Revista Eletrônica de Sistemas de Informação
ISSN 1677-3071

Vol 17, No 1

Jan-Apr 2018

DOI: https://doi.org/10.21529/RESI.2018.1701

Table of Contents

Teaching and Research

Focus on people

Esta revista é (e sempre foi) eletrônica para ajudar a proteger o meio ambiente, mas, caso deseje imprimir esse artigo, saiba que ele foi editorado com uma fonte mais ecológica, a *Eco Sans*, que gasta menos tinta.

This journal is (and has always been) electronic in order to be more environmentally friendly. Now, it is desktop edited in a single column to be easier to read on the screen. However, if you wish to print this paper, be aware that it uses Eco Sans, a printing font that reduces the amount of required ink.

RIESGOS INHERENTES EN LA PRIVACIDAD DE LOS USUARIOS POR EL USO DE LAS TIC

INHERENT RISKS TO USERS PRIVACY BY THE USE OF ICT

(artículo sometido en enero de 2018)

Juan Carlos Pérez Pérez
Licenciado en Informática por la Universidad Nacional Autónoma de México
jcarlperez83@gmail.com

Graciela Bribiesca Correa
Doctora en Administración de las Organizaciones por la Universidad Nacional Autónoma de México
Profesora Investigadora de la Facultad de Contaduría y Administración, Universidad Nacional Autónoma de México
gbribies@fca.unam.mx

Guillermo Rodríguez Abitia
Doctor en Sistemas de Información por la Universidad de Texas en Arlington
Director de Innovación y Desarrollo Tecnológico en la Dirección General de Cómputo y de TIC, Universidad Nacional Autónoma de México
grdrz@unam.mx

ABSTRACT

Information and communication technologies (ICT) are an integral part of our lives, and they bring along risks that are inherent to their use, being the intrusion to the privacy of the users one of the most common ones. This work seeks to estimate the effectiveness of the application of security measures by ICT users to mitigate the inherent use risks, departing from a set of variables drawn from the existing body of knowledge, such as digital literacy, and network activities and behaviors, like compulsion and permissibility. To attain this goal, an observational and cross-sectional study was conducted, through the design of a survey instrument that was applied to 159 internet users who were members of social networks and belonged to a community of videogame players. The data obtained from the survey was analyzed using a binary multivariate model of stepwise logistic regression, by the maximum likelihood method, and selecting explanatory variables through forward and backward techniques, as well as undertaking goodness of fit tests. Amongst the most important results, it is shown that, despite fostering the use of better security practices and showing a lower ratio of intrusions to privacy, digital literacy has no significant impact on the likelihood of becoming a victim of intrusion. When stratifying the sample by age, a trend was clear for having a higher vulnerability when age increased. However, the difference between the groups was not as significant as illustrative.

Key-words: user privacy; risk; logistic regression.

RESUMEN

Las Tecnologías de Información y Comunicación (TIC) forman parte integral de nuestra vida y acarrean riesgos inherentes a su uso, siendo la intrusión a la privacidad de los usuarios uno de los más comunes. Este trabajo busca estimar la efectividad de la aplicación de medidas de seguridad de los usuarios de TIC para mitigar el riesgo a partir de un conjunto de variables como alfabetización digital, actividades y comportamientos en la red como compulsión y permisividad. Para lograr este objetivo, se llevó a cabo un estudio observacional de corte transversal, mediante el diseño de una encuesta que se aplicó a una población de 159 internautas mexicano, usuarios de redes sociales y pertenecientes a una comunidad de video jugadores de computadora. Para analizar los resultados de dicha encuesta, se utilizó un modelo binario y multivariado de regresión logística, por el método de máxima verosimilitud, con el que se seleccionaron variables explicativas mediante la técnica de pasos (hacia adelante y hacia atrás) y se realizaron pruebas de bondad de ajuste. Entre los resultados más importantes se muestra que a pesar de realizar mejores prácticas de seguridad y tener un menor número de intrusiones a la privacidad, el nivel de alfabetización digital no es significativo o determinante para ser víctima de una intrusión. Al estratificar por edad se observó una tendencia a estar en mayor posibilidad de sufrir intrusión cuando se tiene mayor edad, sin embargo, la diferencia entre los grupos no resultó significativa, pero sí ilustrativa.

Palabras clave: privacidad de usuarios; riesgo; regresión logística.

1 INTRODUCCIÓN

La privacidad es un derecho que se ha desarrollado por más de 3,000 años (FERENSTEIN, 2015), plasmado como derecho humano en el artículo 12 de la Declaración Universal de Derechos Humanos (DUDH) en 1948 así como en el artículo 17 del Pacto Internacional de los Derechos Civiles y Políticos de 1976.

El auge de las Tecnologías de la Información y Comunicación (TIC) y la interconexión de millones de personas a través de estas tecnologías, principalmente mediante Internet y redes sociales, las ha convertido en parte integral de nuestra vida. Sin embargo, esta facilidad de acceso a la información, rapidez en la transmisión de datos y el bajo costo en la comunicación acarrea riesgos diversos (SANCHO, 2017). Es así como la preocupación de privacidad es un aspecto de vital importancia en la edad de la información, dada la facilidad que da el internet para recoger, almacenar, procesar y utilizar información personal (SMITH, DINEY, & XU, 2011).

La privacidad de la información se refiere a "la capacidad de controlar cómo la información personal de uno se adquiere y se usa" (PAVLOU, 2011, p. 977).

A lo largo de la historia, han existido personas dispuestas a comerciar privacidad por conveniencia, riqueza o fama (FERENSTEIN, 2015). Hoy en día, esta práctica es común entre individuos que van desde “youtubers”, “bloguers” y hasta usuarios comunes de redes sociales, quienes ponen en riesgo su privacidad.

Aunque los usuarios periódicamente reciben información sobre nuevos ciberdelitos ante los cuales están desprotegidos (SANCHO, 2017) y están cada vez más conscientes de los riesgos que implica el uso de tecnología al adquirir un nuevo dispositivo, demandando seguridad y privacidad, no reflejan esa preocupación en sus hábitos y prácticas de seguridad cotidianos (O’BRIEN *et al.*, 2016).

Debido al uso de Internet, los usuarios propagan huellas digitales (*digital footprints*), es decir, los rastros que dejamos cuando utilizamos Internet y que, en su conjunto, conforman expedientes digitales de cada uno de los usuarios (INTERNET SOCIETY, 2014). Cada foto en redes sociales, información de contacto, fecha de nacimiento, estado de ánimo, datos bancarios, relaciones sentimentales, gustos, preferencias, formación académica, ubicación u otro tipo de *digital footprint* pone en riesgo nuestra privacidad e incluso la de terceros. Esto abre las puertas a una intromisión a nuestra esfera de intimidad por parte de usuarios maliciosos o ciberdelincuentes que pueden hacer mal uso de información sensible que fácilmente puede ocasionar algún perjuicio.

Por lo tanto, estos expedientes y los perfiles de redes sociales son una representación de la realidad de los usuarios, que puede verse distorsionada como consecuencia de la variación de su comportamiento, así

como de sus límites entre lo público y lo privado en el mundo de Internet. Por ello, buscamos explorar si los riesgos y el grado de consciencia que se tenga de ellos afectan el comportamiento de los usuarios, en beneficio del uso de prácticas de seguridad más robustas que prevengan intrusiones en su información. En las secciones subsecuentes, se realizará una revisión general de la vasta literatura en el tema, para pasar a definir la pregunta de investigación, describir la metodología empleada y presentar los resultados y conclusiones que se obtuvieron como consecuencia.

2 MARCO TEÓRICO

Para brindar claridad en el enfoque de este trabajo, se revisará primero, de manera muy general, el estado de la literatura más relevante en el tema de privacidad de la información. Esto será seguido de una sección que trate de establecer las diferencias entre lo público y lo privado, para finalizar con una revisión del concepto de riesgo y sus constructos asociados.

2.1 LA PRIVACIDAD DE LA INFORMACIÓN

Es probable que los esfuerzos más grandes para revisar la vasta literatura que se relaciona con el tema de privacidad de la información sean los de Belanger & Crossler (2011) y de Smith, Diney, & Xu (2011), revisados en el mismo número por Pavlou (2011).

Belanger & Crossler (2011) hacen una revisión literaria de 100 revistas y 100 conferencias para un total de 500 artículos. Definen privacidad de información como la integración de privacidad de datos y de comunicación personal. Abordan preocupación de privacidad como la voluntad personal de brindar información personal y de transacciones. Los autores también indican que la investigación existente se concentra principalmente en la explicación y predicción de la privacidad de la información, después en analizarla y al final en diseñar herramientas para su protección. Recomiendan cinco acciones esenciales: (1) analizar más allá de la unidad de análisis del individuo; (2) utilizar muestras de poblaciones más diversas; (3) llevar a cabo más investigación de acción y de diseño; (4) estudiar más el por qué y menos el cómo y (5) justificar instrumentos de medición existentes y desarrollar otros generales.

