Archivos de Criminología, Seguridad Privada y Criminalística
Año 8, vol. 17, Agosto-Diciembre 2021
ISSN: 2007-2023
www.acspyc.es.tl

Medidas de autoprotección en redes sociales. Análisis de los hábitos de los usuarios de Facebook, Instagram y Twitter

Self-Protection Measures In Social Networks. Analysis Of The Habits Of Facebook, Instagram And Twitter Users

Fecha de recepción: 15/10/2020. Fecha de aceptación: 09/01/2021.

Dra. Mariana N. Solari-Merlo
Universidad de Cádiz
mariana.solari@gm.uca.es
España

Resumen

La aceptación generalizada de las redes sociales las ha convertido en uno de los principales espacios de interacción en el ámbito virtual, donde los ciudadanos no sólo se relacionan con los demás sino que comparten información personal sobre diversos aspectos de sus vidas. En este sentido, diversos estudios han analizado la criminalidad que se origina en dichos entornos a la luz de la Teoría de las Actividades Cotidianas, observando especialmente el comportamiento habitual de los propios usuarios en tanto víctimas potenciales de estos delitos. El presente trabajo constituye un estudio empírico de los hábitos de los usuarios en materia de seguridad pero, en este caso, centrado de modo exclusivo en aquellos aspectos que guardan relación directa con la autoprotección y, en concreto, las conductas asociadas a las contraseñas.

Abstract

The widespread acceptance of social networks has made them one of the main spaces for interaction in the virtual sphere, where citizens not only relate to each other but also share personal information about various aspects of their lives. In this sense, various studies have analyzed the crime that originates in these environments in light of the Routine Activities Theory, especially observing the habitual behavior of the users themselves as potential victims of these crimes. The present work constitutes an empirical study of the habits of the users in the matter of security but, in this case, focused exclusively on those aspects that are directly related to self-protection and, specifically, the behaviors associated with passwords.

Palabras clave: Autoexposición online; Cibercriminología; Criminalidad en redes sociales; Teoría de las actividades cotidianas.

Keywords: Online self-exposure; Cibercriminology; Social media crimes; Routine activity theory.

Introducción

La relevancia que el espacio virtual ha adquirido en las sociedades actuales supone que, desde un punto de vista criminológico, no sea posible entender internet como una mera herramienta, como un instrumento más para la comisión del delito. El mundo paralelo o complementario que se genera *online* conlleva su dosis de criminalidad puesto que el fenómeno criminal está presente allí donde hay bienes jurídicos susceptibles de ser atacados. La utilización masiva de internet en todo el mundo y, de modo especial, su uso intensivo suponen la extensión del espacio virtual a diversos aspectos que antes permanecían ajenos a dicho ámbito originándose, en consecuencia, nuevas oportunidades delictivas entorno a los bienes jurídicos que, ahora, son susceptibles de ser atacados a través de estas nuevas tecnologías.

Mayores interacciones *online* suponen la exposición de un número cada vez más amplio de bienes jurídicos. Así, van surgiendo formas de criminalidad en torno a las relaciones sociales, laborales, sentimentales, institucionales, económicas, entre los muchos otros planos en expansión, que tienen su encaje en el modo en que se producen estas relaciones, esto es, según las posibilidades que ofrece el medio y según el propio comportamiento de los individuos. Cada vez que interactuamos *online*, nos hacemos visibles, y esa visibilidad puede suponer una vulnerabilidad. Según el tipo de actividad que realicemos, el medio donde lo hagamos, nuestro propio comportamiento y las precauciones que tomemos, esa vulnerabilidad será mayor o menor pero su existencia surge con la mera interacción.

En este marco, el papel de las redes sociales (en adelante, RRSS) se vuelve especialmente relevante. Las RRSS son plataformas de comunicación a través de internet, un servicio de la sociedad de la información que funciona en base a la información proporcionada por los usuarios y las interacciones que estos realicen. Cada usuario crea un perfil con datos personales que le permitirá interactuar *online* con otros usuarios. El modo de interacción varía en función de la red social, pero en todas ellas la interacción se vuelve un elemento fundamental. Así, al usar estas plataformas, los usuarios no sólo proporcionan información personal de un modo consciente –al crear su perfil o publicar información en el mismo (esto es, generar contenido)- sino que, inconscientemente, al interactuar con terceros van proporcionando información sobre sus gustos, aficiones, ideología, círculo de amistades, etcétera.

En este sentido, el acceso a este espacio de desarrollo de la personalidad sin consentimiento de su titular supone acceder a información privada de conocimiento limitado

que, en ocasiones, puede estar especialmente protegida. Si a esto añadimos el alto nivel de aceptación y utilización por parte de la ciudadanía, debemos concluir que su potencialidad lesiva es de enorme relevancia y que la autoprotección por parte de los usuarios es fundamental para prevenir su victimización.

Marco teórico

La prevención de delitos en el ciberespacio

La prevención de la cibercriminalidad se ha abordado desde diversos enfoques entre los que destaca especialmente el impulsado por la Teoría de las Actividades Cotidianas (en adelante, TAC). Inserta en las teorías de la oportunidad criminal, la TAC analiza el fenómeno criminal desde un postulado básico y es que, para que el hecho delictivo tenga lugar, deben confluir en un mismo espacio un agresor motivado y un objetivo atractivo, sin que haya guardianes capaces de protegerlo (Cohen y Felson, 1979, Cohen *et al.,* 1981).

Desde su primera formulación, diversos autores han desarrollado esta teoría introduciendo elementos complementarios y adaptándola al estudio de diversas formas de criminalidad. En este sentido, destacan especialmente los trabajos que relacionan la TAC con la criminalidad en el espacio virtual (Yar, 2005) puesto que las características de este ámbito –esto es, el entorno y el modo de relacionarse en él- van a condicionar la interrelación de los elementos clave de la TAC.

El tiempo y el espacio, factores fundamentales en la prevención situacional del delito, tienen una consideración diferente en el ciberespacio. Internet es un espacio atemporal, con una actividad ininterrumpida a lo largo del día, los siete días de la semana. Es, asimismo, un espacio altamente cambiante, volátil, donde los entornos de interacción –y los sujetos que en estos interaccionan- también se modifican con relativa frecuencia. Luego, este parámetro fijo que en marca la actividad criminal, necesariamente, adquiere otra dimensión en el espacio virtual y su utilidad para realizar predicciones se ve muy limitada.

Centrándonos en el objeto de interés para el agresor –esto es, el objetivo adecuado-, es coincidente la doctrina en señalar que, en el entorno virtual, todo objetivo puede reducirse a la obtención de información, datos que dan acceso a otros bienes. Así, por ejemplo, la contraseña que da acceso a la cuenta bancaria, una base de datos con información sobre clientes, documentos confidenciales con información de inteligencia o secretos de empresa, entre otros. En el entorno de las RRSS, señalábamos, se observa una peculiaridad puesto que

son los propios usuarios –víctimas potenciales- los que introducen los objetivos en el espacio virtual (Miró Llinares, 2011, pp. 27-28, y 2013) ya que, a diferencia de lo que ocurre en el espacio físico, en el ámbito virtual los bienes expuestos en cada interacción serán únicamente aquellos que guarden relación con la finalidad de dicha interacción, y serán los usuarios quienes, con su actuar, pueden hacerlos adecuados y susceptibles de ser atacados. Esto es, las RRSS constituyen un medio de interrelación por excelencia cuya propia finalidad y modo de funcionamiento son coincidentes con las características que hacen a los objetivos adecuados en el espacio virtual.

