LA VICTIMIZACIÓN POR CIBERCRIMINALIDAD EN EL ÁMBITO PATRIMONIAL: REVISIÓN TEÓRICA Y PROPUESTA DE INVESTIGACIÓN

Sanae Ben jalloul Ezzoubair
Josselyn Cristina Bolaños Grijalva
Katherine Chávez Collazos
Amanda Gómez Latorre
Universidad Rey Juan Carlos

Resumen

En este texto se presenta un diseño de investigación desde la cibercriminología, en el que se plantea como objetivo general el estudio de la relación entre el desempleo y la probabilidad de sufrir fraudes informáticos. El punto de partida es la reconceptualización que Fernando Miró Llinares hace de la Teoría de las Actividades Cotidianas (TAC). Esta teoría estudia cómo las actividades que realiza una determinada población afectan en la oportunidad delictiva del agresor. Miró expone que en el ciberespacio cambian las características del objetivo adecuado, es decir, lo que hace que alguien sea más victimizado. Este cambia la consideración que hizo Felson sobre el acrónimo VIVA y lo sustituye por el acrónimo, en inglés, ISI (Introduction, self-protection, Interaction).

Concretamente, en este texto se propone un proyecto de investigación que examine si las personas en situación de desempleo cambian las actividades y hábitos, por el hecho de hallarse en tal situación, dando lugar a mayores oportunidades de ser cibervictimizados, máxime en un contexto golpeado por la crisis económica. Con tal fin, esta aportación examina, primero, la bibliografía existente, en la que no suele considerarse este factor de desempleo como facilitador de la victimización. En segundo lugar, formula una serie de objetivos e hipótesis para ser aplicados en España, y propone una estrategia de investigación con la que mostrar su validez.

Palabras Clave: Cibercriminalidad, desempleados, fraudes informáticos, estafas, Criminología.

I. **Objeto**

La Cibercriminología, es una rama de la Criminología que estudia los delitos que se producen a través de las nuevas tecnologías (TICS) y debido a su utilización cada vez mayor a nivel mundial se producen formas alternativas de estudiar la adecuación de los delitos en el ámbito cibernético. A diferencia del mundo físico, en el mundo virtual la actitud de la víctima es un factor primordial porque, de alguna manera, es el que "inicia" el contacto.

Noticias recientes publicadas en el año 2018 acerca de la cibercriminalidad que se produce en España en diversos periódicos como ABC nos señalan la alarma social que se produce. *En 2018, los ciberdelincuentes han usado cada vez más el "ransomware" para móviles. El uso de este tipo de ataque, que secuestra el terminas de su víctima, también ha crecido de forma exponencial en ordenadores*. O Economía Digital que nos dice que *Los ciberdelitos se disparan en España. En los primeros dos meses de 2018, España gestionó más ciberdelitos que en todo 2014: entre enero y febrero se sumaron 125 incidencias frente a las 63 de hace cuatro años.*

Por otro lado el Instituto Nacional de Ciberseguridad (INCIBE), con sede en León, se encarga de llevar a cabo proyectos innovadores relacionados con la ciberseguridad. En cuanto a los ciberdelitos, el Secretario de Estado de Seguridad, Francisco Martínez explica que "en 2015, se registraron 60.400, un 25% más que en 2014 y un 61% más que hace cuatro años", según una noticia publicada en octubre del 2016 en El País.

La Cibercriminología es un campo que no sólo interesa a las personas de a pie por las pérdidas personales que pueden sufrir a través de los ciberataques sino también desde el ámbito de la economía y la política porque les interesan los *fraudes virtuales y hacktivismo*, respectivamente; y en el plano social focalizan la atención en temas relacionados con *el racismo y la xenofobia, hasta la nueva amenaza del terrorismo cibernético y los secuestros en línea* (Trujano Ruiz, 2009:8). En particular, los sectores a los que más concierne son la Criminología porque es la ciencia que se encarga de combatirlo; la Ingeniería Informática ya que estudia en profundidad los mecanismos a través de los cuales se crean y se combaten los ciberdelitos y, por último, a la Sociología de la desviación y Psicología que se suman a los esfuerzos para analizar, comprender y tratar los comportamientos que los cibercriminales desarrollan.