Por otro lado, Smith, Diney, & Xu (2011) revisaron 320 artículos, libros y secciones de libros y los categorizan buscando conceptualizar la privacidad de información y su relación con otros constructos. Hacen mención a conceptos existentes y relacionados con teoría económica como la paradoja de la privacidad y el cálculo de la privacidad. La primera se refiere a la asignación de un valor económico en un análisis costo beneficio que puede variar enormemente de acuerdo al contexto, por lo que los individuos pueden tener grandes valores de preocupación de privacidad, pero actuar de manera contradictoria. La segunda se refiere al valor calculado del beneficio que se podrá obtener por revelar cierta información. Se propone el modelo APCO, que sugiere que los investiga-

dores tengan en cuenta un macro modelo que abarca tres etapas, los antecedentes precursores de una preocupación de privacidad y los resultados en términos de comportamiento.

Pavlou (2011), además de hacer una excelente integración de ambos trabajos, establece que la preocupación de privacidad puede ser un gran obstáculo para realizar transacciones de comercio electrónico.

Xu, Diney, Smith, & Hart (2008) desarrollaron un modelo para explicar cómo los individuos generan su propia preocupación de privacidad, mismo que está basado en teoría de límites de información. Dicha teoría especifica que cada individuo establece los límites de acceso a su información según cada contexto. Un intento de pasar esos límites se considera una intrusión. Los aspectos que más influyen este proceso son el riesgo de privacidad, la percepción de control y la percepción de invasión.

Por su parte, Bal (2014) realizó un análisis, en el caso de los teléfonos móviles, sobre el efecto de un sistema apropiado de comunicación de riesgo y su impacto en la calidad de la toma de decisiones. Concluye que, con la comunicación adecuada, se realiza un cálculo de privacidad más pertinente, guiando a un comportamiento más apropiado. Curiosamente, este aspecto no parece estar ligado a la experiencia, como lo indica el estudio realizado por Lampkton & Tripp (2013), que concluye que la experiencia no tiene efecto en preocupación de privacidad, pero el género sí. Sin embargo, sí podría afectar confianza.

2.2 LO PÚBLICO Y LO PRIVADO

Aún cuando en un ambiente físico podamos ser celosos de nuestra privacidad, al encontrarnos inmersos en un entorno digital perdemos la capacidad de distinguir entre lo público y lo privado (ALBORNOZ, 2016). Todos hemos comenzado a vivir una vida dual, es decir una física y otra virtual, pero ambas están asociadas a datos personales financieros, de geolocalización, de gustos y de preferencias, que compartimos con otros, a veces de manera intencional y otras no (CHAUHAN; PANDA, 2015). Por ello, es importante definir criterios claros de compartición de datos, basados en la diferencia entre lo público y lo privado. Rabotnikof (1998) plantea tres criterios para distinguir entre lo público y lo privado:

A) Colectividad. Lo público es plural y lo privado singular. De este modo lo público puede ser de interés de una comunidad, un pueblo, un país e incluso global. En el mundo de Internet existen comunidades de diversos tipos con individuos qué físicamente se encuentran en distintos puntos geográficos del mundo, pero que aun así mantienen un interés común. Lo privado es de interés individual. Referido al uso de las tecnologías, podemos limitarlo a dispositivos de uso personal como la computadora personal, el teléfono inteligente u otro dispositivo capaz de almacenar información que sólo es relevante para el individuo mismo. El conjunto agregado de intereses individuales reducidos es de mayor envergadura y representa los intereses colectivos.

B) Visibilidad. Bajo este criterio, lo público es visible, volviendo a la analogía con el mundo de Internet, lo público es aquello que pone a la vista, ya sea en perfiles de redes sociales, sitios de Internet, pantallas con anuncios, etc. Bajo este criterio también podríamos referirnos no solo a lo visible si no a lo que es audible, aquello que escuchamos en nuestros dispositivos. Rabotnikof (1998) define lo público como aquellas actividades que realizamos a la mirada de otros. Lo privado se mantiene oculto, en secreto, y es aquello que mantenemos almacenado en nuestros dispositivos para que no pueda ser visualizado o escuchado por otros. Es posible ocultar accesos e información en sistemas de información por distintos motivos, como el criterio de colectividad en su carácter de privado lo que abre paso al tercer criterio.

C) Accesibilidad. El tercer criterio es la accesibilidad que hace referencia a la apertura y la clausura. En el caso de lo público, lo que es accesible para todos, puede referirse a lugares públicos. En Internet, las redes sociales son un ejemplo claro en donde los usuarios pueden abrir al público sus perfiles y sus contenidos para ser visualizados sin restricción por cualquier persona. A partir del criterio de accesibilidad se deriva el sustantivo “el público” que hace referencia a todos aquellos que se benefician de la accesibilidad, que con las TIC se puede ver potenciada en número de personas y lugares (RABOTNIKOF, 1998). Estos tres criterios regularmente son congruentes entre sí y pueden ayudar a delimitar la línea entre lo público y lo privado. Está en una línea delgada que varía en el tiempo, los principios éticos y morales de cada individuo o sociedad.

La Figura 1 ilustra los tres criterios mencionados por Rabotnikof (1998).

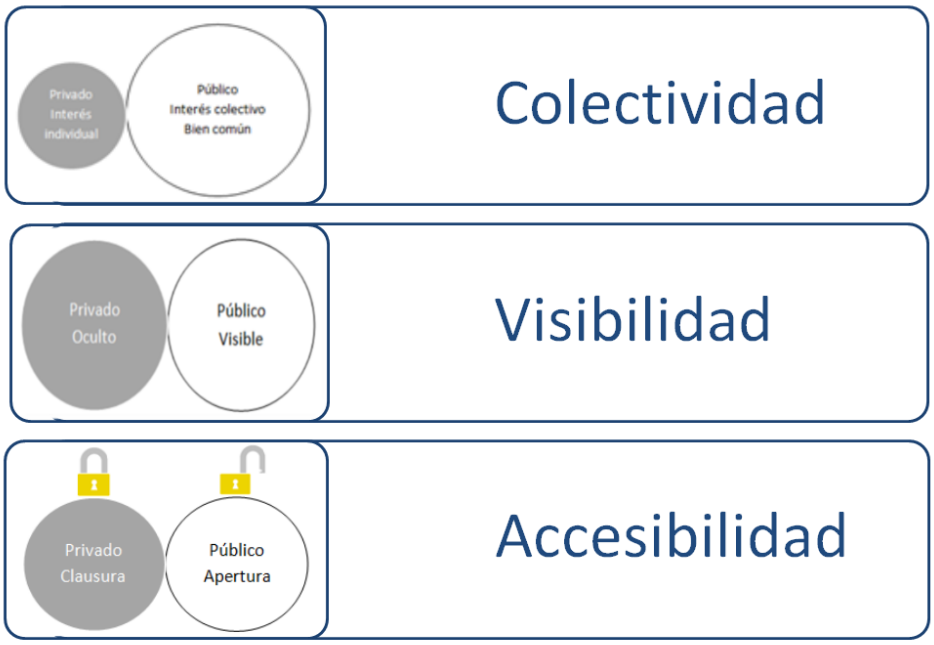

Figura 1. Criterios de distinción entre lo público y lo privado

Fuente: elaboración propia con base en Rabotnikof (1998).

Por su parte Solove (2002) conceptualiza la privacidad con base en seis criterios, los cuales se complementan con los tres criterios planteados anteriormente para diferenciar entre lo público y lo privado. Estos son:

A) El derecho a estar solo: formulado en el ensayo "*The right to privacy*" (WARREN & BRANDEIS, 1890), referente al deseo de un individuo de aislarse de los demás. Este criterio puede analizarse desde dos dimensiones: una espacial y otra de visibilidad equivalente a lo mencionado por Rabotnikof (1998), en que es posible apartar las actividades del individuo de la mirada de otros y esto se considera un derecho.

B) Acceso limitado al *Yo*: en este caso el criterio de accesibilidad es específico al *Yo*. Solove (2002) lo plantea como la capacidad de protegerse del acceso no deseado por parte de otros. Se puede asociar a una combinación de los criterios de colectividad y accesibilidad de Rabotnikof (1998), donde se aplica el interés individual y la clausura.

C) Secreto: este criterio se refiere a la ocultación de actividades y asuntos a terceros, pudiendo asociarse al criterio de visibilidad planteado por Rabotnikof (1998).

D) Control sobre la información personal: es la capacidad de ejercer control sobre la información propia. Este criterio es interesante ya que trata directamente sobre el control de los datos personales, aplicando mecanismos que permitan la combinación de los criterios de colectividad, visibilidad y accesibilidad de Rabotnikof (1998) en su calidad de lo privado, es decir, manteniendo el interés individual, el secreto y la clausura sobre la información personal para restringir la accesibilidad y visualización de su información.

