IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

**Monográfico «Ciberdelincuencia y cibervictimización»**

ARTÍCULO

# Actividades cotidianas de los jóvenes en Internet y victimización por *malware*[*]

Natalia-García Guilabert
Centro Crímina para el Estudio y Prevención de la Delincuencia
Universidad Miguel Hernández

Fecha de presentación: abril de 2016
Fecha de aceptación: mayo de 2016
Fecha de publicación: junio de 2016

**Resumen**
En los últimos años se ha experimentado un crecimiento exponencial de *malware* o programas maliciosos que circulan a través de la Red y, sin embargo, poco se sabe acerca del alcance que tiene esta forma de cibercriminalidad entre la población juvenil y de los factores de riesgo asociadas a la misma. Para conocer más acerca de estos dos extremos se ha realizado un estudio con una muestra de 2.038 estudiantes de entre 12 y 18 años de la provincia de Alicante. Los resultados muestran que el *malware* es uno de los principales riesgos a los que están expuestos los jóvenes y que la probabilidad de sufrirlo viene determinado también por las actividades que realizan día a día en Internet.

**Palabras clave**
cibervictimización, jóvenes, *malware*, actividades cotidianas

**Tema**
Criminología

* El presente artículo ha sido realizado en el marco del proyecto de investigación «CiberApp: estudio sobre las distintas formas de violencia que sufren los menores de la provincia de Alicante a través de las nuevas tecnologías de la información y las comunicaciones», financiado por la Diputación provincial de Alicante (DIPU 1.13 CM) y llevado a cabo en el Centro Crímina para el Estudio y la Prevención de la Delincuencia de la Universidad Miguel Hernández (<http://crimina.es/lineas-de-investigacion>).

# *Everyday activities of young people on the internet and malware victimization*

***Abstract***

*In the last few years, an exponential growth of malware circulating through the Net has been experienced. However, not much is known about the extension of this form of cybercrime among young people and risk factors which are associated with it. In order to learn more about these two extremes, a research has been carried out, with a sample of 2,038 students from the province of Alicante, whose ages range from 12 to 18. The results show that the malware is one of the main risks to which young people are exposed, and the probability of suffering is also determined by the activities which are carried out on the Internet on a daily basis.*

***Keywords***

*cybervictimization, young people, malware, routine activities*

***Topic***

*Criminology*

## Introducción

La cibercriminalidad es un fenómeno en constante evolución que afecta a prácticamente a la totalidad de los usuarios de Internet. Una de las formas más comunes y a la que están expuestos la mayoría de los usuarios es el *malware*, también conocido como códigos maliciosos (Martín *et al.*, 2015; pág. 1). Solo durante el año 2014 se crearon más de 317 millones de nuevos códigos maliciosos (virus, gusanos, troyanos, etc.), lo que supone casi un millón de amenazas lanzadas al ciberespacio cada día (Symantec Corporation, 2015, pág. 7).

Gran parte de estos ataques no suelen suponer un riesgo directo para los usuarios, pero no hay que descuidar que, tras su aspecto poco lesivo, más allá de las molestias que ocasionan en el buen funcionamiento del sistema informático, suelen perpetrarse con la intención de recopilar información confidencial del usuario, controlar el equipo de forma remota para realizar más ataques o dañar el equipo (INTECO, 2007; Holt y Bossler, 2013). Dicho de otro modo, introducir estos programas en los ordenadores, tabletas o móviles es, en muchos casos, el paso previo para la realización de otros ataques que conllevan un mayor daño económico y social para los usuarios (Miró, 2012). Sirvan como ejemplo algunos troyanos bancarios que, cuando logran acceder al sistema, permanecen inactivos hasta que el usuario entra en la página web de su cuenta bancaria, momento en el que se activa y captura la información de acceso a la cuenta, que le servirá al *hacker* para, posteriormente, acceder y transferir el dinero a otra cuenta. O también los programas *ransomware* que han aumentado en la actualidad y cuya misión es cifrar la información que se encuentra en el sistema informático y, a continuación, pedirle al usuario una suma de dinero (un rescate) para que pueda recuperarla.

Lograr prevenir estas formas de ataque debe ser, por tanto, una prioridad. Hasta la fecha, la mayoría de los esfuerzos en este sentido se han centrado principalmente en la creación de programas antivirus y en concienciar a los usuarios para su uso (Martín *et al.*, 2015; pág. 1). No obstante, puede ser fundamental para su prevención, además de conocer cómo funcionan los códigos maliciosos, comprender el papel que desempeña el usuario en su producción, de acuerdo con los últimos estudios que ponen el acento en que ser víctima en el ciberespacio viene determinado, en buena parte, por el comportamiento de los propios usuarios (Bossler y Holt, 2009; Choi, 2008; Holt y Bossler, 2013; Hutchings y Hayes, 2009; Leukfeldt, 2015; Leukfeldt y Yar, 2016; Marcum, Ricketts, y Higgins, 2010; Miró, 2013; Ngo y Paternoster, 2011; Pratt, Holtfreter, y Reisig, 2010; Reyns, 2010, 2013, 2015; Reyns y Henson, 2015; Wilsem, 2011; Yucedal, 2010). Por todo ello, por tratarse el *malware* una de las formas más habituales de victimización y para comprender el efecto del comportamiento del propio usuario en su producción, el presente estudio tiene como objetivos conocer, en primer

lugar, el alcance de la prevalencia de victimización de *malware* entre la población juvenil y, en segundo, determinar qué actividades de las que realizan los jóvenes de manera cotidiana en Internet inciden en la probabilidad de sufrirlo.

# 1. Marco teórico

## 1.1. Uso de los menores de las tecnologías de la información y la comunicación

Según los datos del Instituto Nacional de Estadística (2015) más del 85% de los jóvenes hace uso de Internet a partir de los 10 años, alcanzado el 99% cuando sobrepasan los 15 años. Se trata de un sector de la población que ha crecido rodeado de tecnología y que, por ello, domina el lenguaje digital. Prensky (2001) les bautizó con el término de «nativos digitales» para distinguirlos de aquellas personas que tuvieron que migrar al mundo digital y aprender un lenguaje nuevo, una nueva forma de comunicación. Pero lo cierto es que las tecnologías de la información y la comunicación (en adelante TIC) forman parte de la vida cotidiana de los jóvenes y no tan jóvenes, por lo que es más interesante diferenciar a los usuarios entre «visitantes» y «residentes». Esta terminología acuñada por White y Le Conu (2011) se emplea para diferenciar a los usuarios en función de cómo conciben Internet. Para los primeros, los visitantes, Internet es una herramienta más para desarrollar una tarea y se conectan con un objetivo concreto (comprar una entrada, buscar un restaurante, leer el periódico...). Para ellos el mundo virtual y el mundo físico son dos espacios diferentes. En cambio, los residentes viven en Internet y no son capaces de separar ambos espacios; para ellos es un lugar de encuentro con amigos y familiares, un lugar donde expresar sus sentimientos y emociones como si fuera el espacio físico (Hernández, Ramírez-Martinell y Cassany, 2014). Así, los visitantes no suelen tener perfiles y cuidan su privacidad, mientras que los residentes realizan mucha actividad, cuidan su imagen digital y desarrollan ideas y contenidos constantemente.