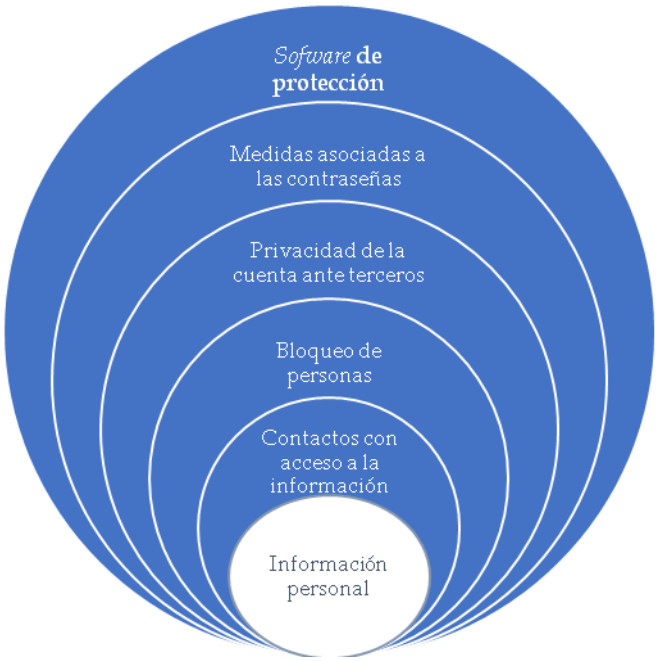
En este sentido, existen dos elementos clave para la prevención de delitos en este ámbito que guardan relación con el modo de utilización de las RRSS y con las medidas de autoprotección establecidas por los usuarios. La forma de relacionarse en RRSS -esto es, el primer elemento- ha sido abordado en diversas ocasiones por las teorías que se centran en el estudio de los estilos de vida (HINDELANG *et al.,* 1978) y, en este sentido, existen numerosos trabajos que estudian el comportamiento de los usuarios de RRSS, especialmente aquellas actividades que supongan una mayor exposición (Miró Llinares, 2013), tales como la publicación de información personal (Reyns *et al.,* 2011, Ngo y Paternoster, 2011), el número de contactos (Choi *et al.,* 2019), la relación con desconocidos (Reyns *et al.,* 2011), el nivel de privacidad de los perfiles, entre otros.

El presente trabajo, en cambio, se centrará en los hábitos relacionados con las medidas de protección establecidas por los propios usuarios, esto es, lo que ha venido a denominarse autoguardianes en los términos que se expondrán a continuación.

La prevención de delitos en RRSS: el papel de los guardianes

Los usuarios de RRSS cuentan con diversos mecanismos de autoprotección a efectos de preservar el acceso no deseado a su información personal, tal y como es expuesto en la Ilustración 1. La forma más efectiva de autoprotegerse es evitando compartir cierto tipo de información –si no hay objeto de interés, no habrá ataques- pero, entendemos, esto resulta opuesto a la intencionalidad de los usuarios al participar en RRSS ya que, aunque este no sea su objetivo, la participación en dichas plataformas supone aceptar, siquiera implícitamente, que su grado de exposición personal aumentará.

Ilustración 1. Guardianes en RRSS



Existen determinadas medidas (guardianes) que los usuarios adoptan para evitar el acceso de terceros a sus sistemas informáticos o cuentas personales. Así, se ha calificado como guardianes técnicos (Choi, 2008, Holt y Bossler, 2009, Ngo y Paternoster, 2011, y van Wilsem, 2013) la utilización de *software*s de protección –antivirus, anti-intrusiones, *firewall*, etc.-, mientras que otras medidas básicas relacionadas con las contraseñas han sido calificadas como guardianes personales, guardián social o autoguardián (Miró Llinares, 2013, p. 11). El empleo de estas medidas suele guardar relación con la prevención de conductas de *hacking* y acceso informático no consentido por parte de personas desconocidas para los usuarios.

Hay otras medidas –guardianes personales, también-, que limitan la aproximación al objeto de interés específicas en las RRSS. Así, los usuarios pueden configurar su red para que la información contenida en la misma sólo sea visible para sus contactos, excluyendo a terceros no identificados. Asimismo, frente a personas conocidas –se requiere un conocimiento mínimo, únicamente es necesario identificar la cuenta del sujeto-, la principales RRSS (Facebook, Instagram y Twitter, entre otras) cuentan con la posibilidad de bloquear a otros usuarios para evitar que el destinatario de esta medida pueda visualizar la información de quien la implementa o ponerse en contacto con este. Y, finalmente, algunas RRSS como

Facebook cuentan con la posibilidad de crear subgrupos entre los contactos, permitiendo al usuario decidir qué información comparte con unos u otros sin que en ningún caso los destinatarios se enteren a qué grupo pertenecen.

Como se representa en la ilustración, la distancia con el objetivo se reduce conforme se supera alguna medida de protección. En este sentido, las tres primeras mencionadas –*software* de protección, medidas asociadas a las contraseñas y privacidad de la cuenta- están orientadas a la protección del individuo frente a cualquier otro usuario de las TICs. En el bloqueo de personas, no obstante, los sujetos se encuentran en un grado más cercano de proximidad puesto que, al menos, el bloqueador deberá conocer al bloqueado y ser capaz de identificar su cuenta en las RRSS. En un nivel más cercano se encuentran los usuarios que son añadidos como contactos, puesto que tienen acceso a su información; en este sentido, constituyen una excepción a la seguridad autorizada por el propio titular de la cuenta. La posibilidad de crear subgrupos de privacidad supone el último recurso con el que cuentan los usuarios para evitar que personas concretas que sí pueden contactar con ellos y conocer algunos de sus datos (por ejemplo, foto de perfil e información básica), puedan tener información más concreta y/o actual de su vida.

En última instancia, los usuarios pueden controlar la información que ellos mismos hacen pública, omitiendo datos que puedan dar acceso a otros bienes protegidos. Entendemos que este tipo de medidas, no obstante, resultan más cercanas a las precauciones a adoptar en el desenvolvimiento habitual en las RRSS –esto es, a las actividades cotidianas- que a la noción de guardián y, en ese sentido, el estudio llevado a cabo se centra en el papel de los guardianes y, entre ellos, en un tipo de medida muy concreta como es la relacionada con la protección que ofrecen las contraseñas de acceso a las cuentas. La información detallada será expuesta en la metodología pero, con carácter previo, es conveniente conocer los antecedentes empíricos que han analizado diversas formas de cibercriminalidad desde el punto de vista de la TAC.

Antecedentes empíricos

Existen diversos estudios que han comprobado la adecuación del modelo planteado por la TAC para explicar la cibercriminalidad. Así, en lo que respecta a las actividades habituales de las víctimas, se ha señalado la relación entre el tiempo pasado *online* y, en particular, el tipo de actividad realizada en el ciberespacio, por un lado, y el ser objeto de victimización, por otro. Holt y Bossler (2009) encontraron que el número de horas pasadas en salas de chat o utilizando mensajería instantánea tiene una relación directa con el riesgo de

sufrir ciberacoso. En el mismo sentido, Marcum *et al.* (2010) destacan esta relación para ciberabuso añadiendo a las anteriores variables la frecuencia e intensidad del uso de RRSS y el envío de email. Ngo y Paternoster (2011) precisan que no cabría hablar tanto de la relevancia del tiempo pasado en el espacio virtual, sino sólo del tiempo pasado realizando actividades que impliquen interacción con terceros; esto es, no sería relevante, por ejemplo, ver vídeos en *YouTube* sino participar en activamente en las RRSS. Así, entre las distintas conductas *online*, Reyns (2015) encontró relevante el realizar reservas, participar en RRSS y publicar información personal toda vez que aumentan el riesgo de sufrir *phishing*, *hacking* o ataques con *malware*. Similares conclusiones hallaron los trabajos de Pratt *et al.* (2010) en relación a las compras *online* y el riesgo de ser víctima de estafas; Miró Linares (2013), para el acoso; Choi *et al.* (2017), para acoso sexual; y Vakhitova *et al.* (2019), para ciberabuso y *ciberstalking*.

En relación a los guardianes, existen pocos estudios al respecto y los realizados, de modo mayoritario, se centran en los mecanismos físicos de protección; esto es, disponer de medios informáticos tales como programas antivirus, de detección de intrusos, *firewall*, etc. En este sentido, Holt y Bossler (2009) y van Wilsem (2013) encontraron que la instalación estos programas no tiene efectos preventivos para los delitos de ciberacoso y *hacking*, mientras que Choi (2008), en cambio, señala su utilidad. Destaca especialmente el trabajo de Ngo y Paternoster (2011) quienes hallaron que la instalación de estos programas se relacionan del modo significativo con los ataques mediante virus y el acoso pero no lo hacen en la dirección esperada, es decir, para reducir las posibilidades de victimización; en su estudio, quienes disponían de estos medios señalaron que habían sido víctimas de estas conductas en más de un 100% y 70% respectivamente; de modo similar, Hutchings y Hayes (2009) en relación a los ataques *phishing*. Otros trabajos han estudiado la efectividad de las habilidades informáticas de los usuarios o las advertencias de los propios sitios *webs* –tales como alertas de fraude o similar-, sin que encontraran relación significativa en ningún caso (Leukfeldt y Yar, 2016; y Whitty, 2019, respectivamente). En este sentido, el trabajo de Baillon *et al.* (2019) señala que la experiencia en sí no es relevante para reducir el riesgo de recibir ataques de *phishing*, debe estar acompañada de información específica sobre el tema. El análisis de las conductas relacionadas con la contraseña, en cambio, no ha tenido un estudio suficiente por parte de la doctrina.