E) Personalidad: este criterio plantea la protección de la personalidad, la individualidad y la dignidad. De acuerdo con Garzón Valdés (2012), dejar al descubierto la propia intimidad significa eliminar lo que es secreto, incluyendo sentimientos y pensamientos no claros y difíciles de capturar por otros. El criterio de visibilidad de Rabotnikof (1998), en este caso, no es suficiente para explicar la protección de la personalidad ya que lo mostrado de la propia intimidad puede ser información no integral y difícil de interpretar, lo cual puede ofrecer una versión distorsionada de nuestra propia personalidad (GARZÓN VALDÉS, 2012).

F) Control sobre la intimidad: implica el control sobre, o el acceso limitado a, aspectos de la vida o relaciones íntimas del individuo. Esto implica la administración del acceso a la intimidad. En el Cuadro 1, se vinculan los criterios de Solove (2002) para conceptualizar y concebir la privacidad, con los criterios de colectividad, visibilidad y accesibilidad en su carácter de privado, planteados por Rabotnikof (1998), donde se identifica que criterios son necesarios para cumplir cada una de las concepciones de privacidad.

Concepción privacidad (Solove, 2002)	Criterio privado (Rabotnikof, 1998)
Derecho a estar solo	Visibilidad (secreto)
Acceso limitado al Yo	Accesibilidad (clausura)
Secreto	Visibilidad (secreto)
Control sobre la información personal	Colectividad (interés individual) Visibilidad (secreto) Accesibilidad (clausura)
Personalidad	Visibilidad (secreto) Accesibilidad (clausura)
Control sobre la intimidad	Accesibilidad (clausura)

Cuadro 1. Relación entre criterios de privacidad y de distinción entre lo público y lo privado.

Fuente: elaboración propia con base en Rabotnikof (1998) y Solove (2002).

En el Cuadro 1 se observa una correspondencia entre los criterios planteados anteriormente por ambos autores. Se destaca que el criterio de privacidad denominado “Control sobre la información personal” no tiene una correspondencia directa y única, sino que se vincula con los tres criterios de Rabotnikof (1998).

La información está sujeta a los tres criterios de distinción entre lo público y lo privado, ya que siempre se ha considerado un activo esencial para los seres humanos, brindado ventajas de competencia en varios ámbitos de la vida, desde el personal hasta el organizacional. Es por ello que reviste una gran importancia no solo identificar que partes de la información deben ser públicas y cuáles privadas, sino garantizar que se mantengan así. Krutz & Vines (2010) proponen el modelo de la triada CIA para lograr este objetivo. Las siglas en inglés CIA se refieren a los componentes de confidencialidad, integridad y disponibilidad de la información. La confidencialidad se refiere a la prevención de la divulgación no autorizada o no intencional de contenidos. Por otra parte, la integridad es la garantía de que la información no sea alterada intencional o no intencionalmente. Finalmente, la disponibilidad se refiere a que sea accesible con oportunidad, por las personas autorizadas.

La seguridad de la información se puede definir como el conjunto de medidas para la protección de la información y de los sistemas de información contra el acceso, uso, revelación, interrupción, modificación o destrucción no autorizados (KISSEL, 2013). En el Glosario de los principales términos de seguridad de la información del Instituto Nacional de Normas y Tecnología del Departamento de Comercio de los Estados Unidos (KISSEL, 2013), mantener la integridad de la información implica protección contra información inadecuada, modificación o destrucción, e incluye el no rechazo y la autenticidad.

El Cuadro 2 vincula las características de la información con los criterios de lo privado, planteados por Rabotnikof (1998). Esta vinculación

ayuda a determinar la importancia de dichos criterios en el control de la información personal y privada. La confidencialidad gana relevancia, al relacionarse con los criterios de interés individual, es decir la secrecía y la clausura.

Características de la información	Criterio privado
Confidencialidad	Colectividad (interés individual) Visibilidad (secreto) Accesibilidad (clausura)
Integridad	Accesibilidad (clausura)
Disponibilidad	Colectividad (interés individual) Visibilidad (secreto) Accesibilidad (clausura)

Cuadro 2. Características de la información y criterios de lo privado.

Fuente: elaboración propia con base en Rabotnikof (1998) y Kissel (2013).

La integridad depende del control que se pueda ejercer sobre la accesibilidad. Por otra parte, la disponibilidad echa mano de la colectividad y la accesibilidad para procurar el acceso controlado a la información disponible solo para aquel a quien le sea de interés personal y esté autorizado a acceder a ella.

Existen diversos tipos de amenazas utilizadas por *hackers* y delincuentes informáticos para obtener datos e información personal, que ponen en peligro la privacidad de los usuarios de TIC, mediante la pérdida del control de la información personal, el acceso al *Yo* y a lo secreto. Estas amenazas forman la base de los riesgos a la privacidad, que no siempre son bien identificados ni entendidos por los usuarios.

2.3 EL RIESGO

El riesgo es definido como la medida en que una entidad está amenazada por una circunstancia o evento potencial, típicamente en función de los impactos adversos que surgirían si se produjera y su probabilidad de ocurrencia (KISSEL, 2013).

La sociedad ha sido calificada por el sociólogo alemán Ulrich Beck (1998) como una sociedad del riesgo, donde los mismos avances de la industria y la modernización se ven acompañados de riesgos y peligros que afectan nocivamente a los miembros de la comunidad. A diferencia de los efectos visibles de la polución tecnológica, es casi imperceptible detectar los síntomas y efectos de ataques por software malicioso utilizado por delincuentes y que se apoyan de técnicas como la ingeniería social, convirtiendo a los usuarios de TIC en victimas que están en peligro de perder el control sobre la información que se administra y procesa en sus dispositivos.

Beck (1998) señala que, a diferencia de hoy, en la antigüedad los peligros eran mayormente perceptibles mediante los sentidos. Sin embargo, los riesgos que acompañan a las TIC son principalmente intangibles. Así, con la modernización evolucionan los riesgos como consecuencia del propio desarrollo técnico y económico.

Con la llegada y masificación de las TIC, llegaron también nuevos riesgos inherentes a su uso, tanto para los dispositivos, como para la información sensible que en ellos se procesa y almacena, pudiéndose generar perjuicios financieros, morales o de bienestar de un individuo o de una sociedad entera. Como consecuencia, se otorga la posibilidad de que el usuario tome un rol de víctima, victimario, espectador o juez, debido a los valores de colectividad, visibilidad y accesibilidad que magnifican las TIC.

Para Beck (1998), al igual que ocurre con la riqueza, los riesgos se reparten de forma desigual, existiendo actores privilegiados, como aquellos que tienen poder, ya sea económico o educativo. El riesgo y la seguridad son un gran negocio, como lo describe dicho autor, ya que actualmente los consumidores son dependientes de los proveedores en cuanto a seguridad y privacidad se refiere (O'BRIEN *et al.*, 2016) y los usuarios con mayor poder (económico o educativo) pueden mitigar el riesgo adquiriendo dispositivos más caros y seguros, o bajo condiciones mejor informadas. Mientras tanto, los usuarios comunes prefieren precios bajos o carecen de los conocimientos necesarios para tomar decisiones de compra que aumenten su seguridad y privacidad (O'BRIEN *et al.*, 2016).

Douglas (1996) una de las críticas de Beck, considera que la percepción de un riesgo también depende de las nociones éticas y morales. Por lo tanto, en cuanto a la afectación se refiere, los mismos ataques pueden tener un significado completamente diferente para personas con distinta edad, sexo, hábitos alimenticios, tipo de trabajo, información, educación, etc. Es por ello que el análisis del riesgo de la información privada varía de persona a persona.

Para Douglas (1996) las formas de percibir los riesgos se ordenarían según códigos privilegiados y, entonces, el usuario común no percibe los riesgos de igual manera que los expertos, debido a privilegios técnicos o de educación. La educación, y un comportamiento sensible en relación a la información, abren nuevas posibilidades de enfrentarse a los riesgos y evitarlos.

De igual forma para Beck (1998) y Douglas (1996), el problema de los riesgos no se vincula a un proceso de educación, ya que supondría aceptar la teoría de que lo sujetos podrían realizar una elección probabilística de determinados peligros. Es ahí donde Douglas (1996) introduce el concepto de "inmunidad subjetiva" en el cual se subestiman los riesgos que se consideren controlados y sean vinculables a los acontecimientos que se dan con poca frecuencia. Con la consideración de "inmunidad subjetiva" se reduce considerablemente la percepción de los riesgos en un análisis,

lo que puede hacer creer a un usuario que su información privada está más segura de lo que en realidad está. Esto se ilustra en la Figura 2.

Figura 2. Percepción del riesgo "inmunidad subjetiva"

Fuente: elaboración propia con base en Douglas (1996).

