MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

ESTUDIO COMPARATIVO SOBRE PRIVACIDAD Y CONFIANZA EN REDES SOCIALES HORIZONTALES Y VERTICALES EN UNA INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por la estudiante:
Janneth Alexandra ROJAS BUSTOS

Bajo la dirección de:
Lohana Mariella LEMA MORETA

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
2019

Estudio comparativo sobre privacidad y confianza en redes sociales horizontales y verticales en una Institución de Educación Superior

Comparative study on privacy and trust in horizontal and vertical social networks in a Higher Education Institution

Janneth Alexandra ROJAS BUSTOS[1]
Lohana Mariella LEMA MORETA [2]

Resumen

En el presente artículo se realizó una comparación de las características de privacidad y confianza en los amigos en cuatro redes sociales; 2 horizontales y 2 verticales específicamente: Facebook, Twitter, Instagram y LinkedIn. Para cumplir con este fin, se revisó literatura relacionada a la temática que permitió diseñar un instrumento de medición – encuesta, la cual fue aplicada en una Institución de Educación Superior a una muestra de 222 personas entre 17 y 50 años. Los resultados indicaron que existen fronteras muy marcadas en cuanto a los comportamientos en privacidad y confianza en la red social horizontal Facebook con alto grado de uso y, en la red social vertical LinkedIn con bajo grado de uso; por lo que no se puede establecer comparación. No obstante, la red social horizontal Twitter y la red social vertical Instagram presentaron similitudes en los comportamientos de los usuarios. En conclusión, se demuestra que dependerá del uso de una red y la temática de la misma para que los niveles de privacidad y confianza en los amigos sean altos, así pues, en este caso la red vertical Instagram es la segunda preferida y por ende los usuarios protegen más la cuenta con la privacidad y se confía más tanto en la red como en sus amigos.

Palabras clave: | Redes sociales, privacidad, ingeniería social, confianza.

Abstract

In the present article, a comparison of privacy and trust characteristics in friends is made in four social networks; 2 horizontals and 2 verticals specifically: Facebook, Twitter, Instagram and LinkedIn. In order to fulfill this goal, literature related to the theme that allowed the design of a survey measurement instrument was reviewed, which was applied in a Higher Education Institution to a sample of 222 people between 17 and 50 years old. The results indicated that there are very marked borders in terms of behaviors in privacy and trust in the horizontal social network Facebook with high degree of use and, in the vertical social network LinkedIn with low degree of use; so no comparison can be made. However, the horizontal social network Twitter and the vertical social network Instagram showed similarities in user behavior. In conclusion, it is shown that it will depend on the use of a network and the theme of it so that the levels of privacy and trust in friends are high, so in this case the Instagram vertical network is the second preferred and therefore the users protect the account with more privacy and rely more on the network and on their friends.

Key words | Social networks, privacy, social engineering, trust.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo–Ecuador. E-mail jarojas@uees.edu.ec.
[2] Magíster en Ingeniería del Software. Docente de la Universidad Espíritu Santo- Ecuador. E-mail lohanalema@uees.edu.ec.

INTRODUCCIÓN

Durante la última década, con el rápido crecimiento de las tecnologías, las formas de interacción social y de comunicación entre las personas, se han modificado. Los encuentros personales, llamadas telefónicas o correos electrónicos, son medios que acortan las distancias y fortalecen vínculos, ya sea con amigos o la misma familia que se encuentra en lugares lejanos.

Un claro ejemplo de esto son las redes sociales y dispositivos móviles, que han revolucionado la interacción social, su uso en conjunto los convierte en un solo medio de comunicación (Podlaski, Hłobaż y Milczarski, 2015).

Así mismo, menciona Zhao y Zhao (2015) como el ámbito de las comunicaciones está cambiando gracias al auge de las redes sociales tales como Facebook, Twitter, Instagram, entre otras; permitiendo a las personas asumir un rol más activo en la sociedad tanto en actividades de carácter económicas, sociales o políticas.

Díaz Gandasegui (2011) expresa que las redes sociales reflejan la sociedad desde un punto de vista tecnológico, de un lado están los beneficios sociales de interacción entre personas, y del otro están los inconvenientes con la privacidad e información falsa que circula, este último es un grave problema pues la información es lo esencial en las redes sociales teniendo en cuenta que hoy por hoy la sociedad gira en torno al poder y control de obtener la misma.

En cuanto a las redes sociales, con los años surgieron sitios que, dependiendo de las temáticas, permiten a los usuarios agruparse en función de una comunidad social, ubicación, preferencias, y más (Ahn, Shehab y Squicciarini, 2011), de forma que, como lo expone Fernández, Chamorro, Gil y Somolinos (2012) las redes se pueden clasificar en redes horizontales dirigidas a todo tipo de usuario ejemplo: Facebook, Twitter; y redes verticales es decir tienen temáticas definidas enfocadas para usuarios con intereses comunes ejemplo LinkedIn una red de tipo profesional.

Por otra parte, consultando estadísticas sobre usuarios de redes sociales en el mundo coinciden Chaffey (2018) y Smith (2018) en el año 2018 se registran aproximadamente 3.196 mil millones de usuarios.

Del mismo modo Campo (2018) indica que a diario se conectan más de 3.000 millones de usuarios equivalente a un 42% de la población a nivel mundial, también señala que en España la media de tiempo que emplean en revisar sus redes sociales es de 58 minutos diarios e incluso los jóvenes sobrepasan esta media alcanzado la hora y 10 minutos.

Así también en Ecuador se encuentran estadísticas del estudio realizado por la empresa WeAreSocial y Hootsuite, como se aprecia en la Figura 1 los usuarios de internet llegan a 13,47 millones divididos en 4 redes sociales que son: Facebook, Twitter, LinkedIn e Instagram (Arboleda Acosta, 2018).

Figura 1. Redes sociales en Ecuador
Fuente: (Arboleda Acosta, 2018)

Además, Arboleda Acosta (2018) revela en la Figura 2 las cifras del perfil digital de nuestro país, donde cabe resaltar sobre todo los usuarios de redes sociales alcanzando un 66% de la población.