Por lo tanto, consideramos la Cibercriminología objeto de estudio de vital importancia en nuestros días y en el presente diseño de investigación planteamos como objetivo

general la demostración de una correlación entre ser desempleado y sufrir fraudes informáticos. Para ello, nos vamos a basar, fundamentalmente, en la reconceptualización que Fernando Miró Llinares hace de la Teoría de las Actividades Cotidianas (más adelante, TAC). Esta teoría estudia cómo las actividades que realiza una determinada población afecta en la oportunidad delictiva que el propio agresor toma en cuenta antes de delinquir. En este sentido, se constata que la crisis que ha sufrido España desde el 2008 ha provocado un gran número de desempleados llegando a su tasa máxima de paro a un 27% a comienzos del 2013. En conclusión, este proyecto de investigación estudiará si este número de personas que han dejado de trabajar han cambiado las actividades que antes hacían cuando estaban empleados para poder constatar la existencia o no de una correlación entre el ser desempleado y sufrir fraudes informáticos.

La teoría más importante en el ámbito del factor de la oportunidad es la Teoría de las Actividades cotidianas que fue propuesta por Lawrence E. Cohen y Marcus Felson en 1979. Este estudio se llevó a cabo cuando se dieron cuenta que una mejora de las condiciones económicas entre la II Guerra Mundial y los años setenta, paradójicamente, produjo un aumento de la delincuencia y para dar una explicación a esta supuesta contradicción estudiaron el cambio de rutinas (actividades) que las personas realizaban tanto las víctimas como los delincuentes (Redondo, S; Garrido, V. 2013).

En cuanto a las víctimas, los desplazamientos de un lugar a otro, el aumento del tiempo que se pasa fuera de casa, el movimiento del dinero en general da lugar a una visibilidad de mayores recursos como la adquisición de coches, artículos de consumo, que darían lugar a que fueran *víctimas apropiadas*. En cuanto a los delincuentes deberían estar *motivados* para el delito y además al existir medios más efectivos para delinquir como automóviles, coches, motos u ordenadores facilitan la comisión de delitos. El tercer factor, reside en la *ausencia de eficaces protectores* como la policía, sin embargo, también lo podemos ser nosotros mismos, familiares o amigos (Redondo, S; Garrido, V. 2013).

Por lo tanto, dentro de la teoría de las actividades cotidianas se distinguen tres elementos mínimos que debe de coincidir en tiempo y espacio para que se produzca un delito, estos elementos son: potencial agresor, objetivo adecuado a los ojos del agresor y la ausencia de un guardián capaz. Pero, ¿qué hace que un objetivo se más o menos adecuado para el agresor? Para resolver esta duda Felson utiliza el acrónimo

VIVA, en el cual se detallan ciertas características que debe de poseer un objetivo para que sea más adecuado al potencial agresor, por tanto, dichas características son:

- **Valor, calculado o simbólico**, desde la perspectiva del delincuente. Felson propone identificar cuál es el objeto más popular en cada delincuente, para conocer cuáles son sus preferidos.

- **Inercia,** hace referencia al peso, tamaño y forma, estos son, los aspectos físicos de la persona o del bien, que funcionan como obstáculos para que el delincuente lo vea como adecuado.

- **Visibilidad,** como exposición de los objetos a los delincuentes, es decir, el atributo que marca a la persona o el bien para el ataque.

- **Accesibilidad,** referido al diseño del lugar y ubicación del objeto que aumenta el riesgo del ataque o lo facilita (Miró, 2015).

Los propios Felson y Cohen sostienen que no necesariamente aumenta la criminalidad respecto a una mejora de las condiciones económicas (citado por Redondo, S; Garrido, V. 2013) y es así como justificamos cuando escogemos como objeto de estudio a los desempleados que provienen de la crisis económica desde el año 2008 que ha empeorado las condiciones socioeconómicas.