Crear una tolerancia al riesgo, al establecer valores de aceptabilidad de acuerdo con el sistema cultural en el que se fraguan los niveles éticos y morales, se puede traducir en la aceptación del mismo por parte de los usuarios y en la vulneración potencial de la privacidad a través de las TIC (MONTENEGRO, 2005).

Esta tolerancia se amplía en la sociedad contemporánea, definida por Llano Cifuentes (1998) como compulsiva, debido a que el comportamiento estadístico prevalece sobre el antropológico. Es ahí donde los individuos tratan de detectar tendencias para seguirlas, en lugar de intentar entender cómo es el hombre, para orientarse. Además, se genera el fenómeno social de la importancia de la demanda sobre la necesidad, donde ya no se distingue entre una y otra, realizando aquello que es compulsivo sobre lo necesario (LLANO CIFUENTES, 1998). Más aún, de acuerdo con este autor, otro de los fantasmas de la sociedad contemporánea es que esta se ha vuelto permisiva e impersonal, dejando que la permisividad niegue la trascendencia de las leyes morales y las considere como forma de un sistema de represión.

Debido a la penetración de las TIC en la sociedad y su importancia para la vida diaria, así como a fenómenos como el de la compulsividad de la sociedad (LLANO CIFUENTES, 1998), es común encontrar usuarios que busquen alcanzar la cima de la pirámide de jerarquía de necesidades propuesto por Maslow (1943), a través de Internet, redes sociales y mundos virtuales, sin asegurar el segundo escalafón de la seguridad y estabilidad que, en un entorno de TIC, involucra análisis del riesgo, prácticas de seguridad y sentido común.

Fenómenos como la compulsividad, la demanda antes que la necesidad, la permisividad y un tanto la anarquía en Internet, extienden la tolerancia al riesgo y la inmunidad subjetiva, sobre todo de los peligros cotidianos más comunes. De esta forma, la realización de cada acción a través de nuestros dispositivos se reduce social y permisivamente a la pregunta "¿qué tiene de malo?" (LLANO CIFUENTES, 1998).

2.4 ALFABETIZACIÓN DIGITAL

Martin (2007) desarrolló una escala de tres niveles de alfabetización digital, misma que se ilustra en la Figura 3.

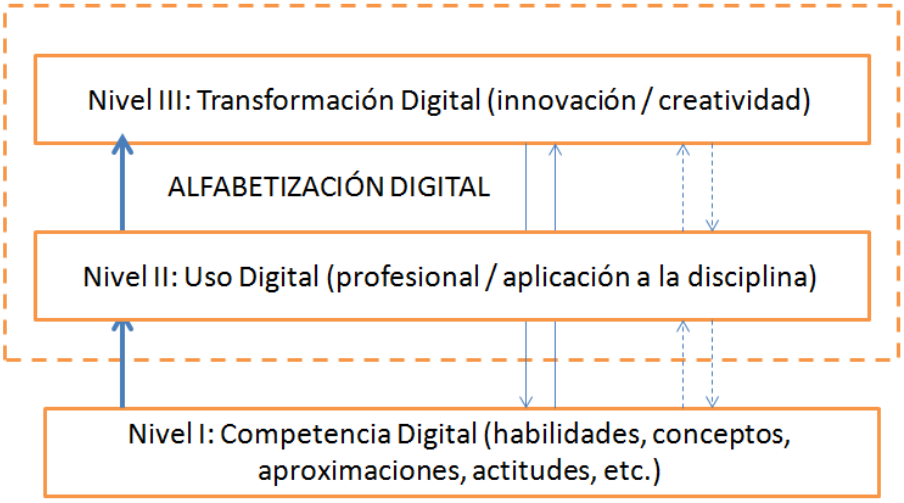

Figura 3. Niveles de alfabetización digital.

Fuente: Martin (2007)

En la base se encuentra el nivel de competencia digital, que abarca habilidades y conocimientos digitales de uso general, incluyendo navegar en Internet, utilizar paquetes de ofimática, participar en juegos digitales, utilizar productos multimedia, etc. Este nivel, de acuerdo con Martin (2007), será recurrido por individuos y grupos tan a menudo como los nuevos desafíos y situación de vida cambien.

En el segundo nivel se encuentra el uso digital, que es donde la competencia digital implica un uso exitoso en situaciones de vida y resolución de problemas específicos en un contexto profesional, de formación o de otro tipo (MARTIN, 2007).

En el tercer escalón se encuentra la transformación digital que, de acuerdo con Martin (2007), se logra cuando los usos digitales se han desarrollado lo suficiente que permiten innovación y creatividad, estimulando un cambio significativo en el ámbito profesional, personal y social. Cabe mencionar que el autor considera la acción reflexiva en todos los niveles de alfabetización, sobre todo en niveles superiores donde esta se vuelve más crítica.

La importancia de categorizar a los usuarios por su nivel de alfabetización digital nos remite Beck (1998) y la repartición desigual del riesgo ante la modernización y la tecnología, así como la percepción del mismo según educación y conocimiento de la tecnología, por lo cual un usuario común no ve los riesgos igual que los expertos, ya que la educación y un comportamiento sensible en relación a la información abren nuevas posibilidades de enfrentarse a los riesgos y evitarlos (MONTENEGRO, 2005).

3 DESARROLLO DEL ESTUDIO

Dados los conceptos revisados y el objetivo establecido en la introducción, es posible plantear la siguiente pregunta de investigación:

¿Las medidas de seguridad para proteger la privacidad en los dispositivos de los internautas con un grado alto de familiarización y conocimiento de TIC son aplicadas con mayor eficacia que las de los que no lo tienen?

Para poder contestar esta pregunta, se consideró definir como población de estudio a los miembros de un grupo de video jugadores en Facebook, ya que son representativos de la familiaridad en la utilización de tecnología y pertenecen, generalmente, a una generación ya más preparada en aspectos digitales.

3.1 METODOLOGÍA

Se llevó a cabo un estudio observacional de corte transversal, mediante el diseño de una encuesta, que se aplicó a una muestra de conveniencia de internautas mexicanos, usuarios de redes sociales pertenecientes a una comunidad de video jugadores de computadora, quienes contestaron un cuestionario con preguntas elaboradas con base en los constructos relevantes en la investigación, con el fin de analizar sus prácticas de seguridad y uso, así como las incidencias sufridas por intromisión a su privacidad.

3.2 ESTRUCTURA DEL INSTRUMENTO

La estructura del cuestionario o instrumento de medición se dividió en tres secciones, iniciando con la descripción de los propósitos de la investigación. Se informó a los participantes sobre la confidencialidad de su colaboración y se les pidió contestar con sinceridad, con el fin de obtener un resultado más cercano a la realidad.

En la segunda sección del cuestionario se preguntaron datos demográficos, teniendo especial interés en controlar por medición las variables alternativas de edad y género, que parecen tener gran relevancia en estudios anteriores.

La tercera sección del cuestionario estuvo conformada por 28 preguntas obligatorias, 4 preguntas de control opcional y una última pregunta opcional destinada a la disposición de los usuarios a comerciar con la

privacidad. Estas preguntas fueron realizadas de acuerdo con la operacionalización de variables, donde se establecen los siguientes 3 constructos: conocimiento y uso de las TIC, medidas de seguridad de los usuarios y comportamiento (Cuadro 3).

Constructo	Variable	Preguntas
Conocimiento y uso de TIC	Formación especializada	¿Eres estudiante o egresado de una carrera afín a las Tecnologías de la Información y Comunicación? ¿Cuál?
	Uso de TIC	¿Qué dispositivos para conectarte a Internet utilizas con más frecuencia?
	Actividades	¿Cuáles son las actividades que realiza a través de las TIC?
	Legal	¿Conoces la legislación sobre privacidad y delitos informáticos en México?
	Sistema operativo	¿Qué sistemas operativos utilizas?
	Perjuicio intromisión	¿Has sido víctima de intromisión a tu privacidad a través de las TIC?
	Conocimiento perjuicios	¿Conoces a alguien que haya sido víctima de intromisión a su privacidad a través de las TIC?
Medidas de seguridad de los usuarios	Análisis del riesgo	¿Analizas el riesgo de cada acción que realizas con tus dispositivos?
	Software de seguridad	¿Utilizas software antivirus en sus dispositivos (computadora, tableta o celular)? ¿Cuáles?
	Seguridad en redes	¿Utiliza Redes Privadas Virtuales (VPN)?
	Accesibilidad	¿Con que frecuencia cambia las contraseñas de sus cuentas personales de correo y servicios?
	Accesibilidad	¿Qué método de autenticación utilizas en su teléfono celular?
	Cifrado	¿Cifra sus carpetas, contraseñas o dispositivos?
	Anonimato	¿Utiliza sesiones de navegación privada o utiliza el navegador Tor?
	Mecanismos de privacidad	¿Configura los parámetros de privacidad de sus redes sociales y aplicaciones?
	Sensores	¿Bloquea o desactiva sensores de cámara, micrófono y geolocalización de sus dispositivos?
Comportamiento de los usuarios	Compulsión	¿Suele compartir su ubicación geográfica a través de redes sociales?
	Compulsión Fotografías	¿Suele subir fotografías personales, viajes o de la familia a redes sociales?
	Compulsión	¿Ha realizado o participado en algún *challenge* de Internet?