Figura 2. Perfil digital en Ecuador
Fuente: (Arboleda Acosta, 2018)

Con estos antecedentes, como se puede observar la población en todo el mundo utiliza las redes sociales, pero sin conocer cuál sea su propósito final y de ahí que, surge la pregunta; ¿las personas están conscientes del riesgo y amenazas a las que están expuestas?, por lo que la mayor problemática que nace alrededor de las redes sociales como lo dice Zhao y Zhao (2015) se centra en las amenazas a la privacidad y seguridad de las personas, empresas y gobiernos.

Además, se conoce que las personas no toman en consideración la gran cantidad de información que se recopilan en las redes sociales, por ello Patel y Joshi (2017) destacan que cualquier información personal como dirección, número de teléfono, ubicación, entre otros deben ser compartidos y vistos únicamente por personas en las que confía y no mantenerlo abierto a todos, ya que con la difusión rápida de la información esta puede ser vista por los amigos, pero al mismo tiempo se propaga a personas o usuarios no deseados (Dinh, Shen y Thai, 2012).

También, existen riesgos que dependiendo a que área afecten se los puede considerar: riesgos de privacidad, pues la red social no informa a los usuarios de los peligros que implica la publicación de su información personal; y riesgos de seguridad, pues se dan ataques de ingeniería social, phishing, virus, robo de identidad, entre otros (Ajami, Ramadan, Mohamed y Al-Jaroodi, 2011).

Así pues, Demidova, Shcherbakova y Vergelis (2018) revelan que en el primer trimestre de 2018 existieron ataques de phishing en las redes sociales sobre todo en Facebook llegando a un 60%. En cuanto a América del Sur, Brasil fue el país más atacado con un 19%, luego Argentina y Venezuela un 13% y Bolivia 12%.

Por consiguiente, ser prudente con la información en las redes sociales es importante debido a que, la mayoría de los usuarios desconoce los riesgos de privacidad que conlleva el almacenamiento de la información en los sitios de las redes sociales (Tootoonchian, Saroiu, Ganjali y Wolman, 2009). De ahí que, Guha, Tang y Francis (2008) señalan que grandes proveedores de redes sociales son las entidades sin rostro que controlan la nube almacenando los datos y que los usuarios para bien o para mal son simplemente los que generan la información.

Asimismo, cabe recordar que muchas veces se ha escuchado en medios de comunicación los problemas actuales en cuanto a los riesgos que se presentan en las redes sociales como son: desconocimiento sobre mecanismos de seguridad, uso indebido de los datos por externos, falta de escrúpulos de los usuarios y sobre todo la ingenuidad de algunas personas al confiar demasiado en la red social y por ende en sus contactos.

Sin embargo, como lo explica Wüest (2010) la mayoría de personas a más de tener pública su información, comparte enlaces y agrega a personas que no conoce a su red siendo blanco de ataques, en especial si los enlaces o contactos provienen de mensajes o recomendaciones de amigos a los que la cuenta ha sido intervenida.

Por lo cual, el factor confianza en los amigos (contactos) en las redes sociales como lo manifiesta Post y Walchi (2014) tiene dos aspectos importantes, el primero, los usuarios publican temas personales y, el segundo los contactos a más de ver esos temas publican algo relacionado o comparten el tema original. De forma que al tratar la confianza se quiere

conocer los alcances que tiene en el grupo de amigos y en la red que gira en torno a ellos.

Por otra parte, se destaca que los usuarios necesitan estar prevenidos y alertas para evitar convertirse en víctimas de ataques o engaños en las redes sociales, de forma que como lo proponen De y Imine (2017) se precisa concientizar a los usuarios en dos puntos principales, el primero entender los problemas en cuanto a la privacidad ocasionados por las acciones de compartir su información; y segundo establecer mecanismos para prevenir esos problemas.

El presente artículo tiene como objetivo analizar las diferencias que existen en los aspectos de privacidad y confianza en los amigos de redes sociales horizontales y verticales, específicamente en Facebook, Twitter, Instagram y LinkedIn.

Para conseguir el objetivo trazado se definió un enfoque cualitativo, primero se realizó una revisión bibliográfica con investigaciones relacionadas al tema para tener bases y construir una encuesta para aplicarla en la Institución de Educación Superior a la muestra que forman docentes, administrativos y estudiantes.

En el presente documento se encuentran cinco secciones: Introducción se detallan los antecedentes, problemática, justificación y objetivo; Marco teórico se explican los conceptos relevantes del tema; Metodología se presenta el enfoque y las fases para validar el instrumento; Análisis de resultados se desglosan las preguntas obteniendo las diferencias entre las redes sociales; y Conclusiones estableciendo el aporte, limitaciones y recomendaciones.

MARCO TEÓRICO

Redes sociales

Xiao, Bu, Hsu, Zhu y Shen (2017) definen a las redes sociales como sociedades virtuales en donde las personas se comunican y relacionan de forma similar como lo hacen en la vida real. De igual manera, Díaz Gandasegui (2011) indica que las redes sociales rompen con las barreras geográficas y sociales facilitando la interacción de las personas que tienen afinidad por algo en común creando una conexión de amistad en línea.

Como lo refiere Grabner-Kräuter y Bitter (2015) registrarse en una red social es fácil y gratis, tan solo se ingresa el nombre y correo electrónico, luego se completa el perfil con más información personal, fotos o videos. Una característica única de las redes sociales es que facilita la oportunidad de conocer gente nueva y además poder ver la red de amigos de esos usuarios.

En estos tiempos las noticias o cualquier tipo de información se trasmiten al instante por internet y se propagan aún más en las redes sociales, las personas comparten la información personal, sus intereses, buscan amistades anteriores o crean nuevas por lo cual se dice que la vida social está en línea (Patel y Joshi, 2017). Por otro lado, Grabner-Kräuter y Bitter (2015) señala que se tienen pruebas de varias redes sociales sobre como las personas comparten sin temor su información en espacios carentes de mecanismos y métodos de seguridad, además confían en los sitios de redes sociales para mantener su privacidad lo cual no estaría justificado.

Por otra parte, para Gross y Acquisti (2005) todas las redes sociales tienen el mismo propósito, comunicar e interactuar en línea, pero al mismo tiempo dependiendo de los intereses y preferencias se pueden agrupar en diferentes temáticas, siendo las principales las redes horizontales y las redes verticales. Las redes sociales horizontales son generales sin ninguna temática especial, tienen características semejantes como el perfil, compartir publicaciones y lo principal son los amigos o contactos (Ponce, 2012). En cambio, Navarro (2015) explica que las redes sociales verticales se distinguen por ser especializadas en un tema en específico, intercambiando aficiones y preferencias que tienen en común sus usuarios.