Es lógico pensar que los denominados «residentes» estarán más expuestos a la cibercriminalidad en la medida que tienen más actividad en el ciberespacio. Este enfoque concuerda perfectamente con los postulados de la teoría de las actividades cotidianas (TAC), formulada por Cohen y Felson a finales de los años setenta, para explicar cómo tras la Segunda Guerra Mundial, los cambios teológicos y, derivados de ellos, los cambios sociales, modificaban los hábitos y las actividades cotidianas de las personas, lo cual, a su vez, creaba entornos de oportunidad para cometer delitos (Cohen y Felson, 1979). Esta misma argumentación sirve para tratar de explicar cómo las TIC, y más que estas, las actividades de los usuarios a través de ellas, generan oportunidades para realizar cibercrímenes, como se verá a continuación.

## 1.2. Factores de riesgo de la cibervictimización a partir de la teoría de las actividades cotidianas en el ciberespacio

Algunos autores han explicado cómo los cambios tecnológicos han favorecido la aparición de la cibercriminalidad, al facilitar el encuentro del delincuente potencial con un mayor número de objetivos y víctimas adecuadas, en ausencia de un guardián capaz (Grabosky, 2001; Miró, 2011; Yar, 2005; Yucedal, 2010). Otros, en cambio, se han centrado en identificar de manera empírica, con mayor o menor acierto, cada uno de los elementos que conforman el triángulo del delito (agresor, víctima/objetivo y guardián) (Bossler y Holt, 2009; Choi, 2008; Holt y Bossler, 2013; Hutchings y Hayes, 2009; Leukfeldt, 2015; Leukfeldt y Yar, 2016; Marcum *et al.*, 2010; Miró, 2013; Ngo y Paternoster, 2011; Pratt *et al.*, 2010; Reyns, 2010, 2013, 2015; Reyns y Henson, 2015; Wilsem, 2011; Yucedal, 2010). Estos autores no llegan a un acuerdo sobre cómo deben ser conceptualizados y medidos los elementos de la TAC en el ciberespacio (García-Guilabert, 2014), pero de sus estudios se puede obtener una serie de factores que pueden ser considerados de riesgo en la medida en que incrementan la posibilidad de convertirse en víctimas en el ciberespacio. A su ver, todos los factores de riesgo pueden ser agrupados de acuerdo con las características que hacen a un objetivo adecuado en el ciberespacio.

Así, el primer grupo de factores puede relacionarse con la visibilidad del usuario en Internet. Algunos autores defienden que en el ciberespacio, como así entendía Felson (1998) para el espacio físico, hay más probabilidad de convertirse en un blanco potencial para el delincuente cuanto se es más visible (Miró, 2011; Leukfeldt, 2015; Yar, 2005). De acuerdo con el planteamiento de Miró (2011; 2012), para hacerse visible en el ciberespacio hay que interaccionar, y esto es concretamente para sufrir un ataque de *malware*: descargar videojuegos, música y películas (Choi, 2008; Leukfeldt, 2015), abrir cualquier archivo adjunto o enlaces recibido por correo electrónico o mensajería instantánea (Choi, 2008), tener amigos que consuman pornografía en línea, compartir con otra persona archivos piratas (Bossler y Holt, 2009), hacer reservas por Internet, usar las redes

sociales (Reyns, 2015) y comprar por Internet (Leukfeldt, 2015). Estas mismas acciones también han sido relacionadas con otras formas de cibercriminalidad económica como el fraude, *phishing* o el robo de identidad (Ngo y Paternoster, 2011; Pratt *et al.*, 2010; Reyns, 2013; Reyns y Henson, 2015).

Otros factores de interacción en el ciberespacio que han sido relacionados con distintas formas de cibevictimización y cuya relación con el *malware* puede ser interesante de comprobar son: hacer uso de la banca electrónica (Hutchings y Hayes, 2009; Reyns, 2013); hacer uso de herramientas de comunicación como los foros (Wilsem, 2011), el correo electrónico y la mensajería instantánea (Reyns, 2013); acceder a los archivos o cuentas de otras personas sin permiso previo (Ngo y Paternoster (2011), y contactar con personas desconocidas (Marcum *et al.*, 2010; Misha *et al.*, 2012; Mitchell, Wolak y Finkelhor, 2008; Reyns, 2010; Sengupta y Chaudhuri, 2011; Vandebosch y Van Cleemput, 2009).

El segundo bloque de factores están relacionados con la idea de introducir en el ciberespacio bienes personales. Son considerados prácticas de riesgo porque sólo cuando son introducidos en el ciberespacio pueden estar disponibles para ser atacados. Así, postear información personal se ha relacionado con el riesgo de sufrir *malware* (Reyns, 2015) y con otras formas de victimización (Marcum, 2008; Marcum *et al.*, 2010; Miró, 2013; Patchin y Hinduja, 2010; Reyns, 2010; Reyns y Henson, 2015). Pero además de cederla voluntariamente, el hecho de tener en el ordenador o móvil información personal (fotos, archivos con contraseñas, etc.) también es un riesgo (Miró, 2013).

El tercer grupo de factores identificados en la literatura científica, relacionados con la probabilidad de cibervictimización, son los que tienen que ver con elementos que los usuarios incorporan (o, en este caso, que no incorporan) a sus sistemas para autoprotegerse de los ataques, como son los programas antivirus, antiespías, cortafuegos, etc. (Choi, 2008; Yucedal, 2010).[1] También hacer una mala gestión de las contraseñas, como facilitarlas a otros, usar siempre la misma o no cambiarlas con frecuencia (Miró, 2013). Estas prácticas han sido identificadas por algunos autores como elementos del «guardián capaz» (Choi, 2008; Bossler y Holt, 2009; Ngo y Paternoster, 2011) y, sin embargo, como han defendido otros autores, es un elemento del objetivo adecuado en tanto que son actividades que hace la propia víctima para protegerse (Miró, 2011; Leukfeldt, 2015). Cabe señalar en este sentido una sutil pero importante diferencia entre la autoprotección y la vigilancia que experimentan los menores por parte de quienes tienen la capacidad para protegerlos en el ciberespacio, como pueden ser los padres, educadores o cualquier otra persona cercana que con su actividad cotidiana pueda protegerla (Grabosky, 2001). Además, el menor puede facilitar con su actuar ser más o menos vigilado por sus guardianes y, por consiguiente, estar más o menos protegido. Así, los padres pueden hacer un control directo mediante el uso de sistemas de control parental o estableciendo normas respecto al uso de los dispositivos, pero también los menores pueden favorecer el control compartiendo con ellos los dispositivos o agregándolos a los perfiles de redes sociales (García-Guilabert, 2014).