Hemos mencionado anteriormente la aplicación de la Teoría de las Actividades Cotidianas (TAC) en el mundo físico pero no en el mundo virtual que es el ámbito que nos interesa para realizar este proyecto de investigación y nos basaremos en el artículo *La oportunidad criminal en el ciberespacio* cuyo autor es Fernando Miró Llinares quien hace una reconceptualización de la TAC porque, como explica, esta nueva forma de comunicación que se produce a través de las TIC´s cambia todos los aspectos que se desarrollan en él y dentro del cual, también, se encuentra el crimen.

Por lo tanto, Miró (2013) en el ciberespacio cambian las características del objetivo adecuado, es decir, lo que hace que alguien sea más victimizado y cambia la consideración que hizo Felson sobre el acrónimo VIVA y lo sustituye por el acrónimo, en inglés, ISI (*Introduction, self-protection, Interaction*):

- **Introducción en el ciberespacio**. Hace referencia a la introducción voluntaria o no por parte de la víctima de bienes ya sean de carácter personal, patrimonial, etc.

- **Self-protection**. Hace referencia a mecanismos que el propio individuo utiliza para protegerse, estos mecanismos o herramientas pueden ser el uso de antivirus, antiespías, cortafuegos, etc.

- **Interacción.** Se establece mediante la comunicación con otros usuarios a través de las múltiples herramientas que ofrece internet, lo cual hace que la víctima esté más accesible y visible a los potenciales agresores (Miró, 2013: 16)

En cuanto a otras teorías que pueden explicar el aumento de la cibercriminalidad, se han encontrado varias, de las cuales se destacan dos. Por un lado, la teoría del patrón delictivo como explica Agustina Sanllehí (citado por Antolínez Cascales, 2015:14) es una teoría situacional que busca explicar cómo el entorno físico, las pautas sociales y el comportamiento de las víctimas aumentan las oportunidades para el delito.

Dado que esta teoría se centra en aspectos relativos al lugar del delito, el autor de este artículo alude a ésta haciendo un paralelismo entre el espacio físico y real y el espacio virtual; en este sentido explica que *"la red sería tanto un lugar criminógeno, en el sentido de que por sus mismas condiciones genera delincuencia, como un espacio propicio que atrae al delincuente a cometer sus delito, en el que existen menores riesgos y abundan distintos objetivos"* (Sanllehí, Agustina, 2009).

Por otro lado, la teoría de la elección racional según Gary Becker (1968), en su artículo "*Crime and Punishment: An Economic Approach*", el delito es un cálculo racional de costes y beneficios.

Un modelo de prevención del delito que, frente a las tradicionales teorías de la criminalidad que se interesan por las razones que llevan a las personas a convertirse en delincuentes, pone el énfasis en la importancia de los factores ambientales, es decir, en la existencia de lugares y momentos que propician la concentración de los delitos, lo que permite la intervención en el ámbito de oportunidad para reducirla y evitar que el criminal motivado pueda cometer el delito. Es obvio que el ciberespacio es también ambiente, concretamente es un nuevo ámbito de oportunidad criminal y por eso es adecuado acercarse al crimen que se desarrolla en dicho nuevo espacio desde el enfoque que parte de la premisa de que las características del lugar donde se produce el delito condicionan el mismo y por ello, de que se puede intervenir en ellas para prevenir su realización (Miró, 2011).

El aval empírico que está relacionado con el objeto de nuestra investigación es amplio y reciente, es decir, se ha estudiado mucho acerca de la relación entre desempleo-

criminalidad, sin embargo, desempleo-cibercriminalidad es un campo aún muy desconocido debido a que no hay tantos profesionales del sector debidamente cualificados que se dediquen a llevar a cabo investigaciones de esta índole. A pesar de lo expuesto anteriormente, consideraremos tres investigaciones de gran alcance profesional y científico que serán los expuestos a continuación.