Por último en las redes sociales la finalidad es formar una red de amigos o contactos, sin embargo, como le dice Díaz Gandasegui (2011) dependiendo de la red social la concepción varía y por tanto el grado de confianza, por ejemplo, Facebook maneja a los miembros como amigos indicando que son conocidos; mientras tanto en Twitter son seguidores debido a que la mayoría de personas que se sigue son celebridades o personas con las que no se tiene ningún contacto en la vida real.

Conceptos de seguridad de la información

Concepto de privacidad

Zhang, Sun, Zhu y Fang (2010) explican que la privacidad es relevante en las redes sociales pues publicaciones ilegales o mal uso de la información privada pueden ocasionar perjuicios a las personas; además expone tres puntos que debe tener una red social: el primero anonimato de la identidad, el segundo privacidad del perfil del usuario y el tercero privacidad en su comunicación, es decir en mensajes y conexión.

Por otra parte, menciona Díaz Gandasegui (2011) que lo público y privado en las redes sociales no tiene diferencia debido a que los usuarios revelan información que antes se consideraba privada. De forma que, al utilizar las redes sociales los perfiles cargados de información personal, fotos, mensajes; se encuentran implícitas amenazas a la privacidad (Fernández, Chamorro, Gil y Somolinos, 2012).

Sin embargo, para Wüest (2010) la privacidad se puede controlar mediante las configuraciones que tiene cada red social, pudiendo restringir o habilitar según sea el grupo de amigos, conocidos o extraños. Es así que, en el trabajo de Li, Zhang y Das (2011) explican los riesgos de privacidad al exponer las relaciones de amistad brindando información que el atacante puede usar para conseguir los datos sensibles que le interesan.

Concepto de integridad

Al referirse a la Integridad en redes sociales De Luz (2014) y Cutillo, Molva y Strufe (2009) coinciden en sus apreciaciones manifestando que, existe integridad cuando se garantiza que la información sea modificada o manipulada únicamente por sujetos autorizados, no obstante, los usuarios de las redes sociales confían demasiado en la red misma, por lo tanto, surgen vulnerabilidades al no verificar la autenticidad de los miembros registrados.

Por otro lado, Zhang, Sun, Zhu y Fang (2010) comentan como en estudios previos se ha demostrado que las relaciones que se realizan en las redes sociales son las mismas que se tienen en la vida real, por consiguiente, si existiera alguna variación de ese modelo deberá ser detectado mediante mecanismos que aseguren la legitimidad del usuario en la red social.

Concepto de disponibilidad

En cuanto a la disponibilidad como su mismo nombre lo indica es cuando los recursos necesarios están siempre disponibles (De Luz, 2014), en este caso como lo indican Cutillo, Molva y Strufe (2009) al hablar de las redes sociales por lo general se las utiliza como medio para hacer negocios, diversión o enviar mensajes por lo que se necesita el servicio de forma ininterrumpida, pero además de esta disponibilidad las redes sociales requieren de herramientas para frenar bloqueos o censuras de nombres o palabras que ocasionen caídas del servicio.

Riesgos de privacidad

Robo de identidad

Desde la perspectiva de Patel y Joshi (2017) el robo de identidad es apropiarse de la información personal o identidad de otra persona y luego aparentar ser esa persona o usar la identidad para actos maliciosos, en las redes sociales los atacantes se ven atraídos por la gran cantidad de información disponible que pueden obtener. Es así que los ataques van desde crear perfiles falsos, transgredir la

imagen de la persona a la que se robó la identidad o también sacar provecho de personas famosas con calumnias (De Luz, 2014).

Asimismo, Zhang, Sun, Zhu y Fang (2010) tratan sobre los problemas que causa el robo de identidad, pero desde un enfoque que afecta a la red social en su reputación, por lo que se necesita tener legitimidad y autenticidad de las entidades de los miembros.

Suplantación de identidad (Phishing)

Acerca de la suplantación de identidad para Fernández, Chamorro, Gil y Somolinos (2012) es fácil hacerlo en las redes sociales pues los usuarios crean su perfil digital, de ahí que como no existen filtros de control se puede suplantar ese perfil a partir de una persona real. Esto afecta gravemente a la privacidad del usuario perjudicado; no obstante, los proveedores de redes sociales trabajan en mecanismos que ayuden a reducir estos ataques.

Clonación de perfil

Tal como lo explica Patel y Joshi (2017) este método de clonar perfiles es robar la identidad para luego introducirse en la red de amigos, pues los usuarios aceptan sus solicitudes sin darse cuenta que se trata de uno falso. Así también como lo enuncia Cutillo, Molva y Strufe (2009) tan solo clonando el perfil y enviando nuevas solicitudes es suficiente para establecer relaciones con los miembros de la lista de amigos valiéndose de la confianza que se tiene en el círculo de la red social.

Ingeniería social

Al hablar de ingeniería social la guía de seguridad de Eset (2013) lo explica como una forma de manipular a las personas con la finalidad de realizar varios ataques como infecciones con malware, estafas, robo de datos, grooming, entre otros.

Asimismo, Borbón Sanabria (2012) compara la ingeniería social como un hacking humano de ahí que lo primero es recolectar información para formar un perfil valiéndose de todos los contenidos publicados en la red social. Además, Algarni, Xu y Chan (2017) señala lo difícil que es reconocer engaños en las redes sociales, por ejemplo, en Facebook se utiliza etiquetas, aplicaciones de juegos o persuasión por chat, solo por mencionar algunos.

Confianza en las redes sociales

A propósito de la confianza varias investigaciones demuestran que los usuarios son el eslabón débil en cuanto a la seguridad en las redes sociales debido a que no miden las consecuencias de sus acciones que parecen simples como aceptar una solicitud de amistad o etiquetar una foto; por esta razón, a pesar de los controles de privacidad que tienen las redes sociales, la confianza inherente que los usuarios tiene en otros perfiles agudizan el problema (Cutillo, Molva y Strufe, 2009).