## 2. Método

### 2.1. Participantes

El estudio ha sido realizado con una muestra compuesta por 2.038 estudiantes de educación secundaria y bachillerato de la provincia de Alicante. Respecto a la edad y sexo de los participante, el 50,5% (n = 1.029) son hombres y 49,5% (n = 1.009) son mujeres, con edades comprendidas entre los 12 y los 18 años; la edad media es de 14,6 años (D. T.=1,72). Asimismo, se distribuyen de manera equitativa entre los cuatro cursos de educación secundaria obligatoria y los dos de bachillerato, como se muestra en la tabla 1.

**Tabla 1. Distribución de los participantes por curso.**

| CURSO | n | % |
|---|---|---|
| 1º ESO | 382 | 18,7 |
| 2º ESO | 381 | 18,7 |
| 3º ESO | 384 | 18,8 |
| 4º ESO | 387 | 19 |
| 1º BACH. | 356 | 17,5 |
| 2º BACH. | 148 | 7,3 |
| Total | 2038 | 100 |

1. Aunque no en todos los estudios ha resultado ser un factor de riesgo (Ngo y Paternoster, 2011; Leukfeldt, 2015).

## 2.2. Variables

### 2.2.1. Dependiente

Se ha incluido como variable dependiente la victimización por *malware*. Se trata de una variable cuantitativa, que hace referencia a si los sujetos de la muestra han sido alertados por el antivirus de la existencia de algún virus en sus dispositivos (*¿El antivirus te ha avisado alguna vez de que tenías algún virus?*). La variable fue transformada en una variable cualitativa nominal con dos categorías, de modo que los sujetos que contestaron que fueron alertados al menos en una ocasión fueron categorizados como «víctimas», mientras que los que contestaron «nunca» fueron categorizados como «no víctimas».

### 2.2.2. Independientes

Se incluyeron un total de veintiuna variables independientes, tanto de naturaleza cualitativa nominal, con dos categorías de respuesta, como de naturaleza numérica.[2] A su vez, las mismas son agrupadas en cuatro categorías haciendo referencia a las actividades cotidianas de los menores en Internet y al control de su actividad por parte de los padres:

- Visibilidad. Esta categoría reúne todas las variables independientes que hacen referencia a la interacción; en otras palabras, a las actividades que realiza un usuario en el ciberespacio y que lo hacen más visible. Concretamente, se incluye el número de archivos que descargan a la semana, el tipo de medio que usan para realizarlo (programas P2P como Jdownloader, Emule, Torrent, etc., o directamente desde páginas web como mega, seriespepito, desdeunlugarmejor.com, rapidshare, etc.), el tipo de programas que descargan (juegos, software, pornografía, música, películas y aplicaciones), si alguna vez han abierto enlaces o descargado archivos enviados por desconocidos, el número de veces que han contactado con desconocidos a través de Internet y hacer uso de diferentes herramientas de comunicación.[3]

- Introducción de bienes en el ciberespacio. Son acciones que hace el usuario para trasladar sus bienes del espacio físico al ciberespacio. Las variables estudiadas son facilitar datos personales[4] y guardar información personal en los dispositivos.[5]

- Falta de autoprotección. Son acciones que llevan a cabo los usuarios y hacen que sus bienes estén menos protegidos. Se mide usar la misma contraseña para todo, haber facilitado alguna vez sus contraseñas a otras personas y hacer uso de software pirata.

- Vigilancia experimentada. Son las actividades que realizan los padres u otros familiares para controlar la actividad de los jóvenes en el ciberespacio o que les puede hacer sentirse controlados. Se incluyen compartir el ordenador/tableta con familiares, controlar las horas que usan los dispositivos, controlar las actividades que realizan y tener instalados sistemas de control parental.

## 2.3. Instrumentos

La herramienta que se empleó para la obtención de los datos es la encuesta electrónica «Hábitos de los menores en Internet». Un instrumento creado *ad hoc* por diferentes profesionales del ámbito de las ciencias jurídicas y sociales (Derecho, Criminología, Psicología y Metodología de las Ciencias del Comportamiento) para conocer, por un lado, las actividades cotidianas que realizan los menores en Internet y, por otro, las distintas formas de violencia que sufren los menores en Internet.

Con el fin de garantizar el correcto funcionamiento de la encuesta, se realizó un estudio piloto con una muestra representativa de la muestra total compuesta por cien alumnos de un centro de enseñanza secundaria de la provincia de Alicante.

## 2.4. Procedimiento

Para la obtención de la muestra se seleccionaron de manera aleatoria veinte centros de educación secundaria y

2. Véase más en las tablas 7 y 8 en anexos.
3. Esta variable numérica ha sido creada a partir de la suma de las respuestas obtenidas en seis ítems de naturaleza categórica 1 = sí/ 0 = no (hacer uso de correo electrónico, mensajería instantánea, redes sociales, chat, blogs y videollamadas).
4. Resulta de la suma de los tipos de datos que los jóvenes facilitan (nombre, apellidos, teléfono, fotos, correo electrónico, colegio en el que estudia, ubicación desde la que habla, dirección y edad).
5. Creada a partir de la información que almacenan en los dispositivos con los que se conectan a Internet (un archivo con contraseñas, fotos personales, fotos íntimas, vídeos personales, información personal/íntima).

bachillerato, tanto públicos como concertados, de dieciséis poblaciones de la provincia de Alicante.[6] Asimismo, antes de obtener los datos, se solicitaron los permisos correspondientes de la Conselleria d'Educació, Cultura i Esport, de la dirección de los centros y de los padres.

La recogida de información se realizó en el aula de informática de los centros. Se procuró un ordenador para que cada participante pudiera acceder a la versión electrónica de la encuesta mediante un enlace web. Tras ser informados por dos encuestadores debidamente formados de la voluntariedad de la participación, así como de las cuestiones de funcionamiento, los participantes contestaron de manera anónima la encuesta. Todos los datos fueron registrados en una base de datos en formato CSV sin identificaciones personales.