	Compulsión Adicción	¿Si estas desconectado de Internet sientes que te pierdes de algo?
	Permisividad Contraseñas compartidas	¿Compartes alguna cuenta de usuario de algún servicio, software, computadora de trabajo o personal?
	Permisividad Computadoras públicas	¿Utilizas computadoras o redes públicas (cibercafé, WiFi gratuito)?
	Permisividad Legal	¿Lees el aviso legal o términos de condiciones de los servicios y aplicaciones que utilizas?
	Permisividad	¿Aceptas el uso de cookies en las páginas web que visitas?
	Piratería Compulsión	¿Has consumido piratería de software, música, películas, series o pornografía a través de internet?
	Permisividad	¿Has practicado *sexting*?
	Tendencia a comercializar con la privacidad	Para participar en un sorteo proporciona tu perfil de Facebook y Steam id.

Cuadro 3. Operacionalización de variables.

Fuente: elaboración propia

El cuestionario fue realizado en línea utilizando el servicio de formularios de Google, lo que permitió que pudieran contestar la encuesta de forma remota y anónima. La invitación a contestar fue distribuida a través de un grupo de Facebook dedicado a la interacción de usuarios mexicanos de una plataforma de distribución digital de videojuegos de computadora. Como incentivo se ofreció la posibilidad de ganar una clave de activación de un producto de dicha plataforma. Las respuestas fueron codificadas de acuerdo con la información mostrada en el Cuadro 4.

Codificación de identificadores

Identificador	Código	Variable	Código
Género	GEN	Hackeo de cuentas	P02
Edad	EDAD	Filtración de fotografías o vídeos	P03
Alfabetización digital	TIC01	Clonación de tarjeta bancaría	P04
Smartphone	TICD1	*Phishing*	P05
Laptop	TICD2	Perdida de información	P06
Computadora personal	TICD3	*Grooming*	P07
Consola de videojuegos	TICD4	*Creepware*	P08
Otros dispositivos	TICD5	Acoso	P09
Redes sociales	TICA01	Conocer a alguien que sufrió intrusión a la privacidad	CVIP
Correo electrónico	TICA02	Análisis de riesgo	MS01
Mensajería instantánea	TICA03	Uso de antivirus	MS02
Búsqueda de información	TICA04	Redes privadas virtuales	MS03

Videojuegos en línea	TICA05	Frecuencia de cambio de contraseñas	MS04
Compra venta en Internet	TICA06	Tipo de autenticación	MS05
Pornografía	TICA07	Cifrado de contraseñas y carpetas	MS06
Transmisión en línea	TICA08	Navegación anónima	MS07
Ver películas y series	TICA09	Configuración parámetros privacidad	MS08
Solicitar transporte	TICA10	Bloqueo de sensores	MS09
Creación de contenidos	TICA11	Compartir geolocalización	CU01
Buscar pareja	TICA12	Compartición de vídeos y fotos	CU02
Banca en línea	TICA13	Participación en *challenge*	CU03
Estudiar	TICA14	Compras por Internet	CU04
Conocimiento de legislación	TIC02	Sentimiento de desconexión	CU05
Windows	OS1	Compartición de cuentas	CU06
OS X	OS2	Uso de redes y computadoras públicas	CU07
Linux	OS3	Lectura del términos y condiciones	CU08
Android	OS4	Aceptación de *cookies*	CU09
iOS	OS5	Piratería	CU10
Otro sistema operativo	OS6	*Sexting*	CU11
Víctimas de intrusión a la privacidad	VIP	Comercialización de la privacidad	CU12
Robo de identidad	P01		

Cuadro 4. Codificación de identificadores de respuesta.
Fuente: elaboración propia

3.3 RECOPILACIÓN DE LA INFORMACIÓN

La muestra final estuvo compuesta por 159 internautas encuestados, que contestaron todas las preguntas. Para facilitar el manejo de los datos obtenidos, se codificaron y se transportaron a una hoja de cálculo.

La variable de interés o de respuesta fue el ser víctima de intrusión a la privacidad (VIP), la cual se codificó como 0 si el encuestado no había tenido un evento de intrusión a su privacidad y como 1 si había sido víctima de un suceso de intrusión.

Las variables independientes o explicativas estuvieron relacionadas a prácticas de los usuarios en sus dispositivos y fueron categorizadas entre buenas y malas prácticas asignando los valores de “0” y “1”, respectivamente.

3.4 ANÁLISIS ESTADÍSTICO

Se realizó análisis exploratorio uni y bivariado. A partir de los resultados, se elaboraron tablas y gráficos descriptivos.

Se llevó a cabo un análisis mediante un modelo de regresión logística binaria multivariada por el método de máxima verosimilitud, con el que se

seleccionaron variables explicativas mediante la técnica por pasos (hacia adelante y hacia atrás) y se realizaron pruebas de bondad de ajuste.

El modelo de regresión logística calcula una variable de respuesta Y cualitativa binomial en la que se obtienen dos valores:

Y = 1 que considera la presencia de un evento o característica, en este caso si hay posibilidad de que se sea VIP debido a una mala práctica, en otros casos presencia del evento.

Y = 0 que considera la posibilidad de que no se presente debido a una buena práctica, o ausencia del evento.

Xn = (X1, X2, ..., Xn), que son las variables independientes o explicativas

El modelo general para calcular la probabilidad de que un evento suceda está dado por:

Y = px + ε

En donde: px es la probabilidad de cada X o variable independiente y ε es el término de error. De tal manera que px es la probabilidad de que la respuesta Y tome el valor 1.

Para el valor observado x, la fórmula del modelo general es:

$$P(Y = 1|X = x) = p_x \frac{\exp\left(\beta_0 + \sum_{i=1}^{n} \beta_n x_n\right)}{1 - \exp\left(\beta_0 + \sum_{i=1}^{n} \beta_n x_n\right)}$$

Siendo x = (x1, x2, ..., xn) un valor observado de las variables independientes o explicativas.

Por lo tanto, 1-px indicará la probabilidad de que Y tome el valor 0. Aplicando la transformación logit a la ecuación del modelo obtenemos un modelo de regresión lineal:

$$logit(p_x = log\left(\frac{p_x}{1 - p_x}\right) = \beta_0 + \sum_{i=1}^{n} \beta_n x_n$$

Con este modelo se calcularon las posibilidades de riesgo de ser VIP ajustando por las variables explicativas (X).

Todo el análisis estadístico se realizó con el programa Stata, versión 14.

4 RESULTADOS

La muestra encuestada final estuvo conformada por 159 internautas mexicanos que aceptaron y respondieron interactivamente y de manera anónima todas las preguntas. De estos 24 (15.1%) fueron mujeres y 135 (84.9%) fueron hombres.

De la aplicación del cuestionario a los 159 internautas se obtuvo como producto de las preguntas de variables alternativas “Género” y “Edad” los resultados mostrados en la Tabla 1.

Tabla 1. Edad y género de la muestra (frecuencias y porcentajes)

Edad	Género		Total
	Femenino	Masculino	
13 - 17 años	1 0.63%	22 13.84%	23 14.47%
18 - 24 años	12 7.55%	65 40.88%	77 48.43%
25 - 30 años	9 5.66%	25 15.72%	34 21.38%
31 - 40 años	2 1.26%	23 14.47%	25 15.72%
Total	24 15.09%	135 84.91%	159 100.00%

Fuente: elaboración propia

Es evidente que, al tratarse de una población de video jugadores, es natural que la mayoría sean jóvenes. En la Tabla 1 se muestra que casi dos terceras partes tienen menos de 24 años. En cualquier caso, ningún participante pasa de 40 años de edad. Eso favorece la intención de estudiar individuos con altos niveles de familiarización en TIC, o bien que sean nativos digitales.

Al estratificar por edad y género se encontró que todos en edades de 18 a 24 años, prefieren conectarse a Internet mediante *smartphone*, seguido por la computadora de escritorio. Esta última quedó por encima de la computadora portátil, aún y cuando ésta ofrezca mayor movilidad. Esto puede ser debido a la potencia que una computadora robusta de escritorio puede ofrecer para ejecutar juegos, actividad asidua entre los miembros de esta población. Finalmente, se relegó al último lugar a la conexión a través de consolas de videojuegos, a pesar de que las mismas sean especializadas para ese uso (Figura 3).

A continuación, se puede apreciar de forma gráfica las preferencias de dispositivo para la conexión a Internet por edad y género, donde se puede distinguir la alta frecuencia en la conexión a Internet a través de *smartphones* entre los hombres de 18 a 24 años.