Por otro lado, Claybaugh y Haseman (2013) manifiestan que se puede evaluar comportamientos de confianza mediante las interacciones en línea, también señala los riesgos de la confianza, a nivel de toda la red cuando se expone la información personal a extraños y el riesgo individual cuando una persona utiliza esa confianza para su propio beneficio. Es decir, como lo precisa Grabner-Kräuter y Bitter (2015) la confianza se puede establecer a nivel macro que abarca toda la red social (proveedor) y a nivel micro que forman los grupos o amigos (contactos) que tiene cada usuario.

TRABAJOS PREVIOS

Se evidencia la existencia de literatura sobre redes sociales desde diferentes enfoques y áreas.

Toranzo (2013) lleva a cabo una investigación con un grupo de jóvenes realizando encuestas para determinar una comparación en la toma de riesgos, confianza, información y actitud privada en las redes sociales en general. Los resultados obtenidos reportan una gran cantidad de perfiles

abiertos y accesibles; concluyendo que la difusión de esta información ayudará a prevenir riesgos que implica el uso de las redes sociales.

Por otra parte Cutillo, Molva y Strufe (2009) en su artículo propone una perspectiva nueva para afrontar los problemas de seguridad y privacidad orientado especialmente a la privacidad en relación con el proveedor de la red social y también de la protección contra extraños o usuarios con malas intenciones, se aplicaron dos enfoques el primero basado en una arquitectura descentralizada del proveedor y el segundo reforzar las relaciones de confianza dando como resultado Safebook. Este prototipo presenta un equilibrio entre privacidad y rendimiento, no obstante, mientras mayores sean los saltos entre enlaces confiables mejora la privacidad, pero genera retrasos de búsqueda y comunicación.

Así mismo continuando con la confianza Post y Walchi (2014) presentan un modelo basado en la privacidad y confianza en los contactos, los autores realizan una prueba aplicando encuestas a grupos. El objetivo es conocer como estas variables impactan el uso de las redes sociales. Los resultados demuestran que las actitudes hacia las redes se ven afectadas por las necesidades individuales de privacidad y por la confianza en los amigos, incidiendo directamente en el índice de uso de las mismas

Tomando como antecedente los trabajos expuestos no resulta extraño que las investigaciones se orienten a realizar comparaciones entre redes sociales específicas. En el artículo de Dwyer, Hiltz, y Passerini (2007) se comparan Facebook y MySpace mediante la aplicación de una encuesta en línea con respecto a parámetros como, la confianza y privacidad, unidos a la facilidad de compartir información y entablar relaciones nuevas. Los resultados muestran que en Facebook tienen mayor confianza en la red y comparten información sensible más abiertamente, en tanto que en MySpace lo utilizan para conocer gente. De ahí se concluye que, en las relaciones en línea, no se necesita confianza como en las relaciones reales, incluso en sitios donde las garantías de confianza y privacidad son débiles.

De igual manera Chang, Liu y Shen (2017) realiza una comparación entre Facebook y LinkedIn con la finalidad de conocer los factores que influyen en la confianza de los usuarios, mediante un estudio empírico con encuestas donde se incluyen constructos como la expectativa de esfuerzo, la influencia social, la preocupación por la privacidad, el riesgo percibido, la confianza y la intención de continuidad. Los resultados alcanzados indican que el riesgo percibido afecta de forma negativa la confianza; así mismo la preocupación por la privacidad intervino de forma positiva en el riesgo percibido; y se demostró que la confianza contribuye de manera directa en la intención de continuidad en la red, estos elementos influyentes son diferentes entre los usuarios de las dos redes sociales.

METODOLOGÍA.

El enfoque del presente artículo es de tipo Cualitativo pues se realizó encuestas que reflejan el comportamiento de los participantes en cuanto a privacidad, uso y confianza en los amigos en las cuatro redes sociales seleccionadas. Mientras el alcance es de tipo Descriptivo pues el objetivo es determinar los niveles de privacidad y confianza en los contactos (amigos) en cada red social para poder establecer diferencias.

Por otro lado, el desarrollo de la investigación se planteó en cuatro fases:

1. Diseño de la encuesta
2. Validación del instrumento
3. Publicación de la encuesta
4. Presentación de resultados

Para la aplicación de la encuesta la población considerada es de una Institución de Educación Superior conformada por estudiantes, profesores y administrativos siendo hombres y mujeres en un rango de edad de 17 a 50 años, dando en total 1200 personas. Se procede a

realizar el cálculo para determinar la muestra con un resultado de 222 personas.

ANÁLISIS DE RESULTADOS

1. Diseño de la encuesta

Se inicia esta exploratoria desarrollando una encuesta que se construyó luego de la revisión bibliográfica donde se evidenciaba la problemática de seguridad en las redes sociales, además de incluir preguntas que recabaran información acerca de los aspectos que deberían conocer todas las personas que las utilizan, hábitos de privacidad en sus cuentas, el grado de concientización al momento de aceptar amigos tanto conocidos como desconocidos y las consecuencias de la divulgación de información personal. Finalmente se plantearon preguntas que permitan averiguar los motivos de uso de las redes sociales y el grado de confianza que tienen en las mismas.

La encuesta, compuesta de 37 preguntas fue categorizada en tres secciones: aspecto demográfico, aspecto de seguridad de las cuentas y aspecto del uso y manejo de las cuentas; cada pregunta presenta múltiples opciones construidas aplicando la escala de Likert, la cual como lo señala el sitio de QuestionPro (2018) la escala se utiliza para poder medir en diferentes niveles por lo general tiene 5, 7 o 9 elementos; va desde totalmente de acuerdo a un totalmente desacuerdo. El instrumento fue diseñado y distribuido mediante la plataforma Google Forms.

2. Validación del Instrumento

La primera prueba de validación que se llevó a cabo de la encuesta fue el 23 de marzo de 2018 mediante la técnica del Grupo de Enfoque como lo indica Bonilla-Jimenez y Escobar (2017) ésta sirve para conocer el comportamiento de los participantes ante distintas ideas, servicios o productos.