Objetivos

El objetivo de este trabajo es analizar las medidas de protección asociadas a las contraseñas de los usuarios de RRSS y su relación con la victimización por acceso ilícito a las cuentas. En concreto, se pretende determinar las características de la población usuaria de RRSS y las medidas de autoprotección adoptadas para evitar el acceso ilícito a su información. Asimismo, en el caso de acceso ilícito, comparar las características y hábitos de autoprotección de ambas poblaciones

La elección de las RRSS a analizar se hizo teniendo en cuenta su popularidad –el número de usuarios-, su carácter genérico –no específico- y el tipo de interacción más habitual entre sus usuarios. Para determinar la popularidad de las RRSS se tomaron las estadísticas que analizan estos datos a nivel global (Kemp, 2020) y en España (IAB, 2020), descartando aquellas RRSS que no tuvieran una alta representación en ambos estudios. Entre estas, se obviaron las RRSS que constituyen formas de mensajería instantánea –Whatsapp, We chat, QQ, Telegram, entre otras- dado que el contacto entre usuarios que desconocidos es muy restringido. Finalmente, se excluyeron las RRSS temáticas –como LinkedIn- y aquellas que permiten la interacción entre usuarios de modo muy limitado –como YouTube, Pinterest, Reddit y TikTok, entre otros. Así, las RRSS que se analizarán serán Facebook, Instagram y Twitter.

Cada una de estas tres RRSS funciona de modo similar pero no coincidente. En todas, los usuarios deben registrarse proporcionando ciertos datos personales, un nombre de usuario –en Facebook será el nombre proporcionado en los datos personales- e introduciendo una imagen. Estos dos últimos elementos serán los que identifiquen el perfil –la cuenta- de dicho usuario ante el resto de la comunidad. A continuación, es necesario que los usuarios añadan contactos para poder interactuar introduciendo en las opciones de búsqueda de la red el nombre de otros usuarios y enviándoles la correspondiente solicitud de establecer contacto -amistad, en Facebook- o añadiéndolos cuando la red lo permite –seguimiento o *follower* en Twitter e Instagram. Cabe destacar que las propias RRSS facilitan algunas herramientas para la búsqueda de contactos como la exploración a través del propio correo electrónico –se sugieren contactos agendados o a quienes se les ha enviado un email previamente-, las sugerencias basadas en contactos en común y, en caso de tener la red social vinculada a alguna otra, la opción de añadir a los contactos de esta.

Si bien podemos entender, como se ha comentado, que todas las RRSS buscan la interconexión e interacción de sus usuarios, el modo de funcionar de cada una difiere. A lo largo de este trabajo se irán exponiendo las diferencias más destacadas conforme se vaya requiriendo para exponer los resultados obtenidos en las encuestas.

Metodología

Muestra

La encuesta fue autoadministrada por los participantes a través de internet (técnica CAWI, *Computer Assisted Web Interviewing*) utilizando la herramienta de *Google Forms* Para esto, se consideró adecuado compartir la encuesta entre las propias RRSS analizadas a efectos de llegar directamente a sus usuarios, solicitándoles, a su vez, que la volviesen a compartir en sus propios muros o grupos. En este sentido, se trata de un muestreo no probabilístico.

La encuesta estuvo abierta a respuestas durante todo el mes de abril de 2020 aunque, cabe destacar, en los primeros diez días se alcanzó el tamaño de muestra requerido, probablemente debido a la situación de confinamiento vivida a nivel global por la pandemia –COVID 19- y a la capacidad de movilización y de alcanzar a un elevado número de personas que tienen las RRSS.

El tamaño de la muestra es de 384 individuos. Dado que el número de respuestas obtenidas fue mayor, se procedió, por orden de respuesta, a comprobar que las encuestas se habían completado de modo adecuado, eliminando aquellas que no cumplían esta condición y tomando una nueva, también por orden de respuestas, entre las disponibles.

Variables y tratamiento de datos

Las encuestas proporcionan información sobre 16 variables, de las cuales 15 son categóricas (C) y 1 numérica (N).

Utilización de RRSS

La información relativa al uso de las RRRSS se utilizó para principalmente para determinar las características de la población objeto de estudio, y su grado de familiaridad y experiencia con el manejo de las RRSS.

En este sentido, se preguntó en primer lugar por las RRSS utilizadas en la actualidad a través de pregunta de opción múltiple de respuesta donde los usuarios debían señalar las redes utilizadas entre las tres objeto de estudio (V1, C), pudiendo añadir las que estimasen

conveniente en la opción *otros.* Se preguntó también sobre la antigüedad en el ámbito de las RRSS –sólo para las tres objeto de estudio- (V2, C) donde los usuarios debían señalar la antigüedad de la primera cuenta creada, con independencia de que esa cuenta sea utilizada en la actualidad, optando entre las siguientes opciones: *menos de 3 años, de 3 a 6 años, de 7 a 10 años* y *más de 10 años.* Finalmente, los encuestados debieron responder sobre la conexión a la red social desde dispositivos móviles (V3, C) a efectos de determinar el modo de acceso más habitual a la red. En este último caso, junto a las 3 objeto de estudio, se añadió Messenger dado que, si bien es el servicio de mensajería instantánea de Facebook, en los móviles requiere la instalación de una aplicación (en adelante, *app*) diferente. En base a esta información, se obtuvieron dos nuevas variables; por un lado, con la información relativa a la antigüedad en cada red social, se creó la variable de antigüedad máxima en RRSS (V4, C) *menos de 3 años, de 3 a 6 años, de 7 a 10 años* y *más de 10 años*, tomando la fecha más antigua proporcionada para alguna de las 3. - y, por otro, con los datos de las RRSS utilizadas, se configuró la variable relativa al uso de múltiples RRSS (V5, C) -*1, 2, 3* o *más de 3 RRSS*

Guardianes: cambio de contraseña

En el módulo específico relativo a la seguridad se realizaron preguntas relacionadas con el cambio de contraseña y con el acceso de terceros a las cuentas en las distintas RRSS.

Así, en primer lugar, se preguntó sobre la frecuencia del cambio de contraseña (V6, C) donde los encuestados debieron responder, para cada red social, entre opciones que remitían a una frecuencia de cambio graduada entre *Mensualmente*, *Semestralmente*, *Anualmente*, *Alguna que otra vez* y *Nunca*. Para el cruce de variables posterior se simplificó esta variable uniendo las categorías que suponían alguna periodicidad en el cambio –*Mensualmente, Semestralmente, Anualmente*-, permaneciendo las otras dos categorías sin alterar (V7, C)

A continuación, los usuarios debieron señalar si compartían las contraseñas de sus cuentas con otras personas, distinguiendo también por RRSS. Esta pregunta permitió la obtención de dos variables; por un lado, una variable dicotómica relativa a compartir la contraseña (V8, C) –*Sí, No*- y, por otro, la información sobre la persona con quien se comparte la contraseña (V9, C) –*Padre, Pareja, Amigos, Otros.* En esta pregunta fue posible señalar múltiples respuestas.

Se preguntó también por el acceso de terceros a cuentas de las distintas RRSS, con distinción entre acceso consentido y no consentido (V10, C). En el caso de acceso no

consentido, se preguntó si sabían lo que había hecho quien accedió a la cuenta (V11, C) ofreciendo una lista cerrada de respuestas que comprendían *Revisar el perfil, Revisar el perfil de un tercero, Interactuar con amigos del titular de la cuenta (like, comentar, etc.), Publicar en el perfil del titular de la cuenta, Enviar solicitudes de amistad o seguimiento, Hablar o intentar hablar por mensaje privado con otra persona.* Asimismo, se preguntó a estos usuarios si el acceso ilícito les acarreó algún problema (V12, C), debiendo señalar, en caso afirmativo, si tuvo un *Carácter legal* o fue con la *Pareja, Familiares, Amigos, En el trabajo* u *Otros*.