En cuanto a la alfabetización digital, se encontró que los participantes tenían perfiles diversos en TIC, desde licenciatura en informática, ingeniería en sistemas, mecatrónica, matemáticas aplicadas, mecatrónica, animación, diseño, técnico informático hasta *marketing* y bibliotecología. Actualmente los campos que conforman la alfabetización digital son variados e incluyen el pensamiento crítico y evaluación, el entendimiento sociocultural, la colaboración, la creatividad, la comunicación, las habilidades prácticas y funcionales, el manejo de información y la seguridad electrónica (PAYTON; HAGUE, 2010).

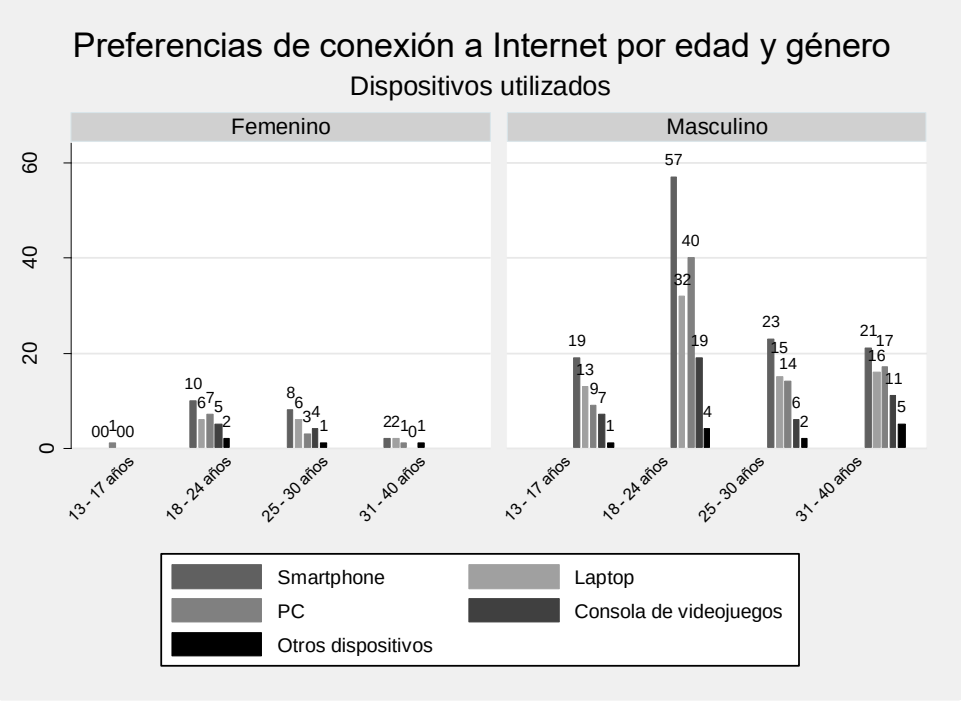

Figura 3. Preferencias de conexión a Internet por edad, género y dispositivos

Fuente: elaboración propia.

Por ello, se retomó la escala de alfabetización digital planteada por Martin (2007) donde se consideran 3 niveles. Para fines de este estudio se consideran el nivel 1 “Competencia digital” y el nivel 2 “Uso digital” debido a la imposibilidad de comprobar un tercer nivel. Se asigna así un nivel 1 de “Competencia digital” a aquellos que no cuentan con una formación en TIC, pero que tienen las habilidades suficientes para realizar sus actividades digitales cotidianas en sus dispositivos. Un nivel 2 se asigna a aquellos cuyo uso digital se encuentra en formación o que incluso alcanza el nivel profesional. El tercer nivel o de “Transformación digital” en el que se encuentran los usuarios que innovan y desarrollan TIC, no se consideró, debido a su complejidad y a que no era realmente necesario para efectos de este estudio.

Con el fin de no confundir los resultados por la distribución dispareja entre hombres y mujeres en la muestra, se estratificó por género. Los resultados de la Tabla 2 muestran que 62.3% de los encuestados posee competencia digital (nivel 1), mientras que 37.7% son usuarios que poseen una formación profesional en TIC (nivel 2), no encontrándose diferencias significativas por género.

Al estratificar por edad se puede distinguir como la mayoría de los usuarios de ambos géneros con un nivel 2 de alfabetización digital se concentran entre los 18 y 24 años (48%), siendo estadísticamente significativa esta diferencia con relación a las demás edades ($p<0.05$).

Tabla 2. Edad y nivel de alfabetización digital

Edad	Alfabetización digital		Total
	Nivel 2	Nivel 1	
13 - 17 años	4 2.52%	19 11.95%	23 14.47%
18 - 24 años	26 16.35%	51 32.08%	77 48.43%
25 - 30 años	17 10.69%	17 10.69%	34 21.38%
31 - 40 años	13 8.18%	12 7.55%	25 15.72%
Total	60 37.74%	99 62.26%	159 100.00%

Pearson chi2(3) = 8.9095 Pr = 0.031

Fuente: elaboración propia

En cuanto a la pregunta sobre si los participantes han sido víctimas de algún perjuicio debido a una intromisión a su privacidad, se encontró que el 36.5% de los participantes de ambos sexos habían tenido algún evento de intrusión a su privacidad. Al analizar por género (Tabla 3), se encontró que el 41.7% de las mujeres habían sido víctimas de intrusión, en tanto que en el caso de los hombres habían sido víctimas el 35.6%, sin que estas diferencias fueran estadísticamente significativas (p>0.05).

Tabla 3. Análisis bivariado de víctima de intrusión a la privacidad por género.

Victima intrusión	Género		Total
	Femenino	Masculino	
NO	14 8.81%	87 54.72%	101 63.53%
SI	10 6.29%	48 30.19%	58 36.48%
Total	24 15.09%	135 84.91%	159 100%

Pearson chi2(1) = 0.3284 Pr = 0.567

Fuente: elaboración propia

Como se observa en la Tabla 4, existe un número menor de intrusión entre los usuarios con nivel 2 de alfabetización digital (25.79%), en contraste con el 37.74% que tienen nivel 1 de alfabetización digital. Sin embargo, esta diferencia no es significativa (p>0.05), por lo que el nivel de alfabetización digital no se puede confirmar como determinante para ser víctima de intrusión a la privacidad.

Tabla 4. Víctima de intrusión y alfabetización digital.

Victima intrusión	Alfabetización digital Nivel 2	Nivel 1	Total
NO	41 25.79%	60 37.74%	101 63.53%
SI	19 11.95%	39 24.53%	58 36.48%
Total	60 37.74%	99 62.26%	159 100%

Pearson chi2(1) = 0.9627 Pr = 0.327

Fuente: elaboración propia

En el gráfico de la Figura 4 se puede observar como las medidas de seguridad (MS) de los individuos que tienen un nivel 2 de alfabetización digital generan un área mayor que aquellos que tienen un nivel 1.

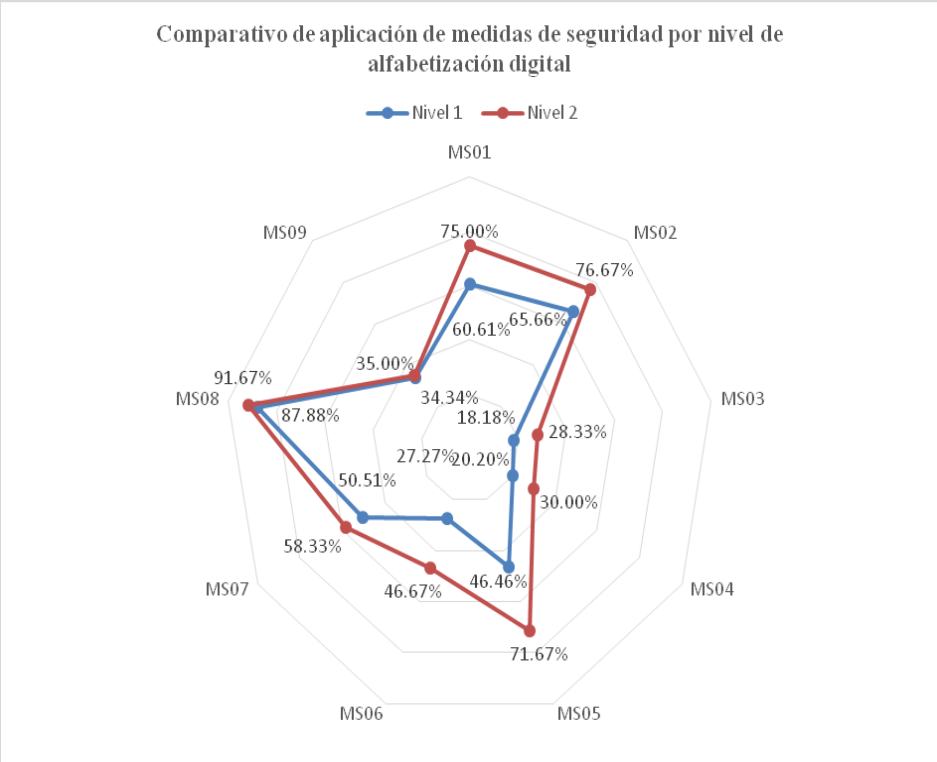

Figura 4. Gráfico comparativo de aplicación de medidas de seguridad por nivel de alfabetización digital.