El objetivo de este grupo focal era el de evaluar el correcto entendimiento de los cuestionamientos planteados, la correcta selección de las escalas y la consistencia de la relación entre preguntas. Para cumplir este fin, se seleccionó un grupo de 10 personas: 6 mujeres y 4 hombres, distribuidos de acuerdo a las características de la muestra en 3 profesores, 2 administrativos y 5 estudiantes. Una vez concluido el grupo focal, el instrumento fue ajustado de acuerdo a las sugerencias y observaciones realizadas durante el proceso.

Una segunda ronda de validación inició una vez se disponibilizó un enlace del instrumento vía WhatsApp, desde el 6 de agosto de 2018 hasta el 24 de agosto de 2018. Durante este periodo, 40 personas atendieron la encuesta, lo cual permitió medir de manera preliminar que tanto las preguntas como las respuestas están ajustadas a los objetivos de este trabajo. Finalmente, el instrumento es ajustado en forma y orden.

3. Publicación de la encuesta

Una vez realizadas las validaciones correspondientes al instrumento, el enlace con la versión final del mismo fue habilitado desde el 4 de octubre de 2018 hasta el 23 de noviembre de 2018 detallando los resultados en la siguiente fase.

4. Presentación de resultados

La encuesta la realizaron 222 personas para el análisis se agrupará las preguntas que tienen relación.

En cuanto al género de los participantes la mayoría son mujeres: 127 dando un 58%, equivalente a más de la mitad; así mismo el rango de edad que predomina es de 18 a 25 años con un resultado de 119 personas correspondiente a 54%, luego está el rango de 25 a 35 años con 74 participantes obteniendo un 33%.

Las preguntas que se detallan a continuación midieron aspectos generales de la población que se encuestó, donde se muestra que el 99% utiliza internet todos los días y de ellos un 96% también utiliza las redes sociales a diario.

De ahí que, al consultar sobre los términos, condiciones de la red y los acuerdos de privacidad de las cuentas en las preguntas 6, 7 y 8 el resultado es contradictorio puesto que la mayoría: 82%, No lee los términos y condiciones, sin embargo, están De acuerdo con el contrato de privacidad de la red alcanzando un 45% y un 24% Totalmente de acuerdo; además la mitad de los encuestados 50% está Totalmente de acuerdo y un 41% De acuerdo, opinando que el acuerdo de privacidad es importante en las redes sociales.

En lo referente a la importancia que tienen las notificaciones de la red social los participantes revelan que en Facebook con 51% les interesa mucho más revisarlas, luego está Instagram con 36%; para Twitter y LinkedIn expresan que no tienen tanto interés en ver las notificaciones o incluso en LinkedIn no tienen cuenta. Por lo que tiene concordancia al preguntar sobre si utiliza grupos en las redes sociales la mayoría con un 95% indico que en Facebook es donde más lo aplica.

Al consultar si disfruta utilizando las redes sociales en la pregunta 21 un 62% de los participantes está De acuerdo y un 27% está Totalmente de acuerdo significando que les gusta estar en las redes, no obstante, cuando se pregunta si las redes sociales son importantes en su vida señalan que únicamente Facebook.

Sobre la conciencia del peligro que pueden traer las redes sociales se planteó las preguntas 28, 29 y 30, el resultado fue que los participantes en su mayoría más del 70% están conscientes que las redes sociales pueden traer consecuencias negativas, poniendo en peligro a familiares o amigos y además la información puede ser utilizada por criminales, aunque una pequeña fracción 17% opina lo contrario.

Las siguientes preguntas expresan el comportamiento de los participantes en cada red social; así como se observa en la tabla 1 se obtuvo que Facebook con 86% es la que más frecuentemente usan pues es la más conocida, luego esta Instagram como la que frecuentemente usan con un 39%; esta información se recaba en la pregunta 5.

Tabla 1: Preferencia de las redes sociales

	Red social	Frecuencia
1	Facebook	Muy frecuentemente uso 86%
2	Instagram	Frecuentemente uso 39%
3	Twitter	Ocasionalmente uso 29%
4	LinkedIn	Raramente uso 20%

Fuente: (Elaboración propia, 2018)

En la pregunta 9 sobre las seguridades básicas en las redes como se aprecia en la tabla 2 sobresale Facebook con un 39% indicando que sus usuarios conocen y aplican las dos reglas principales, luego esta Instagram con 31% revelando que al menos una regla la aplican, Twitter consta con 17% al aplicar una regla, pero así mismo se observa que gran parte de los participantes No aplican ninguna regla.

Tabla 2: Diferencias de seguridad

Red social	No	Al menos una	Si
Facebook	25%	49%	39%
Twitter	61%	17%	6%
Instagram	46%	31%	8%
LinkedIn	61%	1%	4%

Fuente: (Elaboración propia, 2018)

En cuanto al uso de controles de privacidad para limitar quien puede ver la cuenta en la pregunta 10, en la tabla 3 se evidencia que en Facebook se preocupan más en cuanto a la privacidad con un porcentaje del 62% los cuales Frecuentemente protegen sus cuentas, en cambio Twitter y LinkedIn no prestan atención a la privacidad.

Tabla 3: Diferencias de privacidad

Red social	Frecuentemente	Nunca
Facebook	62%	5%
Twitter	17%	58%
Instagram	27%	39%
LinkedIn	3%	55%

Fuente: (Elaboración propia, 2018)

En lo que se refiere a la pregunta 11 sobre el nivel de privacidad activado en la red social Facebook es el más alto con un 60% en el nivel 3, en tanto que Instagram alcanza un 32% en el nivel 2, quedando Twitter y LinkedIn en último como se detalla en la tabla 4, pues más de la mitad de los participantes indican que no tienen activado filtros de seguridad.

Tabla 4: Nivel de privacidad

Red social	Nivel (1 menor, 4 alto)
Facebook	Nivel 3 60%
Twitter	Nivel 1 56%
Instagram	Nivel 2 32%
LinkedIn	Nivel 1 55%.

Fuente: (Elaboración propia, 2018)

Al consultar en la pregunta 12 si conoce si los amigos por lo general utilizan controles de privacidad cuando publican información sobre usted, la respuesta contenida en la tabla 5 que tiene mayor porcentaje más del 40% es Desconozco, no sé si los usa; aunque en Facebook manifiestan que Regularmente con un 36% a los amigos si les preocupa la privacidad.