### 2.5. Técnicas de análisis

En primer lugar se realizaron los análisis descriptivos, tanto para la variable dependiente como para las variables independientes, y se obtuvo para las variables cualitativas las frecuencias y las proporciones, y para las variables numéricas los estadísticos mínimo, máximo, media, mediana, desviación típica y el test de Kolmorov-Smirnov para una muestra.

En segundo lugar se analizó la asociación entre la variable dependiente y las independientes para lo cual se usó el test $\chi 2$ para las variables categóricas dicotómicas y la prueba no paramétrica *U* de Mann-Whitney para las variables numéricas, dado que mostraron una distribución no normal.

Finalmente se elaboró un modelo de regresión logística para identificar los principales factores asociados al riesgo de sufrir un ataque de *malware*. Fueron incluidas en el modelo todas las variables independientes que mostraron, en el análisis bivariado, asociación significativa con la variable dependiente ($p < .05$). Se usó el método hacia delante condicional y la adecuación del modelo fue evaluada con la prueba de Hosmer-Lemeshow.

Todos los análisis se realizaron con el programa estadístico SPSS versión 22.

## 3. Resultados

### 3.1. Prevalencia de victimización por *malware* en jóvenes de la provincia de Alicante

Cabe señalar, en primer lugar, que el 72% de los participantes (n = 1.468) afirmó que el antivirus los avisó de la presencia de algún tipo de virus en sus sistemas informáticos.

**Tabla 2.** Prevalencia de victimización por *malware*

| VICTIMIZACIÓN | n | % |
|---|---|---|
| *No víctima* | 570 | 28 |
| *Víctima* | 1468 | 72 |
| *Total* | 2038 | 100 |

Se trata de una forma de victimización que la mayoría de los participantes en el estudio han sufrido en más de una ocasión. Concretamente, como se muestra en la tabla 3, al 56,2% de las víctimas le ha ocurrido entre una y tres veces, mientras que al 17,1% le ha ocurrido entre cuatro y seis veces, al 4,2% entre siete y nueve veces y al 22,5% diez veces o más.

**Tabla 3.** Frecuencia de victimización por *malware*

| VICTIMIZACIÓN | n | % |
|---|---|---|
| *De 1 a 3 veces* | 825 | 56,2 |
| *De 4 a 6 veces* | 251 | 17,1 |
| *De 7 a 9 veces* | 62 | 4,22 |
| *10 o más veces* | 330 | 22,48 |
| *TOTAL* | 1468 | 100 |

### 3.2. Relación entre el uso cotidiano de las TIC y victimización por *malware*

Con el propósito de determinar la relación entre las actividades cotidianas de los menores en el ciberespacio y la victimización por *malware*, en primer lugar, se llevaron a cabo análisis bivariados (tablas 4 y 5). Los resultados

6. Alicante, Almoradí, Aspe, Benidorm, Castalla, Crevillente, Elche, Elda, Ibi, Jijona, San Juan de Alicante, San Vicente del Rapeig, Santa Pola, Torrellano, Torrevieja y Villajoyosa.

muestran que existe una relación significativa entre la visibilidad en el ciberespacio y la victimización por *malware*. Concretamente, las víctimas descargan un mayor número de archivos a la semana (*U* = 30.4061,5*; p* = ,000), aunque la diferencia es pequeña de acuerdo al tamaño del efecto (*r = -0,22)*. Asimismo, no solo tiene relación con el número de archivos descargados, sino también con la herramienta empleada para realizar las descargas y el tipo de archivos. Así, se observa que el 77,8% de los participantes que afirman haber descargado archivos alguna vez usando programas P2P han sido victimizados ($\chi 2$ = 39,91; *p* = ,000) y el 81,5% que lo ha hecho a través de webs de descarga como mega, seriespepito, etc. ($\chi 2$ = 31,01; *p* = ,000). Respecto al tipo de archivos que descargan, se observa que han sido victimizados por *malware* el 88% de los que descargan archivos con contenido pornográfico ($\chi 2$ = 12,26; *p* = ,000), el 85,5% que descarga programas ($\chi 2$ = 55,55; *p* = ,000), el 81,60% que descarga películas ($\chi 2$ = 67,57; *p*= ,000), el 78,4% que descarga aplicaciones ($\chi 2$ = 34,53; *p* = ,000), el 76,8% que descarga música ($\chi 2$ = 43,45; *p* = ,000) y el 75,9% que descarga juegos ($\chi 2$ = 12,50; *p* = ,000).

Siguiendo con las variables de «visibilidad», descargar archivos o abrir enlaces enviados por desconocidos también tiene relación con la victimización ($\chi 2$ = 17,43; *p* = ,000). Además, cabe señalar que las víctimas usan las TIC en mayor medida para establecer contacto con personas desconocidas (*U*= 30.4061,5*; p* = ,000) y hacen un mayor uso de las herramientas de comunicación (redes sociales, chat, mensajería instantánea, etc.) (*U* = 30.4061,5*; p* = ,000) que las no víctimas, aunque, de nuevo, las diferencias son pequeñas de acuerdo al tamaño del efecto (*r* < 0,3).

Tabla 4. Relación entre las variables independientes y la variable dependiente (I)

| | VÍCTIMA | | NO VÍCTIMA | | $\chi 2$ | Odds Ratio |
|---|---|---|---|---|---|---|
| | n | % | n | % | | |
| ***Visibilidad*** | | | | | | |
| Descargar con programas P2P | 854 | 77,80% | 243 | 22,20% | 39,91*** | 1,872 |
| Descargar en web | 423 | 81,50% | 96 | 18,50% | 31,01*** | 1,999 |
| Descargar juegos | 694 | 75,90% | 220 | 24,10% | 12,50*** | 1,426 |
| Descargar software | 406 | 85,50% | 69 | 14,50% | 55,55*** | 2,776 |
| Descargar pornografía | 81 | 88,00% | 11 | 12,00% | 12,26*** | 2,968 |
| Descargar música | 1030 | 76,80% | 312 | 23,20% | 43,45*** | 1,945 |
| Descargar películas | 701 | 81,60% | 158 | 18,40% | 67,57*** | 2,383 |
| Descargar aplicaciones | 735 | 78,40% | 203 | 21,60% | 34,53*** | 1,813 |
| Abrir enlaces desconocidos | 336 | 80,20% | 83 | 19,80% | 17,43*** | 1,742 |
| ***Autoprotección*** | | | | | | |
| Usar la misma contraseña | 465 | 72,80% | 174 | 27,20% | 0,252 | - |
| Facilitar contraseña por Internet | 235 | 78,60% | 64 | 21,40% | 7,494** | 1,507 |
| Uso de software pirata | 700 | 82,70% | 146 | 17,30% | 82,368*** | 2,647 |
| ***Vigilancia experimentada*** | | | | | | |
| No uso de sist. de control parental | 1288 | 72,40% | 490 | 27,60% | 1,16 | - |
| No control de las horas | 884 | 72,80% | 331 | 27,20% | 0,787 | - |
| No control del uso | 1131 | 73,40% | 410 | 26,60% | 5,823** | 1,310 |