Asimismo, se introdujeron variables de control relativas al género (V13, C), la edad (V14, N) y el nivel de estudios máximo alcanzado (V15, C). La variable relativa a la edad fue categorizada posteriormente (V16, C) para facilitar el cruce con otras variables.

El tratamiento de los datos se realizó con el programa estadístico *Statgraphics Centurion* versión 17.2.07. A efectos de poder medir con mayor precisión la relación entre variables, algunas de ellas fueron consideradas ordinales; así, V2, relativa a la antigüedad (valor mín. para la menor antigüedad), V6, relativa a la frecuencia del cambio de contraseña (valor mín. para la menor frecuencia), y V15 relativa a los intervalos de edad (valor mín. para la menor edad). Una vez creadas estas variables y recodificados los datos, se ejecutó el análisis estadístico.

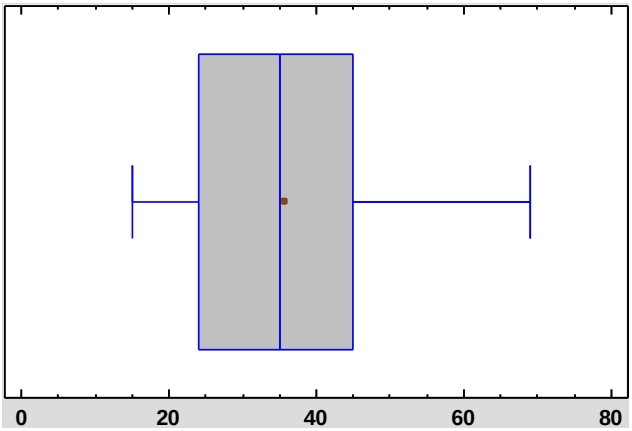
Resultados

Uso de RRSS

Las 384 respuestas obtenidas de distribuyen de forma similar entre mujeres y hombres, con una ligera prevalencia en el primer caso, 51% (N = 194), frente a un 48% (N = 185) en el caso de hombres. 5 sujetos prefirieron no revelar su sexo. En cuanto al nivel de estudios, el 59,6% (N = 229) cuenta con titulación universitaria, el 29,4% (N = 113) tiene un nivel preuniversitario y un 9,4% (N = 36) cuenta con doctorado (1,6%, N = 6, no respondieron a esta pregunta).

La media de edad de la muestra es de 35,8 años (DE = 12,8; Mo = 20; Mín. = 15; Máx. = 69) y, en su distribución por intervalos de edad, destaca el grupo es el de 24 a 32 años (22,7%, N = 87) el grupo con mayor representación situándose el IQR entre los 24 y 45 años.

Gráfica 1. Edad de la muestra



Fuente: elaboración propia.

El test ANOVA -corregido con el estadístico F de Welch, dado que no se cumplía con el supuesto de homocedasticidad o igualdad de las varianzas- señala diferencias en términos estadísticamente significativos, si bien con un efecto medio- $F_{(5;\ 376,13)} = 9,2154$; $p < 0,001$; $\eta^2 = 0,05$. Estas diferencias se dan en todos los grupos (test Games-Howell).

Tabla 1. Perfil de edad por RRSS

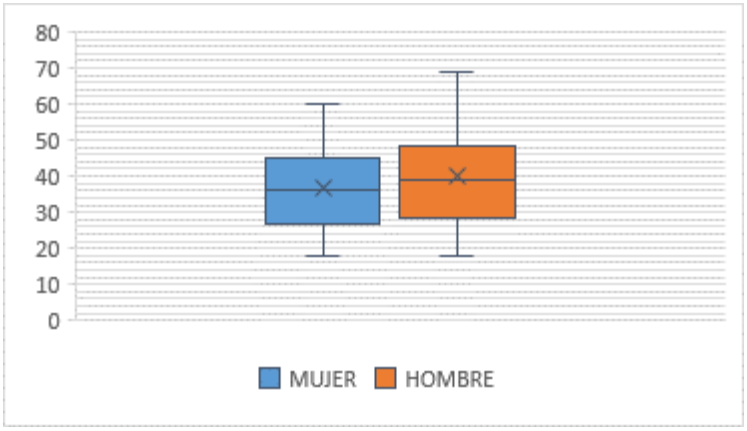
	Facebook	*Instagram*	*Twitter*
		M	*M*
Promedio	6,5 0,1	3 1,4 3,8	3 2,8 6,8
Mediana	6 9	2 8 3	3 0 3
Moda	2 5	2 2 3	2 2 4
Desviación Estándar	0,9 2,7	1 1 2,9	1 1,6 3,5
Mínimo	8 8	1 5 6	1 5 6
Máximo	0 9	5 8 9	5 8 9
Cuartil Inferior	7 7	2 2 3	2 2 5
Cuartil Superior		4	4

5 8	1 2	2 6

Fuente: elaboración propia.

Esto nos ofrece distintos perfiles de usuario en cada red social. Así, en Facebook encontramos son mayoritariamente a mujeres (52,5%, N = 135) que, al igual que los hombres (45,5%, N = 117), muestran una mayor prevalencia para el intervalo de edad comprendido entre los 33 y 41 años (28,9% para mujeres y 28,2% para hombres). Con mayor detenimiento, podemos observar que las usuarias de Facebook son más jóvenes que los hombres, situándose la edad media en los 36,5 años mientras que en estos supera los 40. En relación a la antigüedad de la cuenta, ambos grupos señalan mayoritariamente la opción relativa a una antigüedad de *más de 10 años*, si bien en los hombres tiene una mayor representación respecto del total de respuestas (51,3% frente al 45,9% para las mujeres).

Gráfica 2. Perfil de usuarios de Facebook. Edad y género

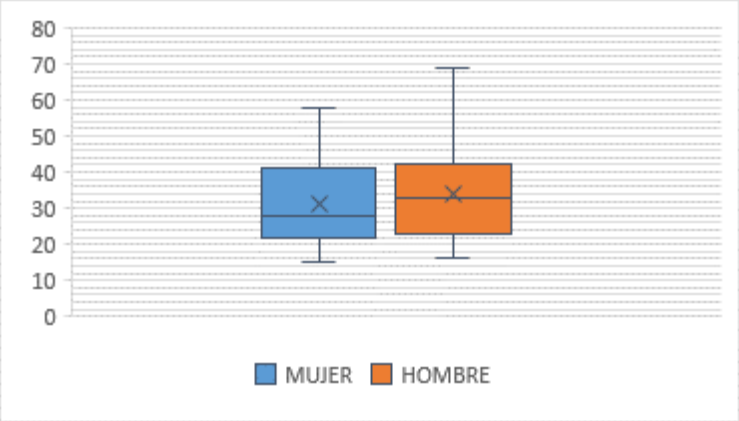


Fuente: elaboración propia.

En Instagram también encontramos una mayoría de mujeres (55,2%, N = 142 frente al 44,8%, N = 115 para los hombres). Al igual que en el caso anterior, la edad de las usuarias es menor que la de los hombres, situándose la media en 31,4 y 33,8 respetivamente. Esto supone, en función de los intervalos realizados, que el relativo a los 24 a 32 años tenga una mayor presentación para las mujeres (27,4%), mientras que para los hombres el más representativo es el de los 33 a 41 años (25,6%). En relación a la antigüedad de la cuenta, la respuesta más frecuente ha sido la de *3 a 6 años* (41,9%, N = 125), seguida por la de *menos de 3 años* (33,6%, N =100); las cuentas de *más de 10 años* suponen apenas un 5,4% (N = 16). Cabe

destacar diferencias en función del sexo que indican que las mujeres tienen una antigüedad ligeramente superior a la de los hombres [$X^2_{(3)} = 8,792$; $p = 0,0322$].

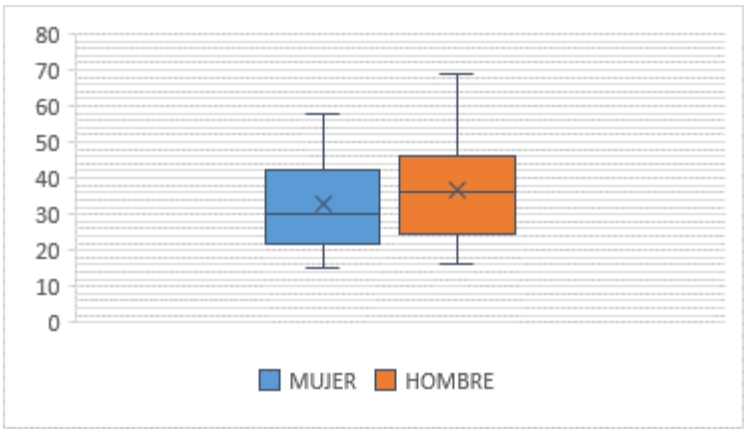
Gráfica 3. Perfil de usuarios de Instagram. Edad y género



Fuente: elaboración propia.