En primer lugar, un proyecto llevado a cabo en 132 países: *Routine Activity Theory and the Determinants of High Cybercrime Countries* cuyo autor, Alex Kigerl. Éste estudió en 2012 cómo afectaba una mayor tasa de desempleo en la incidencia de mayores delitos que se producen en la red debido a que los cibercriminales preferirían una vía económica más fácil y accesible.

"So long as Internet users are controlled for, so that two countries have an equal number of Internet users, but unequal unemployment, the country with high unemployment may have bigger problems with spam. This is hoped to be a measure of motivated offenders, as an Internet user might be more motivated to profit from cybercrime, were there are few legal economic opportunities available" (Kigerl, 2012)

Para lo cual formularon tres hipótesis: (a) países con mayor número de usuarios de Internet, producirán más delitos a través de la red, (b) países con una tasa alta de desempleados, producirán más ciberdelitos y (c) la relación existente entre las legislaciones de anti- cibercrimen y producción de los delitos cibernéticos.

The three research questions relate to these three variables: (a) Does the number of Internet users relate to cybercrime? (b) Does high unemployment relate to cybercrime? and (c) Does anti-cybercrime legislation relate to cybercrime? It was hypothesized that the variables of the first two questions are positively associated with spam. This research has found some support for the first two questions, but not the third (Kigerl, 2012).

Los resultados obtenidos fueron esclarecedores para las dos primeras hipótesis, sin embargo, para la tercera acerca de cómo influían las normas legales en los criminales no fue relevante. Por lo tanto, el autor de dicha investigación pudo extrapolar de los 132 países que analizó que una alta tasa de desempleo de profesionales del TIC´S podría incrementar la actividad cibercriminal en ese mismo país. En consecuencia, la solución plausible sería crear más puestos de trabajo en el campo de las TIC´S.

Siguiendo los resultados de la investigación *Routine Activity Theory and the Determinants of High Cybercrime Countries*, si hay más desempleo aumenta los ataques cibernéticos porque aumenta los cibercriminales, por tanto, aumenta la victimización.

En segundo lugar, el estudio *A Macro-Social Exploratory Analysis of the Rate of Interstate Cyber-Victimization* realizado por Michael J. Lynch y John Cochran en el cual utilizan TAC como base teórica para llevar un estudio acerca de la victimización por robo. Utilizaron dos tipos de variables, en primer lugar, se centran las actividades a través de la TIC´s: 1) el uso de Internet sólo en casa, 2) el uso de Internet fuera de casa, 3) el uso de Internet tanto fuera como dentro de casa; ellos consideraban que existía más victimización en aquellos que utilizaban Internet sólo en casa. Y en segundo lugar, estudian las actividades que realizan en casa (*household activity*) en relación con utilizar Internet sólo fuera o dentro de casa, para lo cual, formulan otras dos hipótesis: 4) un aumento de actividades dentro de casa y el uso de internet sólo en casa están asociados con un aumento de cibervictimización por robo, 5) un aumento de actividades dentro de casa y el uso de internet sólo fuera de casa están asociados con un aumento de cibervictimización por robo.

Para el estudio de las actividades que realizan en casa, se centran en los desempleados y las personas que viven fuera de la ciudad (*non-urban*). Para justificar la elección de los desempleados, nombra estudios donde se analiza la relación entre la tasa de desempleo y cibercriminalidad, sin embargo, nombran que hay estudios realizados por Anderson y Bennett (1996), Land, McCall y Cohen (1990) que observaron que la victimización online que sufren los desempleados baja cuando estos tiene un guardián capaz. Por todo ello, este estudio quiso investigar la relación entre los desempleados y el uso de Internet. Por tanto, pudieron afirmar que se produce una alta cibervictimización en los desempleados en aquellos que sólo utilizan el Internet en casa.

Este estudio también llevó a cabo un análisis sobre las siguientes variables de control: género, edad, etnicidad y riqueza. Las consideraron porque en cada una de ellas, se basaron en estudios anteriores donde explicaron qué patrones podrían estar más relacionados con la cibervictimización.