Tabla 5. Relación entre las variables independientes y la variable dependiente (II)

| | | n | | D.T. | $P_{25}$ | $P_{50}$ | $P_{75}$ | RANGO PROME. | U de M-W | r |
|---|---|---|---|---|---|---|---|---|---|---|
| ***Visibilidad*** | | | | | | | | | | |
| Contacto con desconocidos | Víctima | 1465 | 2,12 | 3,42 | 0 | 0 | 3 | 1068,32 | 346709*** | -0,15 |
| | No víctima | 570 | 1,28 | 2,95 | 0 | 0 | 1 | 893,76 | | |
| N.º archivos descargados | Víctima | 1468 | 3,32 | 3,12 | 1 | 2 | 5 | 1097,37 | 304061,5*** | -0,22 |
| | No víctima | 570 | 2,16 | 2,78 | 0 | 1 | 3 | 818,94 | | |
| Herramientas | Víctima | 1468 | 3,50 | 1,05 | 2 | 4 | 4 | 1074,98 | 336935,5*** | -0,18 |
| | No víctima | 570 | 3,08 | 1,18 | 2 | 3 | 4 | 876,61 | | |
| ***Introducción de datos*** | | | | | | | | | | |
| Facilitar datos | Víctima | 1468 | 1,89 | 2,70 | 0 | 0 | 4 | 1057,4 | 362743*** | -0,12 |
| | No víctima | 570 | 1,19 | 2,19 | 0 | 0 | 2 | 921,89 | | |
| Guardar información | Víctima | 1468 | 2,11 | 2,08 | 0 | 2 | 4 | 1082,17 | 326374*** | -0,16 |
| | No víctima | 570 | 1,37 | 1,83 | 0 | 4 | 2 | 858,09 | | |
| ***Vigilancia experimentada*** | | | | | | | | | | |
| Compartir ordenador con familiares | Víctima | 1468 | 1,20 | 0,84 | 1 | 1 | 2 | 1033,65 | 397604 | |
| | No víctima | 570 | 1,12 | 0,85 | 0 | 1 | 2 | 983,05 | | |

*p < ,05, **p < ,01, ***p< ,001

Respecto a las variables que hacen referencia a la introducción de bienes en el ciberespacio, los resultados muestran que las víctimas facilitan mayor información personal a través de Internet ($U$ = 362.743; $p$ = ,000) y guardan más información personal en sus dispositivos que las no víctimas ($U$ = 326374; $p$ = ,000), aunque las diferencias no son grandes ($r$ < 0,3).

Por otra parte, también han resultado tener relación con la victimización las actividades que los menores no realizan para proteger sus sistemas informáticos. En este sentido, el 78,6% de las personas que afirman haber facilitado alguna vez sus contraseñas a través de Internet han sido victimizadas ($\chi2$ = 7,494; $p$= ,006) y el 82,7% de los que afirman usar *software* pirata también han sufrido ataques de *malware* ($\chi2$ = 82,368; $p$ = ,000). En cambio, no ha resultado tener una relación significativa con la victimización el hacer uso de la misma contraseña para todo ($\chi2$ = 0,252; $p$ = ,616).

Finalmente, respecto a las variables de vigilancia experimentada, únicamente han mostrado tener una relación significativa con la victimización el que no tengan un control sobre el uso que realizan de las TIC ($\chi2$ = 5,823; $p$ = ,016). Así, se puede observar que entre los que afirman no ser controlados respecto al uso el 73,4% han sido victimizados en alguna ocasión. En cambio, no ha resultado tener una relación significativa el que no tengan control sobre las horas ($\chi2$ = 0,787; $p$ = ,375), no tengan instalados sistemas de control parental ($\chi2$ = 1,16; $p$ = ,281) y que compartan el ordenador con otros familiares ($U$ = 397604; $p$ = ,065).

## 3.3. Factores predictores de la victimización por *malware*

Todas las variables independientes que mostraron tener una relación significativa con el proceso de victimización fueron usadas para crear un modelo predictivo mediante un análisis de regresión logística, al objeto de determinar, por un lado, la capacidad que tienen para explicar el proceso de victimización y, por otro, identificar los factores de riesgos asociados al mismo.

Como se puede observar en la tabla 6, las variables incluidas mejoraron significativamente el modelo nulo ($\chi2$ = 188,832; $p$ = ,000), ofreciendo un buen ajuste a los datos ($\chi2$ = 9,648;

Tabla 6. Factores de riesgo de la victimización por *malware*.

| | B | Error estándar | Wald | gl | Sig. | Exp(B) | 95% C.I. para EXP(B) | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | Inferior | Superior |
| ***N.º archivos descargados*** | 0,31 | 0,14 | 4,91 | 1 | 0,027 | 1,36 | 1,036 | 1,784 |
| ***Descargar software*** | 0,37 | 0,16 | 5,52 | 1 | 0,019 | 1,449 | 1,064 | 1,974 |
| ***Descargar películas*** | 0,38 | 0,12 | 10,26 | 1 | 0,001 | 1,467 | 1,16 | 1,855 |
| ***Contacto con desconocidos*** | 0,47 | 0,13 | 13,64 | 1 | 0,000 | 1,605 | 1,248 | 2,063 |
| ***Herramientas*** | 0,59 | 0,13 | 22,85 | 1 | 0,000 | 1,815 | 1,422 | 2,318 |
| ***Guardar información*** | 0,28 | 0,12 | 5,05 | 1 | 0,025 | 1,317 | 1,036 | 1,676 |
| ***Uso de software pirata*** | 0,51 | 0,12 | 17,66 | 1 | 0,000 | 1,672 | 1,316 | 2,126 |
| ***Constante*** | -0,21 | 0,12 | 3,13 | 1 | 0,077 | 0,814 | | |
| Omnibus (Modelo) | $\chi 2$ = 190,773*** | | | | | | | |
| Hosmer y Lemeshow | $\chi 2$ = 6,930 | | | | | | | |
| -2 Log-Likelihood | 2226,836 | | | | | | | |
| R2 Nagelkerke | 0,13 | | | | | | | |

*p < .05, **p < .01, ***p< .001

*p* = ,291), un coeficiente de determinación generalizado R2 de Nagelkerke de 0,13 y un porcentaje global de clasificación correcta de 73%.

