¿Des-confianza en línea?: Relaciones entre ciberseguridad y transacciones en línea

El proceso de digitalización de la economía ha tenido un profundo impacto en los sectores de comercio y servicios financieros, brindando una serie de beneficios tanto a las empresas como a los ciudadanos. Frente a este proceso y a la creciente exposición a riesgos en línea ¿cuál es la perspectiva de un usuario típico de Internet sobre la ciberseguridad?, ¿cómo afectan ciertos aspectos sobre ciberseguridad al uso de comercio electrónico y/o servicios financieros en línea? Este estudio permite profundizar en esta línea de investigación, aún poco tratada en la región.

INTRODUCCIÓN

En los últimos años, los sectores de comercio y servicios financieros se han visto fuertemente influenciados por la digitalización de la economía, lo cual ha llevado a la agilización de procesos, la apertura de nuevos mercados, la reducción de costos de transacción y la creación de nuevos productos; en otras palabras, la generación de nuevas oportunidades. Así, el comercio electrónico promueve emprendimientos, creatividad e innovación. Por otra parte, se han venido fomentando soluciones digitales o móviles para generar una mayor inclusión financiera (United Nations Conference on Trade and Development, 2017).

Junto con estos desarrollos y contribuciones de las TIC, es fundamental notar que la creciente demanda por servicios de Internet ha implicado paralelamente un incremento de la exposición a ciertos riesgos. Esto se debe a que los usuarios, ya sea de manera consciente o no, comparten una gran cantidad de información personal, y, en la mayoría de casos, desconocen el uso que se le da. De esta manera, la falta de seguridad en línea se traduce en delitos informáticos o "ciberdelitos", que van desde el recibir correos no deseados (spam) hasta extorsiones o la destrucción completa de sistemas y redes.

Los riesgos en línea constituyen una preocupación creciente, ya que las amenazas y vulnerabilidades podrían frenar la innovación y el avance de la economía basada en Internet. (BID & OEA, 2016). Además, existe una escasa toma de conciencia en este tema, pues hay muy pocas campañas de educación y sensibilización a la población. En general, los usuarios subestiman su exposición al riesgo y sobre-estiman su capacidad y eficacia para el manejo del mismo (J. M. Bauer & Dutton, 2015).

"A pesar de estos desarrollos y contribuciones de las TIC, es fundamental notar que la creciente demanda por servicios de Internet ha implicado paralelamente un incremento de la exposición a ciertos riesgos"

A pesar del contexto descrito, son escasos los estudios empíricos cuantitativos que relacionen estos elementos desde la perspectiva de un **usuario típico** de Internet en la región latinoamericana. En ese sentido, se resalta la importancia de entender más profundamente cómo podrían afectar los diversos riesgos presentes en Internet, así como la preocupación del usuario por su seguridad en línea, a la posibilidad de que este realice transacciones en línea (comercio electrónico y servicios financieros). Por ello, se plantea la siguiente pregunta de investigación: ¿cómo se vinculan ciertos aspectos sobre ciberseguridad con el uso de comercio electrónico y/o servicios financieros en línea? El presente estudio busca responder esta pregunta

para un conjunto de individuos que ya superaron la valla del acceso – usuarios de Smartphone, computadora, redes sociales e Internet – en cinco países latinoamericanos (Argentina, Colombia, Guatemala, Paraguay y Perú), con información del encuesta *After Access 2017*.

Ciberseguridad y transacciones en línea

Debido a las ventajas respecto a las formas tradicionales de realizar transacciones, el comercio electrónico y los servicios financieros en línea han tenido un crecimiento exponencial. Sin embargo, este crecimiento se ha traducido en un conjunto de vulnerabilidades para el usuario, volviéndose potencial víctima de diversos delitos en la red: fraude a través de desvíos de pagos; robo de identidad virtual; *phishing*; virus o *malwares*; robo de propiedad intelectual, entre otros.

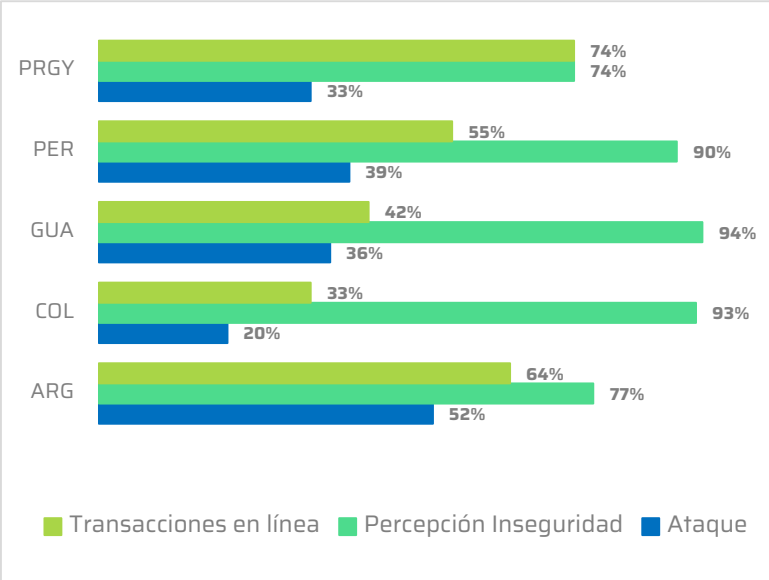
En este contexto, surge el concepto de **ciberseguridad**, en referencia a las tecnologías, procesos y políticas que ayudan al usuario de Internet a prevenir/reducir el impacto negativo de un conjunto de eventos en el ciberespacio.

