la generación Y tienen una autopercepción mayor sobre conocimientos de informática que los estudiantes de la generación Z; así mismo, con respecto a su conocimiento sobre seguridad informática, los encuestados de la generación Y reportaron un mayor conocimiento sobre este tema; probablemente porque estaban cursando semestres más avanzados.

Respecto a la pregunta de ¿Qué tan probable es que instalen programas que no son originales en sus computadoras?, los estudiantes de la generación Y mostraron mayor tendencia a instalar este tipo de programas que los estudiantes de la generación Z. Lo anterior lo podemos interpretar de la siguiente manera: la generación Y dice conocer más, pero también es la que tiene conductas más arriesgadas. Puede ser que se arriesguen más al *percibir* que conocen más, lo cual no implica necesariamente que conozcan más.

La Gen Y también reportó haber visitado más instituciones especializadas en ciberseguridad, seguramente porque fueron víctimas, lo cual puede ser consistente con que toman más riesgos. Resulta relevante que los estudiantes de la Universidad Autónoma de Tamaulipas (UAT) mencionaron haber sido más vulnerables en lo referente al robo de identidad, lo cual los muestra en desventaja ante los alumnos de la UdeG.

Finalmente, respecto a la pregunta de ¿qué tan probable es que compartan alguna de sus contraseñas?, los estudiantes de la UdeG mostraron un mayor riesgo que los de la UAT; sin embargo, fueron los alumnos de la UdeG quienes reportaron cambios en sus contraseñas más frecuentemente. Se coincide con (Johnson, 2019), en que al egresar los estudiantes universitarios tienen una base sólida respecto a la teoría; sin embargo, en muchos casos, no cuentan con las habilidades prácticas que el mercado laboral requiere. Tomando en cuenta a Wang et al., (2020), se sugiere agregar más contenidos prácticos a los programas educativos sobre diversos tópicos de ciberseguridad, enfocados a brindar las habilidades necesarias a los estudiantes para enfrentar los retos que se les presenten en su campo laboral en el mundo real. También se coincide con la Asociación ISC^2, en el sentido de que la mayoría de los estudiantes de esta carrera son del género masculino con un porcentaje bastante similar al obtenido en dicho estudio 70% hombres y 30% mujeres respectivamente.

Aunque la muestra realizada en esta investigación es pequeña para generalizar los resultados, estos proporcionan indicios que conviene estudiar con mayor profundidad en investigaciones posteriores.

CONCLUSIONES.

En este artículo se analizaron los principales hábitos y percepciones sobre seguridad informática entre los estudiantes de dos instituciones de educación superior en México, la Universidad Autónoma de Tamaulipas (Facultad de Comercio, Administración y Ciencias Sociales Nuevo Laredo) y la Universidad de Guadalajara (Centro Universitario de Ciencias Económico-Administrativas). Se concluye que los estudiantes de mayor edad (Generación Y) mencionan tener

un conocimiento superior que los estudiantes de la Generación Z, pero de igual forma se detectaron debilidades que dan oportunidad para una formación más sólida de estos estudiantes, quienes en el corto plazo estarán en el mercado laboral, y sus decisiones y acciones pueden afectar el desarrollo de la empresa.

Una de las principales aportaciones de este trabajo es que se lograron identificar áreas de oportunidad a partir del estudio de las percepciones y hábitos de los estudiantes de la carrera de Tecnologías de la Información sobre la seguridad informática. Se recomienda realizar talleres para capacitar y concientizar a los estudiantes sobre la importancia de la ciberseguridad. Por otro lado, se pueden realizar futuras investigaciones sobre esta misma línea, pero no solo con los estudiantes de la carrera de tecnología, sino también de las diferentes carreras administrativas que ofrecen estas instituciones.

REFERENCIAS BIBLIOGRÁFICAS.

1. Asociación de Internet Mx. (2021). Estudio de Ciberseguridad en empresas, usuarios de Internet y padres de familia en México. Asociación de Internet MX.
2. Baysal, S. (2014). Working with generations X and Y In generation Z period: Management of different generations in business life. Mediterranean Journal of Social Sciences, 5(19), 218–229. https://doi.org/10.5901/mjss.2014.v5n19p218
3. Betz, C. L. (2019). Generations X, Y, and Z. In Journal of Pediatric Nursing (Vol. 44, pp. A7–A8). W.B. Saunders. https://doi.org/10.1016/j.pedn.2018.12.013
4. Castaño, F., Sánchez-Paniagua, M., Delgado, J., Velazco-Mata, J., Sepúlveda, A., Fidalgo, E., & Alegre, E. (2021). Evaluation of state-of-art phishing detection strategies based on machine learning. In M. Serrano, E. Fernández-Medina, C. Alacaraz, N. de Castro, & G. Calvo (Eds.), Investigación en Ciberseguridad (Castilla-La Mancha). Ediciones de la Universidad De Castilla-La Mancha.