Respecto a los factores de riesgo asociados al proceso de victimización por *malware*, los resultados de la regresión logística muestran que descargar archivos aumenta la probabilidad en 57,6% (OR = 1,36). Pero también ha resultado ser un factor de riesgo el tipo de archivos que se descargan. Concretamente, descargar software y películas aumentan el riesgo de sufrir un ataque de *malware* en un 59,2% (OR = 1,45) y un 59,5% (OR = 1,47), respectivamente. También supone un mayor riesgo contactar con desconocidos (Prob. = 61,6%, OR = 1,61), hacer un mayor uso de las herramientas de comunicación (Prob. = 64,5%, OR = 1,42), guardar más información personal en los dispositivos con los que se conecta a Internet (Prob. = 56,8%, OR = 1,32) y utilizar en mayor medida de software pirata (Prob.= 62,6%, OR=1,67).

## 4. Discusión

Respondiendo a los objetivos planteados inicialmente en este estudio, cabe señalar en primer lugar que alrededor de siete de cada diez jóvenes encuestados afirma haber detectado la presencia de códigos maliciosos en sus sistemas informáticos. Este porcentaje contrasta con los obtenidos en diferentes estudios para otras formas de victimización. Así, por ejemplo, atendiendo a estudios sobre ciberacoso realizados en la misma región se observa que el porcentaje de victimización está entre el 24,6% y el 38,8% (Buelga *et al.*, 2010; Estévez, *et al.*, 2010; García-Guilabert, 2014),[7] lo que pone de manifiesto que unos de los riesgos a los que en mayor medida están expuestos los jóvenes es a los ataques de *malware*.

En segundo lugar, los análisis realizados también muestran que existe una asociación significativa entre la actividad

7. Buelga *et al*. (2010) cifraron la prevalencia de victimización por ciberacoso en estudiantes de la Comunidad Valenciana entre el 24,6% y el 29%. El mismo año, Estévez *et al*. (2010) determinaron que un 30,1% de los estudiantes habían experimentado alguna forma de ciberacoso. Unos años más tarde García-Guilabert (2014) encontró que la prevalencia de victimización por ciberacoso continuado en la provincia de Alicante era de 38,8%.

que realizan los jóvenes en Internet y el haber sufrido ataques de *malware*. A nivel descriptivo se observa que el grupo de las víctimas realizan en mayor medida prácticamente todas las actividades cotidianas incluidas en el estudio, además de ser menos controlados por sus padres. Sin embargo, no todas las actividades han resultado ser predictivas para la victimización por *malware*. Las que han resultado tener mayor fuerza predictiva son el contactar con desconocidos y hacer un mayor uso en general de las herramientas de comunicación, como el correo electrónico, la mensajería instantánea, las redes sociales, los chats, blogs y videollamadas. Ambas variables habían sido señaladas como factores de riesgo para otras formas de victimización (Marcum *et al.*, 2010; Misha *et al.*, 2012; Mitchell, Wolak y Finkelhor, 2008; Ngo y Paternoster, 2011; Reyns, 2010, 2013; Sengupta y Chaudhuri, 2011; Vandebosch y Van Cleemput, 2009; Wilsem, 2011).

Otras variables que también son fuertes predictores y que ya habían sido identificadas por la literatura son las relacionadas con realizar descargas de archivos (Choi, 2008; Leukfeldt, 2015). Concretamente, es determinante el número de archivos descargados (a mayor número de descargas, más riesgo), así como descargar películas y software. El riesgo en estas acciones viene determinado porque los *hackers* suelen ocultar gran parte del *malware* en este tipo de archivos (Taylor *et al.*, 2006), que después son distribuidos en los sitios de intercambios de archivos, por lo que las empresas de seguridad recomiendan descargar únicamente archivos legales y hacerlo desde las webs de los proveedores (Symantec, 2015).

Finalmente, también han resultado ser predictores de riesgo el guardar información personal en los dispositivos con los que conectan a Internet y hacer uso de software pirata. Almacenar la información personal implica que pueda estar disponible para ser atacados por otros (Miró, 2013), sobre todo si no se adoptan otro tipo de medidas para proteger la información. En este sentido, de todas las acciones de autoprotección incluidas, la única que ha resultado ser un riesgo para la infección de *malware* es hacer uso de software pirata. La utilización de esta clase de programas es un riesgo para los usuarios porque facilitan la entrada de códigos maliciosos (Symantec, 2011). Tampoco tiene efecto el control por parte de los padres de la actividad de los hijos, como así se había señalado en estudios previos (Lee y Chae, 2007; Shin y Huh, 2011). Quizá se deba, como advierten Sasson y Mesch (2014), a que tener más restricciones en el uso no tiene que derivar precisamente en la realización de menos conductas de riesgo, dado que los jóvenes suelen tener más habilidades en el manejo de los dispositivos que los padres y encuentran la forma de saltar los controles. Y en contra del planteamiento inicial, compartir los dispositivos con los familiares no previene los ataques de *malware*. La disonancia con estudios previos podría deberse a que ellos también realizan actividades de riesgo para la victimización por *malware*, algo que sería interesante analizar en futuras investigaciones.

## Conclusiones

El estudio confirma la importancia del comportamiento del usuario en la probabilidad de que sean víctimas de cibercrimen. Hay determinadas actividades que los jóvenes realizan de manera cotidiana que aumentan el riesgo de que sus dispositivos se infecten de códigos maliciosos. Por ello, los esfuerzos en seguridad no deben ir únicamente encaminados a la creación de nuevos programas antivirus —que inevitablemente siempre van un paso por detrás de la producción de los códigos maliciosos—, sino también a hacer comprender a los usuarios los riesgos que conlleva realizar determinadas actividades, además de enseñarles claves muy sencillas para asegurar sus sistemas. Asimismo, deberían destinarse más recursos para, por un lado, reducir el anonimato en Internet y, por otro, transformar el mercado para hacer más atractivo y fácil el consumo de contenido digital lícito en detrimento del contenido pirata.