De esta manera, considerando una revisión de la literatura, se han identificado tres aspectos sobre la seguridad del usuario en la red:

1. Preocupación por la seguridad en-línea
2. El haber sido víctima de un ciberataque
3. El mostrar comportamientos riesgosos

El gráfico 1 presenta una aproximación a los aspectos de seguridad descritos, en cada uno de los países a analizar. En particular, se observa que más de 70% de los usuarios (aquellos que usan Smartphone, computadora, redes sociales e Internet), variando de país en país, siente que la falta de seguridad en Internet es una barrera para su uso. Y, en promedio, 30% y 50% de estos usuarios, respectivamente, han sufrido algún ataque en línea o han realizado alguna transacción en línea.

Gráfico 1: Porcentaje de usuarios de Internet que han realizado algún tipo de transacción en línea*, que se sienten inseguros en Internet, y que han sufrido un ataque en línea



*Aplicación móvil, dinero móvil, banca en línea, compra-venta, o realiza pagos de gobierno
Datos expandidos. Porcentaje respecto a usuarios de Smartphone, computadora, redes sociales e Internet. Fuente: *After Access 2017*.

"Más de 70% de los usuarios (aquellos que usan Internet, redes sociales y computadoras), variando de país en país, siente que la falta de seguridad en Internet es una barrera para su uso"

A partir de los conceptos de ciberseguridad y transacciones en línea, sobre la base de estudios previos, esta investigación prueba empíricamente las siguientes hipótesis:

H1: Existe una relación negativa entre la preocupación por la seguridad del usuario en la red y la realización de transacciones comerciales o financieras

H2: Existe una relación negativa entre ser víctima efectiva de un ciberataque y la realización de transacciones comerciales o financieras

H3: Los usuarios que muestran mayores niveles de comportamientos riesgosos en línea tienden a realizar mayores transacciones comerciales y financieras en línea
H4: Los comportamientos riesgosos aumentan la posibilidad de ser víctima de un ciberataque
H5: Ser víctima de un ciberataque tiende a aumentar la preocupación del usuario por su seguridad en la red
H6: El aumento de la preocupación por la seguridad del usuario tiende a reducir los niveles de comportamientos riesgosos

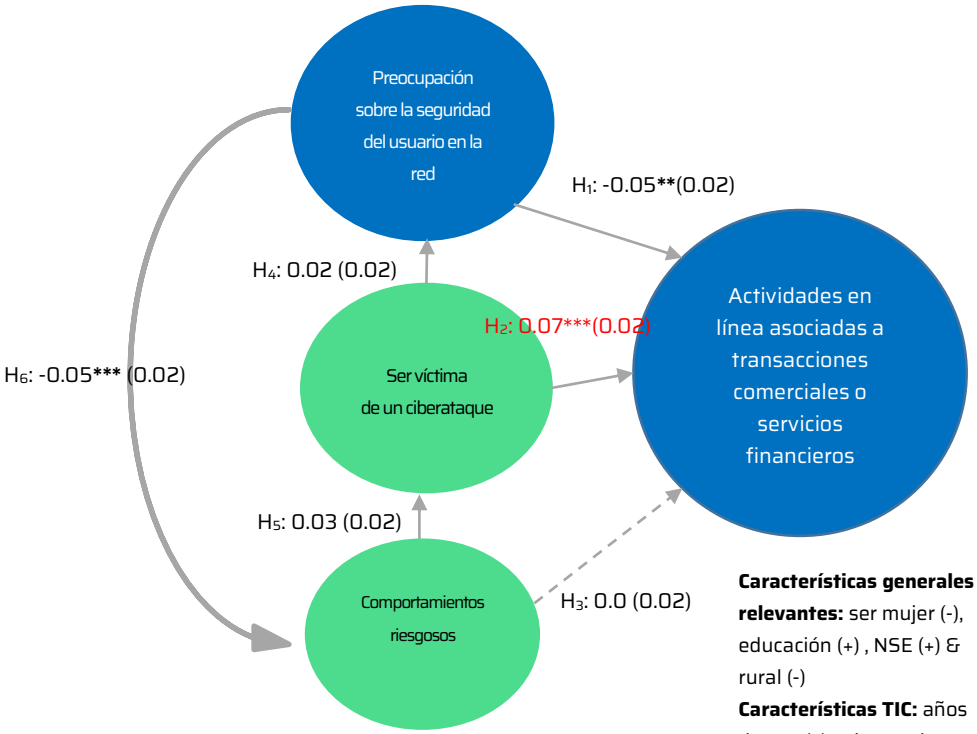
Es importante destacar que las hipótesis o relaciones planteadas, responden a la necesidad de explicar las múltiples interacciones presentes entre los aspectos descritos.