Fuente: elaboración propia.

Sin embargo, a pesar de realizar mejores prácticas de seguridad y tener un menor número de intrusiones a la privacidad, de acuerdo con análisis de regresión logística de la Tabla 5, el nivel de alfabetización digital no es significativo o determinante para ser víctima de una intrusión.

En la Tabla 5 se puede apreciar las variables significativas del modelo ($p<0.05$), en las que se puede encontrar redes sociales (TICA01), correo electrónico (TICA02), videojuegos en línea (TICA05), aplicaciones de transporte (TICA10), conocer a alguna víctima de intrusión a la privacidad a través de las TIC (CVIP), no desactivar los sensores de los dispositivos (MS09), seguir retos de Internet (CU03) y sentimiento de desconexión (adición a Internet, CU05). Sorpresivamente, el resultado para MS09, si bien significativo, fue débil y en la dirección contraria a la esperada, por lo que debe considerarse con cautela ese resultado y merece mayor análisis.

Tabla 5. Análisis de regresión logística binario multivariado de víctima de intrusión a la privacidad por variables con significancia.

Regresión logística — Observaciones = 159; LR chi2(13) = 35.22; Prob > chi2 = 0.0008; Log likelihood = -86.710453; Pseudo R2 = 0.1688

VIP	Coef.	Std. Err.	z	P>z	[95% Conf.	Interval]
GEN	-0.1928218	0.5180114	-0.37	0.71	-1.208106	0.8224619
EDAD						
18 - 24 años	0.5225258	0.6023588	0.87	0.386	-0.6580758	1.703127
25 - 30 años	0.8392949	0.7055588	1.19	0.234	-0.543575	2.222165
31 - 40 años	1.109756	0.753034	1.47	0.141	-0.3661639	2.585675
TIC01	0.3818203	0.4166213	0.92	0.359	-0.4347424	1.198383
TICA01	1.921795	0.9126283	2.11	0.035	0.1330764	3.710514
TICA02	-1.431812	0.5108727	-2.8	0.005	-2.433104	-0.4305198
TICA05	-1.209117	0.5144663	-2.35	0.019	-2.217453	-0.2007818
TICA10	-1.338907	0.4360381	-3.07	0.002	-2.193526	-0.4842879
CVIP	-1.115816	0.4219668	-2.64	0.008	-1.942856	-0.2887767
MS09	1.051651	0.4315742	2.44	0.015	0.2057809	1.897521
CU03	1.144363	0.5980293	1.91	0.056	-0.0277532	2.316478
CU05	0.7926928	0.4026989	1.97	0.049	0.0034176	1.581968
_cons	-1.253227	1.203318	-1.04	0.298	-3.611687	1.105234

Fuente: elaboración propia.

Para el caso de la regresión cuyos resultados se muestran en la Tabla 6, las razones de momios estiman posibilidad de que algo suceda con respecto a que no suceda, y son útiles para estimar el riesgo en estudios transversales, dado que en este tipo de estudios no se puede determinar causalidad y por lo tanto un riesgo. Es importante recalcar que son razones y no probabilidades las cuales toman valores mayores o menores a 1 incluso pueden ser negativos. Mientras que en el caso de las probabilidades estiman riesgo en valores de 0 a 1.

Se puede apreciar la regresión logística del modelo con las variables significativas para una intrusión a la privacidad donde se observa que las personas con un nivel 1 de alfabetización digital (TIC01) a pesar de no ser una variable significativa, tienen 46% más de posibilidades de ser vulnerados que las personas que tienen un nivel 2 de alfabetización.

Los usuarios que utilizan redes (TICA01) sociales son los más vulnerables teniendo 6.83 veces más posibilidades de ser vulneradas en su privacidad en comparación con los que no las utilizan.

Tabla 6. Regresión logística: razones de momios.

Regresión logística — Observaciones= 159
LR chi2(13)= 35.22
Prob > chi2= 0.0008
Log likelihood = -86.710453 — Pseudo R2= 0.1688

VIP	Odds Ratio	Std. Err.	z	P>z	[95% Conf.	Interval]
GEN	0.8246289	0.4271672	-0.37	0.71	0.2987627	2.276096
EDAD						
18 - 24 años	1.686282	1.015747	0.87	0.386	0.5178468	5.491094
25 - 30 años	2.314734	1.633181	1.19	0.234	0.5806687	9.227284
31 - 40 años	3.033617	2.284417	1.47	0.141	0.6933892	13.27225
TIC01	1.464949	0.6103288	0.92	0.359	0.6474314	3.314753
TICA1	6.833213	6.236184	2.11	0.035	1.142337	40.8748
TICA2	0.2388757	0.1220351	-2.8	0.005	0.087764	0.6501711
TICA5	0.2984607	0.1535479	-2.35	0.019	0.1088861	0.8180909
TICA10	0.2621321	0.1142996	-3.07	0.002	0.1115229	0.6161358
CVIP	0.3276477	0.1382564	-2.64	0.008	0.1432941	0.7491795
MS09	2.862373	1.235326	2.44	0.015	1.228484	6.669339
CU3	3.140439	1.878074	1.91	0.056	0.9726283	10.1399
CU5	2.209338	0.8896978	1.97	0.049	1.003423	4.86452
_cons	0.2855819	0.3436459	-1.04	0.298	0.0270062	3.019931

Fuente: Elaboración propia.

Aquellos usuarios que no bloquean los sensores de sus dispositivos (MS09) tienen casi 3 veces más posibilidad de ser vulnerados. Los usuarios que realizan retos de internet los llamados "*challenges*" (CU3) tienen 3.14 veces más posibilidades de ser vulnerados en su privacidad. Así como aquellos que tienen una adicción al Internet y sufren un sentimiento de desconexión (CU5) al no estar en línea, que tienen 2.20 más posibilidades de sufrir una intrusión que aquellos que no lo tienen.

Así también se observó un efecto protector de las personas que utilizan el correo electrónico (TICA02) con un 77% menos posibilidades de ser vulnerados en su privacidad, 70% menos posibilidades para quienes hacen uso de video juegos (TICA05), 74% menos posibilidades para los usuarios que hacen uso de aplicaciones de transporte (TICA10), quienes

refirieron conocer a alguien que sufrió una intrusión a la privacidad (CVIP) tienen un 77% menos de posibilidades de una intrusión.

Los marginales representan el valor promedio de posibilidad de riesgo que tiene cada variable en el modelo obtenido, encontrándose que todos estos factores contribuyen a la posibilidad de ser vulnerados en nuestra privacidad a través de las TIC. Al obtener los valores marginales del modelo se encontró que efectivamente existe una tendencia a aumentar la posibilidad de ser vulnerado en los grupos de mayor edad.

En la Tabla 7 se confirman las estimaciones a través de los promedios obtenidos para cada variable en el modelo.

Tabla 7. Obtención de los valores marginales del modelo

	Delta–Method					
	dy/dx	Std. Err.	Z	P>Z	[95% Conf.	Interval]
GEN	-0.0355212	0.0953124	-0.37	0.709	-0.2223301	0.1512877
VIP						
18 - 24 años	0.0875034	0.0951325	0.92	0.358	-0.0989528	0.2739596
25 - 30 años	0.1457473	0.116201	1.25	0.21	-0.0820024	0.3734971
31 - 40 años	0.197394	0.1263313	1.56	0.118	-0.0502108	0.4449987
TIC01	0.0703381	0.0760654	0.92	0.355	-0.0787474	0.2194235
TICA1	0.3540287	0.1597953	2.22	0.027	0.0408357	0.6672217
TICA2	-0.2637651	0.0858304	-3.07	0.002	-0.4319896	-0.0955405
TICA5	-0.2227408	0.0887281	-2.51	0.012	-0.3966446	-0.048837
TICA10	-0.2466503	0.0715387	-3.45	0.001	-0.3868636	-0.1064371
CVIP	-0.2055531	0.0717133	-2.87	0.004	-0.3461087	-0.0649976
MS09	0.1937327	0.0744485	2.6	0.009	0.0478163	0.3396491
CU3	0.2108118	0.1056744	1.99	0.046	0.0036939	0.4179298
CU5	0.1460281	0.0709555	2.06	0.04	0.0069578	0.2850983

Fuente: elaboración propia.

Finalmente, el modelo propuesto de acuerdo con la prueba de bondad de ajuste de Hosmer Lameshow explica el 75% de la posibilidad de ser vulnerado en la privacidad para la población encuestada (Tabla 8).