Tabla 5: Utilización de controles

Red social	Desconozco, no sé si los usa	Opción
Facebook	45%	Regularmente 36%
Twitter	42%	Nunca 36%
Instagram	45%	Nunca 29%
LinkedIn	31%	No uso la red 39%

Fuente: (Elaboración propia, 2018)

Mientras que en la pregunta 13 Le preocupa sobre las fotos o comentarios que lo exponen públicamente, en todas las redes se evidencia que los participantes están conscientes de que la información pública puede traer consecuencias negativas, puesto que las opciones De acuerdo y Totalmente de acuerdo tienen los mayores porcentajes, aunque cabe destacar que también existe un pequeño porcentaje que están En desacuerdo lo cual se interpreta que estas personas no se sienten en peligro, se especifica en la tabla 6.

Tabla 6: Diferencias en exposición pública

Red social	En desacuerdo	De acuerdo	Totalmente de acuerdo
Facebook	16%	42%	39%
Twitter	13%	36%	28%
Instagram	16%	39%	25%
LinkedIn	10%	25%	24%

Fuente: (Elaboración propia, 2018)

Por otro lado, se mide el nivel de confianza en las redes sociales con respecto a la protección de la información en la pregunta 14, como se puede apreciar en la tabla 7 los participantes tienen la confianza entre 60%-90% en Facebook alcanzando un 66%, luego Instagram con un 50%; en cambio Twitter la confianza es entre 30%-60% de más de la mitad de los participantes obteniendo un 57%, en el caso de LinkedIn la confianza no es tan grande.

Tabla 7: Diferencias de confianza

Red social	30%-60%	60%-90%
Facebook	28%	66%
Twitter	57%	21%
Instagram	31%	50%
LinkedIn	21%	38%

Fuente: (Elaboración propia, 2018)

Al pedir que se ordene las redes desde la más segura a la menos segura, consideran a Facebook la más segura en el Nivel 4 con 30%, seguida Instagram en el Nivel 3 con 46%, en tanto que Twitter y LinkedIn están en el Nivel 2, la información se aprecia en la tabla 8 correspondiendo a la pregunta 15.

Tabla 8: Ordenación de las redes

	Red social	Nivel (1 menos, 5 más)
1	Facebook	Nivel 4 30%
2	Instagram	Nivel 3 46%
3	Twitter	Nivel 2 52%
4	LinkedIn	Nivel 2 30%.

Fuente: (Elaboración propia, 2018)

Por otra parte, en la pregunta 18 si pide a los amigos que elimine publicaciones, como se visualiza en la tabla 9 en Facebook la opción No tantas veces con 46% es la mayor en cambio en Twitter y LinkedIn la opción Nunca sobrepasa el 50%.

Tabla 9: Eliminar publicaciones

Red social	Nunca	No tantas veces
Facebook	17%	46%
Twitter	68%	9%
Instagram	40%	37%
LinkedIn	61%	2%

Fuente: (Elaboración propia, 2018)

Se expone en la tabla 10 el resultado de la pregunta 19 obteniendo que en Facebook con 59% La mayoría de veces comparten la información con amigos, pero no con la familia sugiriendo que tienen más confianza en los amigos, no así en las otras redes.

Tabla 10: Diferencias de compartir información

Red social	Nunca	No tantas veces	A veces	La mayoría de veces
Facebook	5%	9%	25%	59%
Twitter	53%	9%	10%	8%
Instagram	21%	23%	21%	18%
LinkedIn	56%	4%	2%	0%

Fuente: (Elaboración propia, 2018)

Asimismo, en la pregunta 20 con qué frecuencia se arrepiente de las publicaciones el resultado es similar al obtenido en la tabla 9, la opción No tantas veces 69% es la mayor en Facebook, en tanto que en Instagram Nunca 40% y No tantas veces 39% casi son iguales; no así en Twitter y LinkedIn donde Nunca es la mayor, sobrepasa el 50%.

En lo referente a los contactos o amigos que tienen en las redes sociales se formuló las preguntas 23, 24, 25 y 26 para tener una idea del número de miembros de la familia, amigos, conocidos y desconocidos que se acepta en las redes obteniendo los siguientes resultados como lo muestra la tabla 11. En Facebook los contactos que son familia es superior pues tienen de 10 a 30 en un 45%; en Instagram y Facebook los amigos pasan de 50 pero asimismo en Facebook en mayor porcentaje 72%; con los conocidos tanto en Instagram, Twitter y Facebook se cuenta con más de 50 contactos y nuevamente en Facebook es mayor con 77%; por último con los desconocidos en Twitter e Instagram se tiene de 50 en adelante más del 40%, no así en Facebook que se tiene de 30 a 50 en un 51%, en tanto que en LinkedIn esta de 0-10 en un 40%.

Tabla 11: Diferencias de contactos

Red social	Familia	Amigos	Conocidos	Desconocidos
Facebook	10-30 45%	50 en adelante 72%	50 en adelante 77%	30-50 51%
Twitter	0-10 73%	10-30 38%	50 en adelante 39%	50 en adelante 47%
Instagram	0-10 69%	50 en adelante 31%	50 en adelante 54%	50 en adelante 59%
LinkedIn	0-10 54%	0-10 26%	0-10 22%	0-10 40%

Fuente: (Elaboración propia, 2018)

Con respecto a la pregunta 27 sobre la frecuencia con la que actualiza la información a la semana tanto Facebook con un 75% Muy frecuentemente como Instagram con un 38% Frecuentemente, son las redes donde más actividad se registra, se detalla en la tabla 12.

Tabla 12: Diferencias de frecuencia

Red social	Frecuencia
Facebook	Muy frecuentemente 75%
Twitter	Nunca 39%
Instagram	Frecuentemente 38%
LinkedIn	Nunca 41%

Fuente: (Elaboración propia, 2018)

En la pregunta 31 se consulta si acepta desconocidos en las redes, observando la tabla

13 sobresale que en Twitter e Instagram la opción 50%-80% de las veces tiene un 48% mientras que el 100% de las veces en las mismas redes es más del 10% aunque es bajo, pero a pesar del riesgo que esto implica si lo hacen.