Por lo que respecta a Twitter, encontramos un mayor número de hombres (52,9%, N = 174) con una edad media de 36,8 años. Las mujeres (47,1%, N = 155) tienen una edad media de 32,8 años y presentan una mayor representación para el grupo de edad comprendido entre los 15 y 23 años (29,7%) seguido, en igual medida, por los de 24 a 32 años y 33 a 41 años (24,5% en cada caso). En el caso de los hombres, el intervalo de edad con mayor representación es el de los 33 a 41 años (24,7%), seguido por el de 24 a 32 años (21,3%). En relación a la antigüedad de la cuenta, se aprecia que el grupo más representativo es el comprendido entre los 7 y 10 años (36,9%, N = 134), seguido del de 3 a 6 años (28,7%, N = 104). Cabe destacar que mientras que para los hombres el grupo de menor antigüedad –*menos de 3 años*- es el menos frecuente (12,1%), para las mujeres lo es el relativo a la mayor antigüedad –*más de 10 años*- con un 12,9%. Este último grupo representa para los hombres un 20,7% del total.

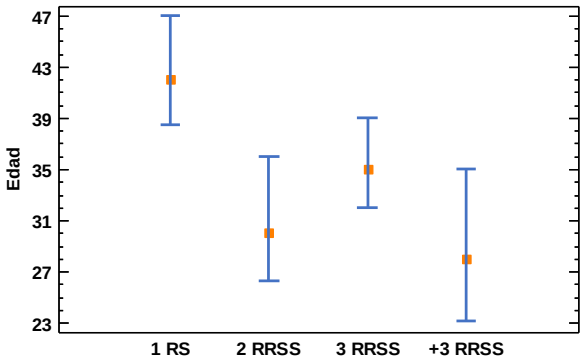
Gráfica 4. Perfil de usuarios de Twitter. Edad y género



Fuente: elaboración propia.

En cuanto al uso de múltiples RRSS, un 19,5% que afirmó utilizar sólo una (N = 75; Facebook = 24, Instagram = 3, Twitter =48), un 34,4% (N = 132) utiliza 2, el 39,6% (N = 152) usa 3, y el 6,5% (N = 25) utiliza más de 3. Tras realizar el test ANOVA con la corrección de Welch, se observó un efecto significativo medio [$F_{(3;\ 380)} = 7{,}93$; $p = 0{,}0001$; $\eta^2 = 0{,}06$] que señala una relación entre esta variable y la relativa a la edad de los usuarios. Esta concordancia se da entre quienes tienen 1 red social y cada uno de los restantes grupos, pero no entre estos grupos entre sí (test Tukey).

Gráfica 5. Multiplicidad de RRSS y edad de usuarios



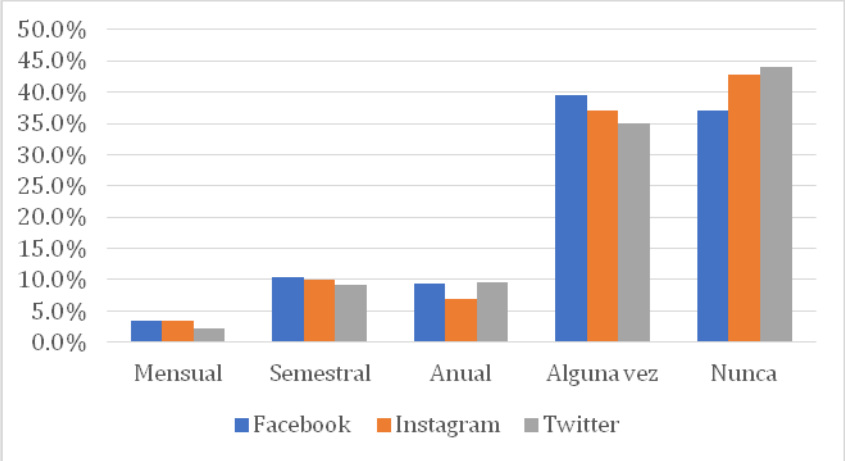
Fuente: elaboración propia.

Finalmente, en cuanto a la forma de conexión, en todas las redes los usuarios señalaron mayoritariamente conectarse desde la correspondiente aplicación para móviles. Así lo han manifestado un 70,5% de usuarios de Facebook, un 88,9% de Instagram y un 88,4% de Twitter.

Autoprotección de la cuenta (autoguardianes)

Como se observa en la Gráfica 6, los usuarios de las 3 RRSS analizadas presentan un comportamiento similar en todas ellas. Mayoritariamente, han señalado que nunca han cambiado la contraseña de la red social (Facebook, 37,1%; Instagram, 42,8%; y Twitter, 44%) o que la han cambiado alguna que otra vez (Facebook, 39,6%; Instagram, 37%; y Twitter, 35%). Las opciones que señalan cierta periodicidad o hábito en el cambio –*Mensualmente, Semestralmente, Anualmente*- suponen en todos los casos –y de modo conjunto- porcentajes que rondan el 20% (Facebook, 23,3%; Instagram, 20,2%; y Twitter, 21%).

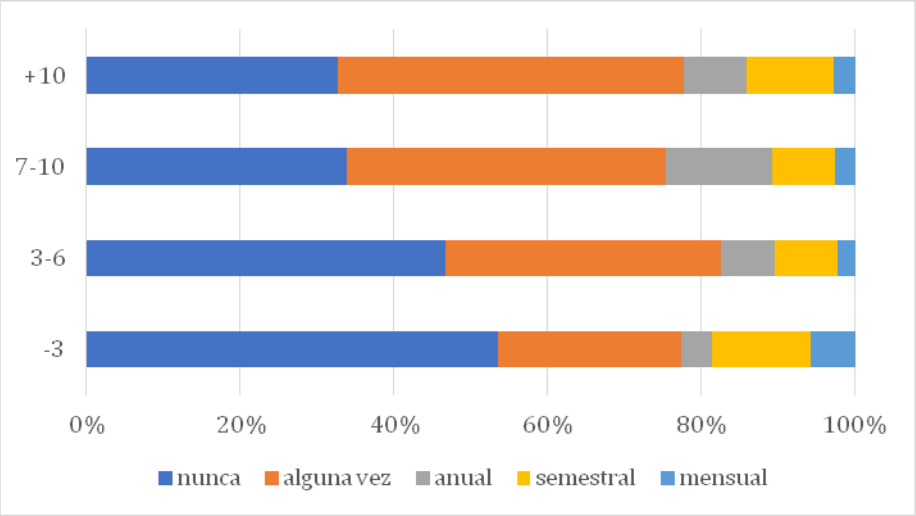
Gráfica 6. Frecuencia de cambio de contraseña por RRSS



Fuente: elaboración propia.

El cruce de variables no ha arrojado resultados significativos para el sexo, la edad o el hecho de tener múltiples redes. La antigüedad del usuario en la red social, en cambio, guarda relación con la frecuencia del cambio de contraseña en todas las RRSS, aunque siempre de un modo débil. Así, Facebook [$r^2_{(206)} = 0,02$; $p = 0,0411$], Instagram [$r^2_{(174)} = 0,05$; $p = 0,0027$] y Twitter [$r^2_{(206)} = 0,06$; $p = 0,0004$].

Gráfica 7. Frecuencia de cambio de contraseña y antigüedad de la cuenta

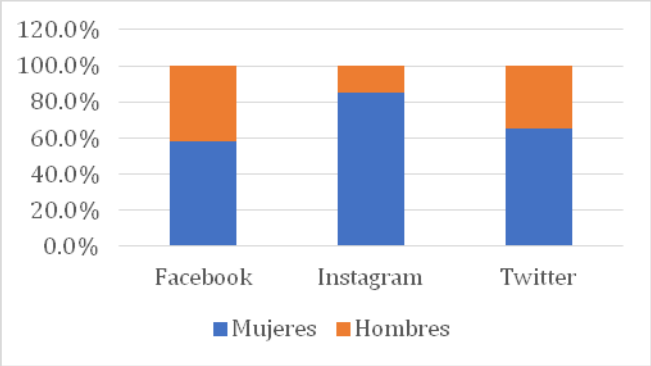


Fuente: elaboración propia.