¿Cómo se vinculan ciertos aspectos sobre ciberseguridad con el uso de comercio electrónico y/o servicios financieros en línea?

Mediante una metodología cuantitativa (Ecuaciones Estructurales) que permite analizar diferentes tipos de relaciones entre las variables de un marco teórico de referencia, se estima la magnitud y el signo para cada una de las hipótesis planteadas (Gráfico 2), así como la importancia de otras variables de carácter más estructural (género, edad, nivel educativo, nivel socioeconómico, entre otras).

En primer lugar, el resultado asociado a la H1, resalta la importancia de la percepción de seguridad del usuario en la adopción de transacciones comerciales en línea; el percibir de un ambiente no seguro podría llevar a que el usuario se encuentre menos propenso a brindar la información necesaria para realizar estas transacciones. Por ello, se resalta la importancia de un ambiente virtual seguro si se desea promover y potenciar el uso de este tipo de actividades; el esfuerzo por brindar seguridad en línea no puede darse solo por parte de los dueños de las plataformas, sino también desde el sector público, debido a las propiedades de externalidad positiva que presenta un ciberespacio seguro.

Gráfico 2: Principales resultados de las hipótesis



Errores estándar en paréntesis y asteriscos representan nivel de significancia estadística usual (***p<0.01, **p<0.05, * p<0.01). Fuente: *After Access 2017.* Elaboración propia

Respecto a la H2 (marcada en rojo), su no cumplimiento podría explicarse por una relación de doble sentido existente entre ambos aspectos; si bien un ciberataque podría desincentivar a un usuario de realizar transacciones en línea, es poco probable que un ciberataque ocurra si el usuario no ha hecho uso de este tipo de transacciones. Además, la información disponible solo permite conocer si el usuario ha realizado alguna transacción en línea, y no si la realizó, pero dejó de hacerlo después por algún inconveniente ocurrido (por ejemplo, haber sido víctima de un ataque en línea); así, se complejiza la distinción de los efectos. Esto llama la atención sobre la importancia de continuar con los esfuerzos para la recolección de este tipo información.

Las tres hipótesis siguientes, de la (3) a la (5), muestran el mismo signo que el propuesto inicialmente; sin embargo, la relación no es lo suficientemente fuerte para destacar estadísticamente. Por último, la Hipótesis 6, como se esperaba, indica una relación negativa entre la preocupación por la seguridad y la realización de comportamientos riesgosos en línea.

Conclusiones

El aumento del uso de Internet ha generado un conjunto de beneficios para los ciudadanos en diferentes esferas de sus vidas, desde mayores oportunidades de trabajo y educación; aumento en la eficiencia en comunicación; aumento de transacciones comerciales; hasta la facilitación de la provisión de servicios públicos. Sin embargo, este crecimiento ha venido acompañado por un conjunto problemas asociados a la seguridad en la red.

En ese sentido, los principales hallazgos de este estudio son: (1) la percepción de seguridad por parte del usuario juega un rol fundamental en la adopción de transacciones en línea (comercio electrónico y servicios financieros); usuarios que reportan sentirse inseguros en la red tienden a realizar significativamente menos transacciones en línea. (2) Existe una fuerte relación positiva entre el uso de comercio electrónico y la probabilidad de ser víctima de un ciberataque, mostrando a este grupo de usuarios como más vulnerable a este tipo de delitos. (3) Las usuarias con menor nivel educativo y socioeconómico, así como aquellos que viven en un contexto rural, son los que tienen mayores desventajas en términos de adopción de actividades comerciales en línea.

"... el esfuerzo por brindar seguridad en línea no puede darse solo por parte de los dueños de las plataformas, sino también desde el sector público, debido a las propiedades de externalidades positivas que presenta un ciberespacio seguro"

Referencias

Bauer, J. M., & Dutton, W. H. (2015). The New Cybersecurity Agenda: Economic and Social Challenges to a Secure Internet. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2614545

BID & OEA. (2016). Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? Washington, D.C: Banco Interamericano de Desarrollo; Organización de los Estados Americanos.

United Nations Conference on Trade and Development. (2017). Information Economy Report 2017: Digitalization, trade and development.