Finalmente, es necesario señalar las limitaciones que presenta el estudio. La principal es que en el tiempo que se ha empleado en esta investigación, desde su planteamiento hasta la publicación de este artículo, las TIC en general, pero el *malware* en especial, han seguido transformándose, con lo que se corre el riesgo de que los resultados aquí vertidos queden desfasados antes de su publicación. También es importante señalar que el instrumento utilizado en este estudio no ha sido diseñado exclusivamente para el análisis de la victimización por *malware*, por lo que se ha dejado de lado, por tanto, otras variables que pueden ser clave para la comprensión de este fenómeno y que deberán ser estudiadas en futuras investigaciones.

## Referencias bibliográficas

BOSSLER, A. M.; HOLT, T. J. (2009). «On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory». *International Journal of Cyber Criminology*. Vol. 3, núm. 1, págs. 400-420.

CHOI, K. (2008). «Computer Crime Victimization and Integrated Theory: An Empirical Assessment». *International Journal of Cyber Criminology*. Vol. *2*, págs. 308-333.

COHEN, L.; FELSON, M. (1979). «Social Change and Crime Rate Trends: A Routine Activity Approach». *American Sociological Review*. Vol. 44, págs. 588-608. ‹http://dx.doi.org/10.2307/2094589›

FELSON, M. (1998). *Crime and Everyday Life* (2nd ed.). Thousand Oaks, California: Pine Forge Press.

GARCÍA-GUILABERT, N. (2014). *Victimización de menores por actos de ciberacoso continuado y actividades cotidianas en el ciberespacio* [tesis doctoral]. Murcia: Servicio de Publicaciones de la Universidad de Murcia.

GRABOSKY, P. (2001). «Virtual Criminality: Old Wine in New Bottles?». *Social & Legal Studies*. Vol. 10, págs. 243-249.

HERNÁNDEZ, D.; RAMÍREZ-MARTINELL, A.; CASSANY, D. (2014). «Cetegorizando a los usuarios de sistemas digitales». *Revista de Medios y Educación.* N.º 44, págs. 113-126. ‹http://dx.doi.org/10.12795/pixelbit.2014.i44.08›

HOLT, T. J.; BOSSLER, A. M. (2013). «Examining the Relationship Between Routine Activities and Malware Infection Indicators». *Journal of Contemporary Criminal Justice.* Vol. 29, núm. 4, págs. 420-436. ‹http://dx.doi.org/10.1177/1043986213507401›

HUTCHINGS, A.; HAYES, H. (2009). «Routine activity theory and phishing victimisation: who gets caught in the "net"?». *Current Issues in Criminal Justice*. Vol. 20, núm. 3, págs. 1-20.

INTECO (2007). «La respuecta jurídica frente a los ataques contra la seguridad de la información» [en línea]. Instituto Nacional de Ciberseguridad. [Fecha de consulta: 15 de marzo de 2016]. Disponible en: https://www.incibe.es/file/ePXa1SmtJPgGEiZl7GiXgQ

LEE, S. J.; CHAE, Y. G. (2007). «Children´s Internet use in a family context: Influence on family relationships and parental mediation». *CyberPsychology & Behavior*. Vol. 10, núm. 5, págs. 640-644. ‹http://dx.doi.org/10.1089/cpb.2007.9975›

LEUKFELDT, E. R. (2015). «Comparing victims of phishing and malware attacks». *International Journal of advanced studies in Computer Since and Engineering.* Vol. 5, núm. 5, págs. 26-32.

LEUKFELDT, E. R.; YAR. M. (2016). «Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis». *Deviant Behavior.* Vol. 37, núm. 3, págs. 263-280. ‹http://dx.doi.org/10.1080/01639625.2015.1012409›

MARCUM, C. D.; RICKETTS, M. L.; HIGGINS, G. E. (2010). «Assessing Sex Experiences of Online Victimization: An Examination of Adolescent Online Behaviors Using Routine Activity Theory». *Criminal Justice Review*. Vol. 35, núm. 4, págs. 412-437. ‹http://dx.doi.org/10.1177/0734016809360331›

MARTÍN, A.; HERNÁNDEZ, A.; MARTÍN, J.; QUEIRUGA, A.; RODRÍGUEZ, G. (2015). Propagación del malware: nuevos modelos para nuevos escenarios. *Actas de las Primeras Jornadas Nacionales de Investigación en Ciberseguridad.*

MIRÓ, F. (2011). «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen». *Revista Electrónica de Ciencia Penal y Criminología*, núm. 13-07.

MIRÓ, F. (2012). *El cibercrimen. Fenomenología criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons.

MISHNA, F.; KHOURY-KASSABRI, M.; GADALLA, T.; DACIUK, J. (2012). «Risk factors for involvement in cyber bullying: Victims, bullies and bully–victims». *Children and Youth Services Review*. Vol. 34, núm. 1, págs. 63–70. ‹http://dx.doi.org/10.1016/j.childyouth.2011.08.032›

MITCHELL, K. J.; WOLAK, J.; FINKELHOR, D. (2008). «Are blogs putting youth at risk for online sexual solicitation or harassment?». *Child Abuse & Neglect*. Vol. *32*, núm. 2, págs. 277-294. ‹http://dx.doi.org/10.1016/j.chiabu.2007.04.015›

NGO, F.; PATERNOSTER, R. (2011). «Cybercrime Victimization: An examination of Individual and Situational level factors». *International Journal of Cyber Criminology*. Vol. 5, núm. 1, págs. 773-793.

PRATT, T. C.; HOLTFRETER, K.; REISIG, M. D. (2010). «Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory». *Journal of Research in Crime and Delinquency*. Vol. 47, núm. 3, págs. 267-296. ‹http://dx.doi.org/10.1177/0022427810365903›

PRENSKY, M. (2001). «Digital Natives, Digital Immigrants». *On the Horizon*. Vol. 9, núm. 5, págs. 1–6. ‹http://dx.doi.org/10.1108/10748120110424816›

REYNS, B. W. (2010). *Being Pursued Online: Extent and Nature of Cyberstalking Victimization from a Lifestyle/Routine Activities Perspective* [tesis doctoral]. University of Cincinnati.