El 9,6% (N = 37) de los usuarios señala compartir su contraseña con otra persona, porcentaje que se incrementa ligeramente en el caso de las mujeres (10,8% del total de mujeres) y disminuye en los hombres (8,6%).

Según la red social, estas personas representan el 11% del total de usuarios de Facebook, el 6,7% en Instagram y el 5,5% en Twitter, lo que supone una diferencia estadísticamente significativa [$X^2_{(2)}$ = 7,881; p = 0,0194]. La distribución de mujeres y hombres que comparten la contraseña según las distintas RRSS varía significativamente [$X^2_{(5)}$ = 16,869; p = 0,0048]. Así, mientras que en Facebook encontramos una distribución pareja (12% del total de usuarias de Facebook y 10% del total de usuarios masculinos), en Instagram estos porcentajes representan el 10,5% para mujeres y el 2,2% del total de usuarios respectivamente. En Twitter, como se ha visto, el número de sujetos que comparten la contraseña es menor y, entre estos, representan el 7,2% y 3,9% del total de mujeres y hombres, respectivamente. En la siguiente Gráfica 8 se observa la distribución por sexos entre quienes comparten su contraseña en cada red social.

Gráfica 8. Contraseñas compartidas por sexo y RRSS



Fuente: elaboración propia.

A partir de estos datos, se ha podido determinar que prácticamente la totalidad de usuarios que comparte la contraseña tiene cuenta en las 3 RRSS (94,6%) y que, de modo mayoritario, comparten la contraseña sólo de 1 red social (51,4%) o de las 3 (37,1%). Esta distribución, no obstante, cambia en atención al sexo dado que las mujeres obtienen porcentajes similares para compartir la contraseña en 1 o 3 RRSS (43,5%) mientras que los hombres la comparten mayoritariamente en 1 sola red social (66,7%).

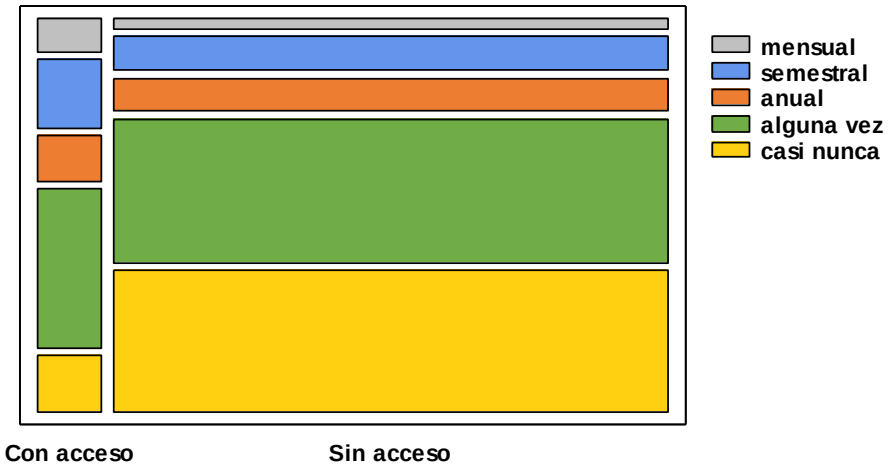
Quienes comparten su contraseña han señalado en mayor medida hacerlo con la pareja (83,8%, N = 31), porcentaje que se eleva hasta el 85,7% de mujeres que comparten su contraseña y se reduce al 81,2% en el caso de los hombres que lo hacen. Las alternativas señaladas fueron *con amigos*, 10,8%, *con los padres*, 5,4%, u *otras opciones* con porcentajes inferiores.

Por otra parte, el 13,5% (N = 52) de los encuestados señaló haber sufrido un acceso no consentido en alguna de sus cuentas, el 9,8% de los cuales afirmó que fue en más de una cuenta. El acceso ilícito se da con mayor frecuencia en cuentas de mujeres (58,8%, N = 30) que de hombres (41,2%, N = 21), representando el 15,5% y 11,4% del total de mujeres y hombres encuestados, respectivamente. Asimismo, es más habitual que tenga lugar en Facebook (10,2% del total de usuarios de la red), seguido de Instagram (3,8%) y, en menor medida, en Twitter (1,7%).

Se ha comparado la frecuencia de cambio de contraseña de los usuarios que señalaron haber sufrido un acceso ilícito con la del resto encontrando diferencias en todas las RRSS, si bien únicamente en Facebook se vuelven significativas en términos estadísticos [$X^2_{(4)}$

= 10,569; p = 0,0319]; en todos los casos se observa una frecuencia superior en el cambio de los primeros respecto de los segundos, lo que podría indicar cierta preocupación por la seguridad.

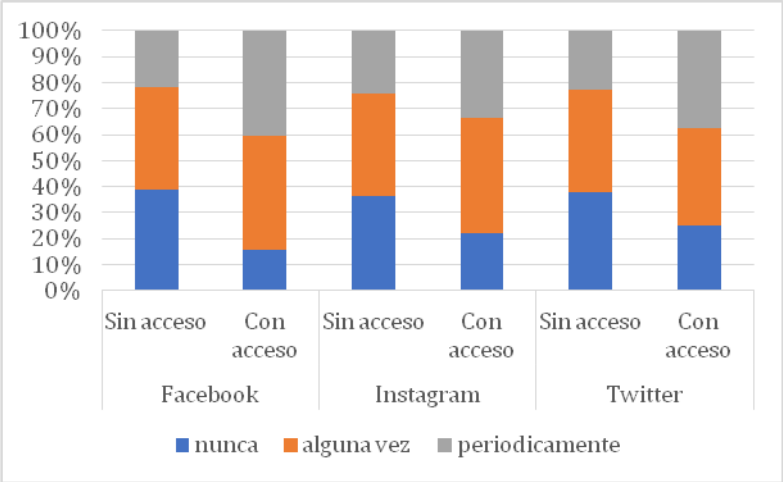
Gráfica 9. Cambio de contraseña en Facebook. Comparativa entre usuarios con y sin acceso ilícito



Fuente: elaboración propia.

Con la comparación en base a la variable de la periodicidad simplificada, V7, estas diferencias entre el comportamiento de los usuarios que han sufrido el acceso ilícito y quienes no han sufrido pueden observarse de un modo más claro. Así, los usuarios que nunca cambiaron su contraseña son menos numerosos en todas las redes en el caso de haber sufrido un acceso ilícito que los que no lo sufrieron con unos porcentajes similares (diferencias del -23,2% en Facebook; -14,1% en Instagram, y -12,9% en Twitter); es decir, con acceso ilícito, es menos habitual no haber cambiado la contraseña nunca. Para la opción de haber cambiado la contraseña alguna vez, los valores aumentan ligeramente para el grupo que sufrió un acceso ilícito (4,2% en Facebook; 4,9% en Instagram; y 1,7% en Twitter). Finalmente, se observa una diferencia más pronunciada en el caso de usuarios que señalaron alguna frecuencia periódica en el cambio de contraseña que arroja valores más elevados para usuarios que sufrieron el acceso (18,7% en Facebook; 14,2% en Instagram; 16,5% en Twitter).