Tabla 13: Diferencias de aceptar desconocidos

Red social	20%-40% de las veces	50%-80% de las veces	100% de las veces
Facebook	68%	22%	2%
Twitter	15%	48%	13%
Instagram	15%	48%	17%
LinkedIn	37%	2%	0%

Fuente: (Elaboración propia, 2018)

Para conocer el grado de confianza que brindan los usuarios de las redes sociales a los amigos o contactos se realizaron las preguntas 32, 33, 34 y 35. Como se puede diferenciar en la tabla 14 la mayoría de los participantes confía en sus contactos y acepta relacionarse e incluso encuentros personales con gente que no conoce sin medir el peligro que esto representa. Así pues, se destaca que en Facebook con un 51% aceptan encuentros entre 50-80% si un amigo da una referencia; no así en el caso de encuentros personales con desconocidos Facebook, Twitter e Instagram aceptan en más del 50% la posibilidad de un 20-40%; lo mismo ocurre con los encuentros personales con un amigo del amigo.

Tabla 14: Diferencias en confianza en los amigos

Red social	Pide publicación el amigo del amigo	Referencia para un encuentro	Encuentro personal con desconocido	Encuentro personal con amigo del amigo
Facebook	De acuerdo 81%	50-80% de las veces 51%	20-40% de las veces 64%	20-40% de las veces 64%
Twitter	De acuerdo 57%	20-40% de las veces 51%	20-40% de las veces 52%	20-40% de las veces 53%
Instagram	De acuerdo 64%	50-80% de las veces 37%	20-40% de las veces 56%	20-40% de las veces 55%
LinkedIn	De acuerdo 35%	20-40% de las veces 33%	20-40% de las veces 32%	20-40% de las veces 29%

Fuente: (Elaboración propia, 2018)

En la pregunta 36 sobre las razones se observa en la tabla 15 las razones principales son entretenimiento con un 78%, y estar en contacto con amigos y conocidos un 67%

En cuanto a las razones para utilizar las redes sociales las principales son: Entretenimiento con un 78% Totalmente de acuerdo, y Estar en contacto con amigos y conocidos un 67% Totalmente de acuerdo, lo cual demuestra que las redes sociales son tomadas como esparcimiento y medio de comunicación, esta información viene de la pregunta 36 y se detallan todas en la tabla 15.

Tabla 15: Razones para utilizar las redes sociales

Razones	
Entretenimiento	78% Totalmente de acuerdo
Estar en contacto con amigos y conocidos	67% Totalmente de acuerdo
Hacer amigos nuevos	58% De acuerdo
Encontrar pareja	54% De acuerdo
Intereses profesionales	64% De acuerdo
No quedarse rezagado	62% En desacuerdo

Fuente: (Elaboración propia, 2018)

Para terminar, en la pregunta 37 los motivos para publicar en las redes sociales, llama la atención que la opción Alguien me lo pide tenga un porcentaje que sobrepasa la mitad de los participantes 58% que están de acuerdo, dejando ver que se puede influenciar en el

comportamiento de las personas tanto a que publiquen información personal o propague alguna información que tenga fines maliciosos, los demás datos se desglosan en la tabla 16.

Tabla 16: Motivos para publicar en las redes sociales

Motivación	
Pienso que es interesante o divertido	72% Totalmente de acuerdo
Expresa mi manera de ser	58% De acuerdo
Alguien me lo pide	59% De acuerdo
Un amigo publica algo similar o sobre un tema relacionado	56% De acuerdo
Con un propósito específico para persuadir a alguien u obtener información	61% En desacuerdo
Estoy interesado en escuchar lo que otros piensan al respecto	49% En desacuerdo

Fuente: (Elaboración propia, 2018)

CONCLUSIONES

En este artículo se analizó las redes sociales clasificadas en redes horizontales y redes verticales, realizando un estudio cualitativo basado en encuesta, a fin de establecer una comparación entre sus características de privacidad y confianza.

De ahí que del análisis de resultados se obtiene que la red horizontal Facebook y la red vertical LinkedIn marcan las fronteras de la muestra analizada una con un alto grado de uso ratificando que es la red más popular, por ende, la privacidad es mayor, así como la confianza en la red misma como en sus amigos; y otra con bajo grado de uso pues así tengan cuenta no la utilizan resultando niveles bajos tanto en privacidad como en confianza. Es importante puntualizar que la edad de la muestra que realizó la encuesta, jóvenes de 18 a 25 años, no contemplan el uso de una red social laboral como primordial.

Por lo tanto, se concluye que entre Facebook y LinkedIn no se puede establecer una comparación de las características de privacidad y confianza ya que son fronteras muy marcadas dejando en claro las preferencias y comportamientos en ambos aspectos, no obstante, Twitter e Instagram presentan similitudes en el comportamiento de sus usuarios y además cumplen la premisa de ser una red social horizontal y vertical respectivamente.

En lo referente a la privacidad la red social vertical Instagram es la que brinda mayores opciones de configuración de diferentes reglas de seguridad y controles, considerando que su nivel de privacidad es más alto en contra parte con la red horizontal Twitter.
Por otro lado al tratar sobre la confianza en los amigos la red vertical que destaca en este aspecto vuelve a ser Instagram debido a que la consideran en un nivel 3 de seguridad sobre 5, así también expresan que confían más en sus amigos o contactos cuando se trata de interactuar con personas que no conocen pero aceptan conversaciones y encuentros al existir ese lazo en común, así mismo a mayor confianza en los amigos acepta las publicaciones y no pide eliminarlas; mientras que en la horizontal Twitter se evidencia un grado más bajo de confianza indicando que aunque los amigos den referencias de personas desconocidas la probabilidad de aceptar el encuentro es baja.

De manera que, el grado de uso de la red y la temática están estrechamente ligados con la privacidad y el grado de confianza pues la red vertical Instagram resultó ser la que más privacidad tiene activada y en la que más confianza tiene en los amigos, esto se debe a que es la segunda red más usada y al ser la muestra mayoritariamente de jóvenes la encuentran atractiva ya sea por su temática visual que les permite mostrarse públicamente exponiendo información con fotos de maneras graciosas o idealizadas mediante los filtros, entrar en contacto con gente famosa que a la final es desconocida pero como confían en la red igual interactúan mediante etiquetas para tener mayor visibilidad y seguidores.