REYNS, B. W. (2013). «Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses». *Journal of Research in Crime and Delinquency*. Vol. 50, núm. 2, págs. 216–238. ‹http://dx.doi.org/10.1177/0022427811425539›

REYNS, B. W. (2015) «A routine activity perspective on online victimisation: Results from the Canadian General Social Survey». *Journal of Financial Crime*. Vol. 22, núm. 4, págs. 396-411. ‹http://dx.doi.org/10.1108/JFC-06-2014-0030›

REYNS, B. W.; HENSON, B. (2015). «The Thief With a Thousand Faces and the Victim With None: Identifying Determinants for Online Identity Theft Victimization With Routine Activity Theory». *International Journal of Offender Therapy and Comparative Criminology,* págs. 1-21. ‹http://dx.doi.org/10.1177/0306624X15572861›

SASSON, H.; MESCH, G. (2014). «Parental mediation, peer norms and risky online behavior among adolescents». *Computers in Human Behavior*. Vol. 33, págs. 32-38. ‹http://dx.doi.org/10.1016/j.chb.2013.12.025›

SHIN, W.; HUH, J. (2011). «Parental mediation of teenagers' video game playing: Antecedents and consequences». *New Media & Society*. Vol. 13, págs. 945-962. ‹http://dx.doi.org/10.1177/1461444810388025›

SENGUPTA, A.; CHAUDHURI, A. (2011). «Are social networking sites a source of online harassment for teens? Evidence from survey data». *Children and Youth Services Review*. Vol. 33, núm. 2, págs. 284–290. ‹http://dx.doi.org/10.1016/j.childyouth.2010.09.011›

SYMANTEC CORPORATION (2015). *Internet Security Threat Report 2015*, Volume 20. The Symantec Corporation World Headquarters.

SYMANTEC CORPORATION (2011). «Cómo evitar la piratería» [en línea]. [Fecha de consulta: 20 de marzo de 2016]. Disponible en: ‹http://es.norton.com/how-to-be-pirate-free/article›

TAYLOR, R.W.; CAETI, T.J.; LOPER, D.K.; FRITSCH, E.J.; LIEDERBACH, J. (2006). *Digital crime and digital terrorism*. Upper Saddle River, NJ: Pearson Prentice Hall.

VANDEBOSCH, H.; VAN CLEEMPUT, K. (2009). «Cyberbullying among youngsters: profiles of bullies and victims». *New Media & Society*. Vol. 11, núm. 8, págs. 1.349-1.371. ‹http://dx.doi.org/10.1177/1461444809341263›

WHITE, D.; LE CONU, A. (2011) «Visitors and Residents: A new typology for online engagement». *First Monday*. Vol. 16, núm. 9. <http://dx.doi.org/ 10.5210%2Ffm.v16i9.3171>

WILSEM, J. V. (2011). «"Bought it, but Never Got it" Assessing Risk Factors for Online Consumer Fraud Victimization». *European Sociological Review*. Vol. 29, núm. 2, págs. 168-178. <http://dx.doi.org/10.1093/esr/jcr053>

YAR, M. (2005). «The Novelty of "Cybercrime" An Assessment in Light of Routine Activity Theory». *European Journal of Criminology*, Vol. 4, núm. 2, págs. 407-427. <http://dx.doi.org/10.1177/147737080556056>

YUCEDAL, B. (2010). *Victimization in Cyberspace: An Application of Routine Activity and Lifestyle Exposure Theories* [tesis doctoral]. Kent State University.

## Anexos

Tabla 7. Análisis descriptivo de las variables independientes (I)

| | n | SÍ Frc. (%) | NO Frc. (%) |
|---|---|---|---|
| ***Descargar con programas P2P*** | 2038 | 1.097 (53,8%) | 941 (46,2%) |
| ***Descargar en web*** | 2038 | 519 (25,5%) | 1.519 (74,5%) |
| ***Descargar juegos*** | 2038 | 914 (44,8%) | 1.124 (55,2%) |
| ***Descargar software*** | 2038 | 475 (23,3%) | 1.563 (76,7%) |
| ***Descargar pornografía*** | 2038 | 92 (4,5%) | 1.946 (95,5%) |
| ***Descargar música*** | 2038 | 1.342 (65,8%) | 696 (34,2%) |
| ***Descargar películas*** | 2038 | 859 (42,1%) | 1.179 (57,9%) |
| ***Descargar aplicaciones*** | 2038 | 938 (46%) | 1.100 (54%) |
| ***Abrir enlaces desconocidos*** | 2038 | 419 (20,6%) | 1.619 (79,4%) |
| ***Usar la misma contraseña*** | 2038 | 639 (31,4%) | 1.399 (68,6%) |
| ***Facilitar contraseña por Internet*** | 2038 | 299 (14,7%) | 1.739 (85,3%) |
| ***Uso de software pirata*** | 2038 | 846 (41,5%) | 1.192 (58,5%) |
| ***No uso de sistemas de control parental*** | 2038 | 1.778 (87,2) | 260 (12,8%) |
| ***No control de las horas*** | 2038 | 1.215 (59,6%) | 823 (40,4%) |
| ***No control del uso*** | 2038 | 1.541 (75,6%) | 497 (24,4%) |

Tabla 8. Análisis descriptivo de las variables independientes (II)

| Variables independientes | n | Mín. | Máx. | | D.T | Me | Z K-S | p |
|---|---|---|---|---|---|---|---|---|
| Contacto con desconocidos | 2038 | 0 | 10 | 1,88 | 3,32 | 0 | 0,335 | 0,000 |
| N.º archivos descargados | 2038 | 0 | 10 | 2,99 | 3,07 | 2 | 0,213 | 0,000 |
| Herramientas | 2038 | 0 | 6 | 3,39 | 1,11 | 3 | 0,182 | 0,000 |
| Facilitar datos | 2038 | 0 | 9 | 1,69 | 2,59 | 0 | 0,383 | 0,000 |
| Guardar información | 2038 | 0 | 9 | 1,91 | 2,04 | 1,5 | 0,208 | 0,000 |
| Compartir ordenador | 2038 | 0 | 3 | 1,18 | 0,84 | 1 | 0,226 | 0,000 |

**Cita recomendada**

GARCÍA-GUILABERT, Natalia (2016). «Actividades cotidianas de los jóvenes en Internet y victimización por malware». En: Josep Maria TAMARIT SUMALLA (coord). «Ciberdelincuencia y cibervictimización». *IDP. Revista de Internet, Derecho y Política*. N.º 22, págs. 59-72. UOC. [Fecha de consulta: dd/mm/aa]
<http://journals.uoc.edu/index.php/idp/article/view/n22-garcia-guilabert/n22-garcia-guilabert-pdf-es>
<http://dx.doi.org/10.7238/idp.v0i22.2969>



**Sobre la autora**

Natalia García-Guilabert
n.garcia@crimina.es

Centro Críminia
Universidad Miguel Hernández

Docente e investigadora colaboradora del Centro Crímina para el Estudio y Prevención de la Delincuencia de la Universidad Miguel Hernández

Centro Crímina para el Estudio y Prevención de la Delincuencia
Universidad Miguel Hernández
Avda. de la Universidad s/n. Edif. Hélike
03201 Elche

UOC
Universitat Oberta de Catalunya