Gráfica 10. Comparativa de frecuencia de cambio de contraseña entre usuarios con y sin acceso ilícito para todas las RRSS



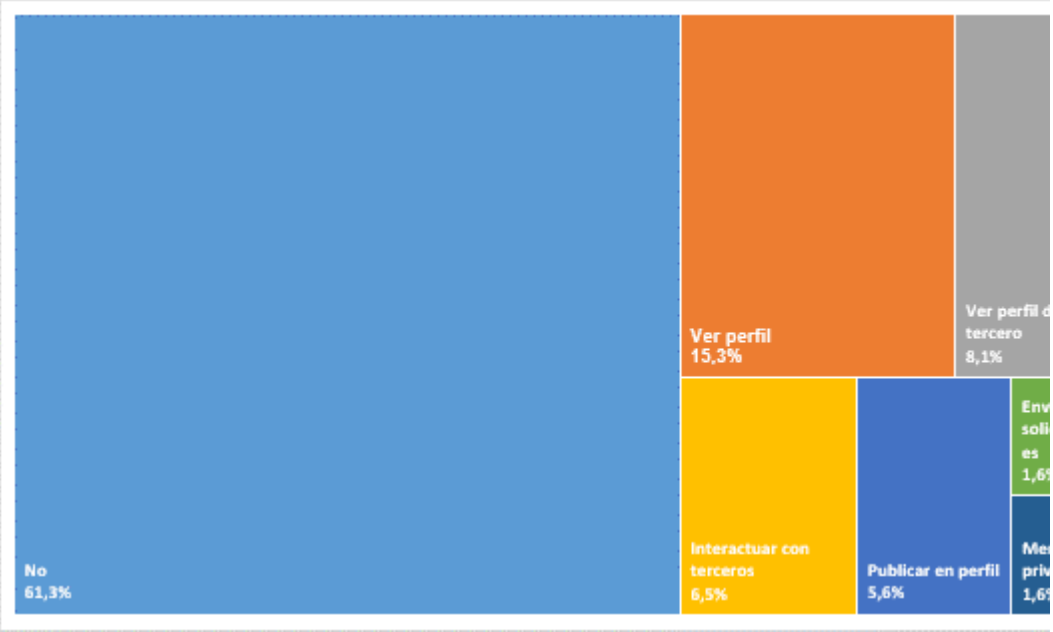
Fuente: elaboración propia.

Cabe destacar que quienes sufrieron acceso ilícito señalaron mayoritariamente no compartir ni haber compartido su contraseña con otra persona (88,9% en Facebook, 95% en Instagram, y 100% en Twitter).

El acceso de un tercero con consentimiento del titular de la cuenta es menos frecuente que el anterior (8,9% del total de sujetos, N = 34) y se da con similar frecuencia en cuentas de mujeres (52,9%, N = 21) y hombres (47,1%, N = 15), representando el 9,3% y 8,6% del total de mujeres y hombres encuestados, respectivamente.

A quienes sufrieron un acceso ilícito se les preguntó si sabían lo que había hecho el intruso en la cuenta. Como se puede ver en la Gráfica 11, los usuarios no suelen conocer esta información, lo cual podría entenderse considerando que, cuando lo saben, las opciones más señaladas son la de revisar el perfil o revisar el perfil de un tercero, esto es, acciones que no requieren interacción con otra persona y, por ende, no dejan un rastro visible o acarrean consecuencias notorias para el usuario, al menos en un primer momento. De hecho, si no tenemos en cuenta a quienes no conocen las acciones del intruso, obtenemos que un 61,3% ha marcado alguna de esas dos respuestas frente al 38,7% que ha señalado alguna de las otras respuestas que requieren una interacción.

Gráfica 11. Actividades realizadas en cuentas ajenas



Fuente: elaboración propia.

Finalmente, un 23,1% de quienes sufrieron un acceso sin consentimiento señalaron que el hecho le acarreó problemas personales, principalmente con la pareja (40%) y, en menor medida, con amigos (26,7%), familiares (13,4%) o en el trabajo (6,7%). Nadie señaló haber tenido problemas legales.

Discusión

Los datos analizados nos remiten a una población de usuarios de RRSS distribuida de modo similar entre mujeres (51%) y hombres (48%), una edad media de 36 años y un intervalo de edad mayoritario entre los 24 y 32 años. En su mayoría cuentan con estudios de nivel universitario (59,6%) o preuniversitario (29,4%). No existen datos a nivel mundial que recojan estos datos, por lo que no podemos realizar comparaciones. En España, no obstante, el último estudio del IAB (2020) analiza estas características en la población usuaria de RRSS en España y señala que se trata principalmente de mujeres (51%), con una edad media de 40 años, con mayor representación para el intervalo de edad comprendido entre los 25 y 54 años (y especialmente entre los 41 y 54), y mayoritariamente titulados universitarios (48%), seguidos de preuniversitarios (36%). Como puede comprobarse, aunque estos dos últimos

valores se asemejan, el presente trabajo presenta una representación mayor de personas jóvenes y tituladas de lo que respecta al total de esta población en España.

Los usuarios de cada RRSS presentan características diferentes de modo estadísticamente significativo. Así, en Facebook e Instagram encontramos una mayoría de mujeres (52,5% y 55,2%) mientras que en Twitter los hombres son mayoritarios (52,9%). Por lo que respecta a su edad, en todas las RRSS las usuarias son más jóvenes que los usuarios pero, en función de las distintas RRSS, es en Instagram donde encontramos la población de menor edad (mediana de edad de 28 para mujeres y de 33 para hombres) y en Facebook los de mayor edad (mediana de 36 para mujeres y 39 para hombres); los valores de Twitter están entre ambos (mediana de 30 para mujeres y 33 para hombres).

En consonancia con la antigüedad de la creación de las propias RRSS, se puede ver que en Facebook –la red social más antigua fundada en 2004- se encuentran las cuentas de mayor antigüedad, superior a 10 años, que, a su vez, tiene una mayor representación de respuestas masculinas para esta categoría; es decir, los hombres señalan tener cuentas más antiguas en Facebook en mayor medida que las mujeres. En Twitter, fundada en 2006, las cuentas tienen una antigüedad de 7 a 10 años con una tendencia hacia la categoría inferior -3 a 6 años- e, igual que en el caso anterior, con cuentas de hombres más antiguas que las de mujeres. Instagram, creada en 2010, presenta una mayoría de cuentas de 3 a 6 años de antigüedad con una tendencia hacia las cuentas de menos de 3 años; en este caso, las cuentas de las mujeres son más antiguas que las de los hombres.

La población de RRSS suele hacer uso de múltiples redes de modo simultáneo. Así, destaca un 39,6% que señaló usar 3 RRSS y un 34,4% que utiliza 2 RRSS. Los usuarios que sólo usan una red social se relacionan de modo significativo con las personas de intervalos de mayor edad, especialmente por encima de los 40 años.

En materia de seguridad, se puede observar que los usuarios no suelen establecer medidas de protección relativas al cambio de contraseña. En todas las RRSS, se respondió mayoritariamente no haber realizado cambios en ninguna ocasión o haberlo hecho de modo aislado; los cambios que remiten a cierta frecuencia o hábito tienen una representación minoritaria que gira en torno al 20%.

Por el contrario, se observa cierta precaución en los usuarios al no compartir su contraseña con terceros de modo mayoritario (90,4%). Las mujeres, y especialmente en Instagram, presentan los valores más elevados entre quienes comparten la contraseña. La

pareja suele ser la persona más habitual con quien se comparte la contraseña, por encima de otras opciones como los amigos o padres. En consonancia con estos datos, sólo un 8,9% señala haber permitido el acceso de un tercero en su cuenta.

Un 13,5% de los usuarios sufrió un acceso ilícito en su cuenta que, de modo mayoritario, se trata de mujeres. En este sentido, la red social señalada con mayor frecuencia es Facebook, seguida, en menor medida, por Instagram y Twitter.

Comparando los hábitos relativos a las contraseñas de quienes sufrieron un acceso ilícito y quienes no lo han sufrido, se puede observar que los primeros presentan valores más elevados de respuestas que refieren cambios periódicos de contraseña o al haberla cambiado, al menos, en alguna ocasión. La información obtenida, no obstante, no permite afirmar que tras el acceso ilícito los usuarios hayan adquirido un hábito que suponga una mayor frecuencia en el cambio de la contraseña. Según los datos, únicamente podemos señalar que el comportamiento de estas dos poblaciones difiere de modo estadísticamente significativo y apunta a una mayor periodicidad en el cambio entre los usuarios que padecieron un acceso no consentido en su cuenta.

En el caso de acceso ilícito, podemos ver que lo habitual es que las acciones del intruso no dejen un rastro visible en la cuenta del titular, siendo la opción mayoritaria no saber lo que este ha realizado o, en el caso de saberse, limitarse esta actividad al consultar el perfil del usuario o, en menor medida, revisar el perfil de un tercero. Opciones como interactuar con terceros o publicar en la cuenta del usurpado -en su nombre- tienen escasa representación. En este sentido, estas acciones no suelen acarrear problemas personales al usuario y, cuando lo hacen, es principalmente con la pareja, amigos o familiares. Los problemas legales no han sido señalados en ninguna respuesta.