5. Dida, S., Hafiar, H., Kadiyono, A. L., & Lukman, S. (2021). Gender, education, and digital generations as determinants of attitudes toward health information for health workers in West Java, Indonesia. Heliyon, 7(1). https://doi.org/10.1016/j.heliyon.2021.e05916
6. Ferreiro, R. F. (2006). El reto de la educación en el siglo XXI: la generación N.
7. Galbusera, C. I. (2020). La evolución de los modelos de enseñar-aprender diseño en el nuevo escenario generacional. 78, 103–114.
8. Gartner.Com. (2021). Gartner Forecasts Global Devices Installed Base to Reach 6.2 Billion Units in 2021. https://www.gartner.com/en/newsroom/press-releases/2021-04-01-gartner-forecasts-global-devices-installed-base-to-reach-6-2-billion-units-in-2021
9. Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. Computers and Security, 73, 345–358. https://doi.org/10.1016/j.cose.2017.11.015
10. Instituto Economía Digital. (2017). Las 6 Generaciones de la Era Digital. https://cdn5.icemd.com/app/uploads/2018/12/Estudio_6-generaciones-de-la-era-digital-.pdf
11. ISC2. (2020). ISC2 2020 Global Information Securtity Workforce Study.
12. Jirí, B. (2016). The Employees of Baby Boomers Generation, Generation X, Generation Y and Generation Z in Selected Czech Corporations as Conceivers of Development and Competitiveness in their Corporation. Journal of Competitiveness, 8(4), 105–123. https://doi.org/10.7441/joc.2016.04.07
13. Johnson, C. (2019). University of South Wales national cyber security academy–creating cyber graduates who can ‘hit the ground running’: an innovative project based approach. Higher Education Pedagogies, 4(1), 300–303. https://doi.org/10.1080/23752696.2019.1605837

14. Kashif, M., Malik, S. A., Abdullah, T., Umair, M., & Khan, P. W. (2018). A Systematic Review of Cyber Security and Classification of Attacks in Networks. In IJACSA) International Journal of Advanced Computer Science and Applications (Vol. 9, Issue 6). www.ijacsa.thesai.org
15. Kaspersky Labs. (2021). Estableciendo una conexión: más del 80% de las personas se siente más sola ahora que antes de la pandemia | Kaspersky. https://latam.kaspersky.com/about/press-releases/2021_estableciendo-una-conexion-mas-del-80-de-las-personas-se-siente-mas-sola-ahora-que-antes-de-la-pandemia.
16. North, J., y Pascoe, R. (2016). Cyber security and resilience It's all about governance. Governance Directions, 68(3), 146–151.
17. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers and Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004
18. Roque, R., & Juárez, C. (2018). Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios. PAAKAT: Revista de Tecnología y Sociedad, 8(14), 5. https://doi.org/10.18381/pk.a8n14.318
19. Shahim, A. (2021). Security of the digital transformation. Computers & Security, 108, 102345. https://doi.org/10.1016/j.cose.2021.102345
20. van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. Computers in Human Behavior, 75, 547–559. https://doi.org/10.1016/j.chb.2017.05.038

21. Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as "the three R's." Heliyon, 5(12). https://doi.org/10.1016/j.heliyon.2019.e02855

22. Vogel, R. (2016). Closing the Cybersecurity Skills Gap. Salus Journal, 4(2), 32.

23. Wang, L., Yang, J., & Wan, P. J. (2020). Educational modules and research surveys on critical cybersecurity topics. In International Journal of Distributed Sensor Networks (Vol. 16, Issue 9). SAGE Publications Ltd. https://doi.org/10.1177/1550147720954678

DATOS DE LOS AUTORES.

1. **Adán López Mendoza**. Profesor-Investigador de tiempo completo en la Universidad Autónoma de Tamaulipas. Doctor en Educación Internacional. SNI Nivel 1. Correo electrónico: alopez@uat.edu.mx
2. **Ramón Ventura Roque Hernández**. Profesor-Investigador de tiempo completo en la Universidad Autónoma de Tamaulipas. Doctor en Ingeniería Telemática y Doctor en Educación. SNI Nivel 1. Correo electrónico: rvhernandez@uat.edu.mx
3. **Ma. Teresa Prieto Quezada.** Profesora-Investigadora en la Universidad de Guadalajara, Centro Universitarios de Ciencias Económico Administrativas. Doctora en Educación. SNI Nivel 2. Correo electrónico: materesaprieto@yahoo.com.mx
4. **Rolando Salazar Hernández.** Doctor en Informática, Profesor de la Facultad de Comercio, Administración y Ciencias Sociales de la Universidad Autónoma de Tamaulipas, Nuevo Laredo. Correo electrónico: rsalazar@docentes.uat.edu.mx

RECIBIDO: 6 de enero del 2022. **APROBADO:** 19 de marzo del 2022.