Las limitaciones del artículo se presentaron en el rango de edad de la muestra pues la mayoría resulto ser entre 18 y 25 años lo cual propició que de la información recabada resulten extremos orillando a realizar las diferencias únicamente entre 2 redes sociales de las 4 planteadas desde el inicio. Así también no se explicó a los participantes conceptos de seguridad o riesgos de privacidad por lo que los resultados son en base a su conocimiento y comportamiento en las redes.

Para el futuro se recomienda aplicar el instrumento ya sea en la misma Institución de Educación Superior o en otra, pero esta vez tomando como población a estudiantes de post grado de tal manera que se podría contrastar los resultados pues variarán los rangos de edad, así como la situación económica y laboral.

Referencias Bibliográficas

Ahn, G. J., Shehab, M., & Squicciarini, A. (2011). Security and privacy in social networks. *IEEE Internet Computing, 15(3)*, 10-12.

Ajami, R., Ramadan, N., Mohamed, N., & Al-Jaroodi, J. (2011). Security challenges and approaches in online social networks: A survey. *IJCSNS, 11(8)*.

Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. *European Journal of Information Systems, 26(6)*, 661-687.

Arboleda Acosta, M. (2018). *Estadísticas digitales Ecuador 2018*. Retrieved from http://www.hablemosdemarcas.com/estadisticas-digitales-ecuador-2018/

Bonilla-Jimenez, F. I., & Escobar, J. (2017). Grupos focales: una guía conceptual y metodológica.

Borbón Sanabria, J. S. (2012). REDES SOCIALES, ENTRE LA INGENIERÍA SOCIAL Y LOS RIESGOS A LA PRIVACIDAD. *Revista Seguridad*.

Campo, A. M. (2018). *Las Redes Sociales más utilizadas: cifras y estadísticas*. Retrieved from https://www.iebschool.com/blog/medios-sociales-mas-utilizadas-redes-sociales/

Chaffey, D. (2018). *Global social media research summary 2018*. Retrieved from https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/

Chang, S. E., Liu, A. Y., & Shen, W. C. (2017). User trust in social networking services: A comparison of Facebook and LinkedIn. *Computers in Human Behavior, 69*, 207-217.

Claybaugh, C. C., & Haseman, W. D. (2013). Understanding professional connections in LINKEDIN—a question of trust. *Journal of Computer Information Systems, 54(1)*, 94-105.

Cutillo, L. A., Molva, R., & Strufe, T. (2009). Safebook: A privacy-preserving online social network leveraging on real-life trust. *IEEE Communications Magazine, 47(12)*, 94-101.

De Luz, S. (2014). Privacidad y Seguridad en las Redes Sociales.

De, S. J., & Imine, A. (2017). Privacy Scoring of Social Network User Profiles through Risk Analysis. *In International Conference on Risks and Security of Internet and Systems* , pp. 227-243.

Demidova, N., Shcherbakova, T. y Vergelis. M. (2018). *Spam and phishing in Q1 2018* . Retrieved from https://securelist.com/spam-and-phishing-in-q1-2018/85650/

Díaz Gandasegui, V. (2011). Mitos y realidades de las redes sociales. Información y comunicación en la Sociedad de la Información. *Prisma social*, (6), 1-26.

Dinh, T. N., Shen, Y., & Thai, M. T. (2012). The walls have ears: optimize sharing for visibility and privacy in online social networks. *Information and knowledge management*, (pp. 1452-1461).

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace.

Eset. (2013). *Guía de seguridad en redes sociales*. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2013/11/guia-redes-sociales-eset.pdf

Fernández, J. R., Chamorro, E. F., Gil, R. H., & Somolinos, J. A. (2012). Evaluación de la privacidad de una red social virtual. *RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação, (9)*, 59-73.

Grabner-Kräuter, S., & Bitter, S. (2015). Trust in online social networks: A multifaceted perspective. *In Forum for social economics Vol. 44, No. 1*, pp. 48-68.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *In Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pp. 71-80.

Guha, S., Tang, K., & Francis, P. (2008). NOYB: Privacy in online social networks. *In Proceedings of the first workshop on Online social networks* , pp. 49-54.

Li, N., Zhang, N., & Das, S. (2011). Preserving relation privacy in online social network data. *IEEE internet computing, 15(3)*, 35-42.

Navarro, I. (2015). *Tipos de redes sociales: ¿cómo clasificarlas?* Retrieved from https://www.deustoformacion.com/blog/redes-sociales/tipos-redes-sociales

Patel, R. B. R. M. P., & Joshi, M. H. (2017). Privacy and Security Issues in Social Online Networks.

Podlaski, K., Hłobaż, A., & Milczarski, P. (2015). New Method for Public Key Distribution Based on Social Networks.

Ponce, I. (2012). *MONOGRÁFICO: Redes Sociales-Clasificación de redes sociales.* Retrieved from http://recursostic.educacion.es/observatorio/web/es/internet/web-20/1043-redes-sociales?start=3

Post, G. V., & Walchli, S. B. (2014). Social network privacy: Trusting friends. *Journal of Information Privacy and Security, 10(3)*, 113-137.

QuestionPro. (2018). *¿Qué es la escala de Likert y como utilizarla?* Retrieved from https://www.questionpro.com/blog/es/que-es-la-escala-de-likert-y-como-utilizarla/

Smith, K. (2018). *116 estadísticas interesantes de las redes sociales*. Retrieved from https://www.brandwatch.com/es/blog/116-estadisticas-de-las-redes-sociales/

Tootoonchian, A., Saroiu, S., Ganjali, Y., & Wolman, A. (2009). Lockr: better privacy for social networks. *Emerging networking experiments and technologies*, (pp. 169-180).

Toranzo, F. M. (2013). Riesgos en el uso de las redes sociales. *Big Data*.

Wüest, C. (2010). The risks of social networking. *Symantec Corporation*.

Xiao, Y., Bu, Z., Hsu, C. H., Zhu, W., & Shen, Y. (2017). Trust-Aware Recommendation in Social Networks. *In International Conference on Knowledge Science, Engineering and Management*, pp. 380-388.

Zhang, C., Sun, J., Zhu, X., & Fang, Y. (2010). Privacy and security for online social networks: challenges and opportunities. *IEEE network, 24(4)*.

Zhao, J., & Zhao, S. Y. (2015). Security and vulnerability assessment of social media sites: An exploratory study. *Journal of Education for Business, 90(8)*, 458-466.