Tabla 8. Prueba de bondad de ajuste del modelo logístico (Hosmer Lameshow)

Modelo logístico para VIP, goodness-of-fit test (Hosmer Lameshow)

(Table collapsed on quantiles of estimated probabilities)

Número de observaciones	= 159
Número de grupos	= 10
Hosmer-Lemeshow chi2(8)	= 5.07
Prob > chi2 = 0.7505	= 0.7505

Fuente: elaboración propia.

5 CONCLUSIONES

En conclusión, se encuentra que, a pesar de realizar mejores prácticas de seguridad y tener un menor número de intrusiones a la privacidad, el nivel de alfabetización digital no es significativo o determinante para prevenir ser víctima de una intrusión. Al estratificar por edad se observó una tendencia a estar en mayor posibilidad de sufrir intrusión cuando se tiene mayor edad, sin embargo, la diferencia entre los grupos no resultó significativa. Es probable que exista un efecto generacional, dada la experiencia nata de las nuevas generaciones en el uso de TIC, pero éste merece ser estudiado en mayor profundidad antes de poder generar conclusiones al respecto.

Cabe mencionar que resulta que algunas de las actividades de estos usuarios de TIC como el correo electrónico, los video juegos, las aplicaciones de transporte y el conocer la experiencia de alguien que ya fue vulnerado en su privacidad a través de las redes, tienen un efecto protector debido a que son actividades que, si bien pueden representar un riesgo por la sensibilidad de la información que se procesa, de alguna manera provocan en el usuario la aplicación de mayor cuidado en la las medidas de seguridad, disminuyendo la posibilidad de ser vulnerado. Este no es el caso para la diferencia del uso de redes sociales, el descuido de la administración de los sensores de los dispositivos de los usuarios, la participación en retos de Internet y la adicción al Internet.

En el caso del efecto protector observado en la mayoría de las actividades significativas y el conocimiento de una víctima de intrusión, este puede deberse a la “inmunidad subjetiva” que, en la codificación de los peligros de acuerdo con la naturaleza de la información, se consideran importantes, aumentando su percepción en el análisis del riesgo. Esto también es aplicable a actividades en redes sociales, aunque también existe la posibilidad de que no se desdeñen los riesgos pequeños o improbables, sino que simplemente no se detecten.

Los resultados obtenidos pueden resultar sorprendentes para algunos, al considerarse un hecho que un mayor nivel de alfabetización digital llevará a un menor nivel de vulnerabilidad. Pero el proceso puede ser más complicado de lo que parece en un principio. La escala de alfabetización de Martin, se basa en competencias digitales y en su aplicación profesional. Correia y Compeau (2017) desarrollaron un modelo de consciencia de privacidad de la información que va mucho más allá de conocer los elementos y las prácticas comunes. Hacen un trabajo detallado para diferenciar los conceptos de conocimiento, alfabetización y conciencia, siendo esta última basada fuertemente en el entendimiento tecnológico y legal, que no necesariamente poseen los usuarios intensivos de TIC, aunque se trate de nativos digitales o profesionales con fuerte orientación a TIC.

Es necesario establecer diferencias claras también entre la vulnerabilidad y los elementos que proveen privacidad de la información dependiendo

del tipo de tecnología y de usuario. Escalas de valores, amenazas intangibles y la ya mencionada inmunidad subjetiva tendrán un impacto directo en el cálculo económico de riesgo, llevando a muy diferentes resultados de comportamiento y vulnerabilidad dependiendo de cada caso y contexto.

Se recomienda establecer más estudios exploratorios que permitan generar un modelo basado en elementos bien identificados, así como sus variables moderadoras. Al tratarse de un fenómeno sociotécnico, esta tarea no se antoja fácil, pero puede lograrse en relativamente poco tiempo con la triangulación adecuada de métodos.

Es importante fortalecer la investigación en este rubro, dados los retos que el advenimiento de la cuarta revolución industrial trae consigo, como consecuencia del desarrollo de la hiper-conectividad y los nuevos modelos de negocio basados en el uso intensivo y ubicuo de los dispositivos electrónicos y las redes (CORREIA & COMPEAU, 2017).

REFERENCIAS

ALBORNOZ, María Belén. Cibercultura y las nuevas nociones de privacidad. *Nomadas*, v. 28, 2016.

BAL, Gökhan. Explicitness of consequence information in privacy warnings: experimentally investigating the effects of perceived risk, trust, and privacy information quality. Proceedings of the Thirty-fifth International Conference on Information Systems. Auckland, New Zealand, 2014.

BECK, Ulrich. La sociedad del riesgo. Barcelona: Paidós, 1998.

BELANGER, France, & CROSSLER, Robert E. Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, v. 35, n. 4, p. 1017-1041, 2011.

CHAUHAN, Sudhanshu; PANDA, Notan Kumar. *Hacking web intelligence*: open source intelligence and web reconnaissance concepts and techniques. Amsterdam: Syngress, 2015.

CORREIA, John., & COMPEAU, Deborah. Information privacy awareness (IPA): a review of the use, definition and measurement of IPA. Proceedings of the 50th Hawaii International Conference on System Sciences. 2017.

DOUGLAS, Mary. La aceptabilidad del riesgo según las ciencias sociales. Barcelona: Paidós, 1996.

FERENSTEIN, Greg. The birth and death of privacy: 3,000 years of history told through 46 images. *The Ferenstein Wire*, 2015. Disponible: <https://medium.com/the-ferenstein-wire/the-birth-and-death-of-privacy-3-000-years-of-history-in-50-images-614c26059e>

GARZÓN VALDÉS, Ernesto. Lo íntimo, lo privado y lo público. México: IFAI, 2012.

INTERNET SOCIETY. Digital footprints: an internet society reference framework | Internet Society. *Internet Society*, 2014. Disponible: <https://www.internetsociety.org/doc/digital-footprints-internet-society-reference-framework>.

KISSEL, Richard L. Glossary of key information security terms. NIST Interagency/Internal Report (NISTIR) - 7298rev2, 2013.

KRUTZ, Ronald L.; VINES, Russell Dean. *Cloud security*: a comprehensive guide to secure cloud computing. Indianapolis: Wiley, 2010.

LAMPKTON, Nancy., & TRIPP, John. A quantitative and qualitative study of Facebook privacy using the antecedent-privacy concern-outcome macro model. Proceedings of the Nineteenth Americas Conference on Information Systems. Chicago, IL, USA, 2013.

LLANO CIFUENTES, Carlos. Los fantasmas de la sociedad contemporánea: compulsiva, permisiva, impersonal, hedonista y anárquica. México: Trillas, 1998.

MARTIN, Allan. Digital literacy for the third age: sustaining identity in an uncertain world. Fifth European Learning in Later Life Conference, 2007 Disponible: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.581.43&rep=rep1&type=pdf&fbclid=IwAR0tZMtmgZqzNYwIJv18rv8QeWmHYT5urMkpepuYgN_gbsSQXQ-C7Ir7rmY>.

MASLOW, A. Conflict, frustration, and the theory of threat. *J. Abnorm. (soc.) Psychol.*, v. 38, p 81-86, 1943.

MONTENEGRO, Silvia. M. La sociología de la sociedad del riesgo: Ulrich Beck y sus críticos. *Pampa*, v. 1, n. 1, p. 117–130, 2005.

O'BRIEN, David; BUDISH, Ryan; FARIS, Robert; GASSER, Urs; LIN, Tiffany *Privacy and cybersecurity research briefing*. Rochester, NY: Social Science Research Network, 2016. Disponible: <https://papers.ssrn.com/abstract=2842801>.

PAVLOU, Paul A. State of the information privacy literature: where are we now and where should we go? *MIS Quarterly*, v. 35, n. 4, p. 977-988, 2011.

PAYTON, Sarah.; HAGUE, Cassie. Digital literacy across the curriculum a Futurelab handbook. Disponible: <www.futurelab.org.uk/>.

RABOTNIKOF, Nora. Público-privado. *Debate Feminista*, v. 18, p. 3–13, 1998.

SANCHO, Carolina. Ciberseguridad. Presentación del dossier/Cybersecurity. Introduction to Dossier. *URVIO - Revista Latinoamericana de Estudios de Seguridad*, v. 0, n. 20, p 8–15, 2017.

SMITH, H. Jeff., DINEY, Tamara., & XU, Heng. Information privacy research: an interdisciplinary review. *MIS Quarterly*, v. 35, n. 4, p 989-1015, 2011.

SOLOVE, Daniel J. Conceptualizing privacy, 2002. Disponible: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103>.

WARREN, S.; BRANDEIS, L. D. The right to privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, Dec., 1890.

XU, Heng., DINEY, Tamara., SMITH, H. Jeff., & HART, Paul. Examining the formation of individual's privacy concerns: towards an integrative view. Proceedings of the Twenty-ninth International Conference on Information Systems. Paris, France. 2008.