Conclusiones

Los datos obtenidos en este trabajo demuestran la poca utilización que los usuarios de RRSS otorgan a una medida de autoprotección de tan sencilla implementación como es la relativa a los cambios de contraseña. Únicamente quienes padecen un acceso ilícito –esto es, una vez que la victimización se ha producido- hacen uso de esta medida de un modo claro. Las otras medidas asociadas a las contraseñas, por el contrario, son utilizadas de modo mayoritario. Así, se ha podido ver que los usuarios no suelen compartir su contraseña con terceros ni permiten a terceros acceder de modo voluntario a sus cuentas.

En este sentido, la información que proporciona este estudio puede ser de utilidad para el diseño de campañas de prevención que fomenten la utilización de dichas medidas de autoprotección. Así, se pueden conocer las carencias donde es necesario incidir y, algo especialmente relevante en la concepción de dichas campañas, el público al que van destinadas, dado que la primera parte de este trabajo contienen las principales características de los usuarios de RRSS y, en particular, de aquellos con los hábitos menos consolidados en esta materia.

Lista de referencias

Alonso García, J. (2015). *Derecho penal y redes sociales.* Cizur Menor: Aranzadi.

Alvarado, R. y Morales, R. (2012*). Cibercrimen*. Guatemala: IUS Ediciones.

Baillon, A. *et al.* (2019). Informing, simulating experience, or both: A field experiment on *phishing* risks. *PLoS ONE 14(12): e0224216.*

Berner, J. E. y Santander, J. (2012). Abuso y dependencia de internet: la epidemia y su controversia. *Revista chilena Neuro-Psiquiat*, *50 (3).* 181-190.

Bossler, A. M. *et al.* (2012*).* Predicting *online* harassment victimization among a juvenile population, *Youth & Society*, 44 (4). 500–523.

Choi, K. S. (2008*).* Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, *2 (1),* 308–333.

Choi, K. S. *et al.* (2017*).* Mobile Phone Technology and *Online* Sexual Harassment among Juveniles in South Korea: Effects of Self-control and Social Learning. *International Journal of Cyber Criminology*, *11 (1),* 110–127.

Choi, K. S. *et al.* (2019*).* Impacts of *online* risky behaviors and cybersecurity management on cyberbullying and traditional bullying victimization among Korean youth: Application of cyber-routine activities theory with latent class analysis, *Computers in Human Behavior, 100*, 1-10.

Clarke, R. V. (1999*).* Hot Products: Understanding, Anticipating and Reducing Demand for Stolen Goods. *Police Research Series*, Paper 112, Policing and Reducing Crime Unit, Research Development and Statistics Directorate. Home Office.

Cohen, L. E. y Felson, M. (1979*).* Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*, 588-608.

Cohen, L. E. *et al.* (1981*).* Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American Sociological Review*, *46*, 505-524.

Eck, J. E. y Clarke, R. V. (2003*).* Classifying Common Police Problems: A Routine Activity Theory Approach. En M. J. Smith y D. B. Cornish (Editores). *Theory and Practice in Situational Crime Prevention. Crime Prevention Studies*, *16*, Nueva York: Criminal Justice Press.

Eurostat (2019*). Acceso a internet en los hogares, 2013 y 2018*. Recuperado de https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals/es#Privacidad_y_protecci.C3.B3n_de_la_identidad_personal_.28encuesta_de_2016.29

Felson, M. y Clarke, R. V. (1998*).* Opportunity makes the thief: practical theory for crime prevention. *Police Research Series*, Paper 98, Policing and Reducing Crime Unit, Research Development and Statistics Directorate. Home Office.

Felson, M. y Eckert, M. A. (2018*). Crime and Everyday Life A Brief Introduction,* 6ª ed.*,* California: SAGE Publications.

Fernández Hermana, L. (2008). *Investigar en tiempos de crisis... y redes*. Madrid: Fundación para el Conocimiento, Madri+d.

Hindelang, M. J. *et al.* (1978*). Victims of personal crime: An empirical foundation for a theory of personal victimization.* Cambridge: Ballinger.

Holt, T. J. y Bossler, A. M. (2009*).* Examining the applicability of lifestyle-routine activities theory for cyber crime victimization. *Deviant Behavior*, *30*, 1-25.

Hutchings, A. y Hayes, H. (2009*).* Routine Activity Theory and *Phishing* Victimisation: Who Gets Caught in the 'Net'?, *Current Issues In Criminal Justice*, *20 (3),* 433-451.

IAB, España. (2020*). Estudio de Redes Sociales 2020*. Recuperado de https://iabspain.es/estudio/estudio-redes-sociales-2020/

Ibrahim, S. (2016*).* Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44-57.

Redondo Illescas, S. y Garrido Genovés, V. (2013*). Principios de Criminología*, 4ª ed. Valencia: Tirant lo Blanch.

ITU (2018*). Measuring the Information Society Report*. Volumen 1. Recuperado de http://www.itu.int/pub/D-IND-ICTOI/es

Kemp, S. (2020*). Digital 2020: Global Digital Overview*. Recuperado de https://datareportal.com/reports/digital-2020-global-digital-overview

Leclerc, B. y Felson, M. (2016*).* Routine Activities Preceding Adolescent Sexual Abuse of Younger Children. *Sexual Abuse: A Journal of Research and Treatment*, *28 (2),* 116-131.

Leukfeldt, E. R. y Yar, M. (2016*).* Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37 (3),* 263-280.

Marcum, C. D. *et al.* (2010*).* Potential factors of *online* victimization of youth: An examination of adolescent *online* behaviors utilizing routine activity theory. *Deviant Behavior*, *31 (5)*, 381-410.

Mclaughlin, E. (2006*).* Routine Activities Theory. En Eugene Mclaughlin y John Munice (Editores). *The Sage Dictionary of Criminology.* Londres: SAGE Publications.

Medina Ariza, J. (2013*). Políticas y estrategias de prevención del delito y seguridad ciudadana*. Madrid: Edisofer.

Miró Llinares, F. (2011*).* La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *RECPC* 13-07.

Miró Llinares, F. (2013*).* La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio. REIC, 5 (11), 1-35.

Monasterio Astobiza, A. (2018). Internet y cognición social. *Revista de Humanidades*, *33*, 115-130.

Navarro, J. N. y Jasinski, J. N. (2012*).* Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum*, *32 (1),* 81–94.

Newman, G. R. y Clarke, R. V. (2003*). Superhighway Robbery: Crime Prevention and E-commerce Crime (Crime Science Series).* Cullompton: Willan.

Ngo, F. T. y Paternoster, R. (2011*).* Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5 (1),* 773–793.

Ortiz López, P. (2010). Redes sociales: funcionamiento y tratamiento de la información personal. En Martínez Martínez, R. y Rallo Lombarte, A. *Derecho y redes sociales.* Madrid: Civitas.

Papastylianou, A. (2013). Relating on the Internet, Personality Traits and Depression: Research and Implications. *The European Journal of Counselling Psychology*, *2 (1)*, 65–78.

Torregrosa, F. J. y López, R. M. (2016). Redes sociales y personalidad: una revisión sistemática. *Behavior & Law Journal*, *2 (1),* 11-41

Pratt, T. C. *et al.* (2010*).* Routine *Online* Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, *47 (3),* 267-296.

Reyns, B. W. (2015*).* A routine activity perspective on *online* victimisation. *Journal of Financial Crime*, *22 (4),* 396 – 411.

Reyns, B. W. *et al.* (2011*).* Being Pursued *Online*: Applying Cyberlifestyle-Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, *38 (11),* 1149-1169.

Stodt, B. *et al*. (2018). Investigating the Effect of Personality, Internet Literacy, and Use Expectancies in Internet-Use Disorder: A Comparative Study between China and Germany. *Int. J. Environ. Res. Public Health*, *15*, 579

Vakhitova, Z. I. *et al.* (2019*).* Lifestyles and routine activities: Do they enable different types of cyber abuse? *Computers in Human Behavior*, *101*, 225–237.

van Wilsem, J. (2013*).* 'Bought it, but never got it': Assessing risk factors for *online* consumer fraud victimization. *European Sociological Review*, *29 (2),* 168-178.

Whitty, M. T. (2019*).* Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26 (1),* 277-292.

Yar, M. (2005*).* The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, *2*, 407-427.

Ybarra, M. L. y Mitchell, K. J. (2008*).* How risky are social networking sites? A comparison of places *online* where youth sexual solicitation and harassment occurs. *Pediatrics*, *121 (2)*, 350-357.