En tercer lugar, Miró (2013) en su estudio *"la victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio"* pretende, a través de la TAC, medir la victimización mediante *online harassment* de un individuo focalizándose en las actividades cotidianas que éste realiza en el ciberespacio.

Al principio, Miró hace un recopilatorio sobre estudios anteriores sobre la victimización en el ciberespacio que se basan en la TAC como el de Holt y Bossler en 2009 que además distinguen entre guardián físico (programas de protección) y guardián social (amigos con comportamiento antisocial en el ciberespacio); posteriormente, al año siguiente, en 2010 Marcum, Ricketts y Higgins realizan un estudio en el que añaden la división de la muestra en hombres y mujeres. El mismo año, Reyns incluye en su estudio el elemento de la proximidad entendiéndolo como frecuentar lugares con agresores. Por último, en 2011, Nego y Paternoster añaden variables de control tales como: género, edad raza, estado civil y laboral y comportamiento desviado.

En su mayoría las investigaciones estudiaban el *online harassment* o formas derivadas de éste (*cyberstalking*) y los resultados no fueron concluyentes ya que no todas las variables propuestas funcionaban. Aunque, en general, obtenían ideas como: que ser victimizado en internet no depende del tiempo sino de lo que se hace durante ese tiempo, que la figura del "guardián capaz" tiene más efecto si se trata de la vigilancia de otra persona y no un software de protección y que las mujeres son más victimizadas en internet.

El estudio de Miró utiliza tres hipótesis, la primera "*cuanto mayor sea la introducción de objetivos en el ciberespacio, mayor será el riesgo de victimización",* la segunda *"cuanto mayor sea la interacción en el ciberespacio, mayor será el riesgo de victimización"*, y la tercera "*cuanto menor sea la autoprotección, mayor será el riesgo de victimización."* De las cuales obtiene la variable dependiente, *cibervictimización por online harassment,* y las variables independientes, *introducción* (voluntaria o involuntaria de bienes al mundo virtual)*, interacción* (personal o con extraños) *y autoprotección* (software del tipo "anti virus" y/o rutinas de riesgo)*.* Además, incluyó la variable sociodemográfica *género.*

El estudio se realizó a través de una encuesta *ad hoc* a una muestra de 500 participantes formado por hombres y mujeres mayores de edad hasta los 65 años y que utilizaban internet un mínimo de 8 horas semanales*.* Miró consiguió demostrar que la introducción, interacción y autoprotección en el ciberespacio estaban relacionados con una mayor cibervictimización.

Al finalizar su estudio Miró propone otras investigaciones que se deberían realizar en el campo de las TIC y el ciberespacio para salvar las limitaciones del realizado por él. Una de ellas es estudiar otras formas de victimización en el ciberespacio como las que

afectan al patrimonio ya que afectan a gran parte de la población usuaria de las TIC. En este punto es donde vamos a centrar nuestro trabajo.

Por todo lo expuesto hasta ahora, enfocaremos nuestro objeto de estudio en averiguar si existe una relación entre el desempleo y la tasa de cibervictimización. En primer lugar, hemos visto con el primer estudio que en los países donde había más desempleo se correspondía con mayores tasas de cibercriminalidad, sin embargo, dicho estudio realizaba la unidad de análisis sobre los cibercriminales y este proyecto de investigación lo hará sobre los cibervictimizados y del último trabajo expuesto, realizado por Miró, es el que fundamentalmente nos basaremos para llevar a cabo nuestro proyecto de investigación ya que él reconceptualiza del VIVA al ISI para explicar las variables que contribuyen a que aumente la cibervictimización, por lo tanto, este presente trabajo se centrará en dos hipótesis, en primera instancia, las actividades por necesidad económica tiene relación con la *Interaction y ,* en segunda instancia, las actividades por imprudencia se relaciona con el *Self-proteccion* e *Introduction*.

II. **Objetivos**

Nuestro objeto general trata de demostrar si el **tipo de actividades que realizan los desempleados en la red los hacen más propensos a ser cibervictimizados**.

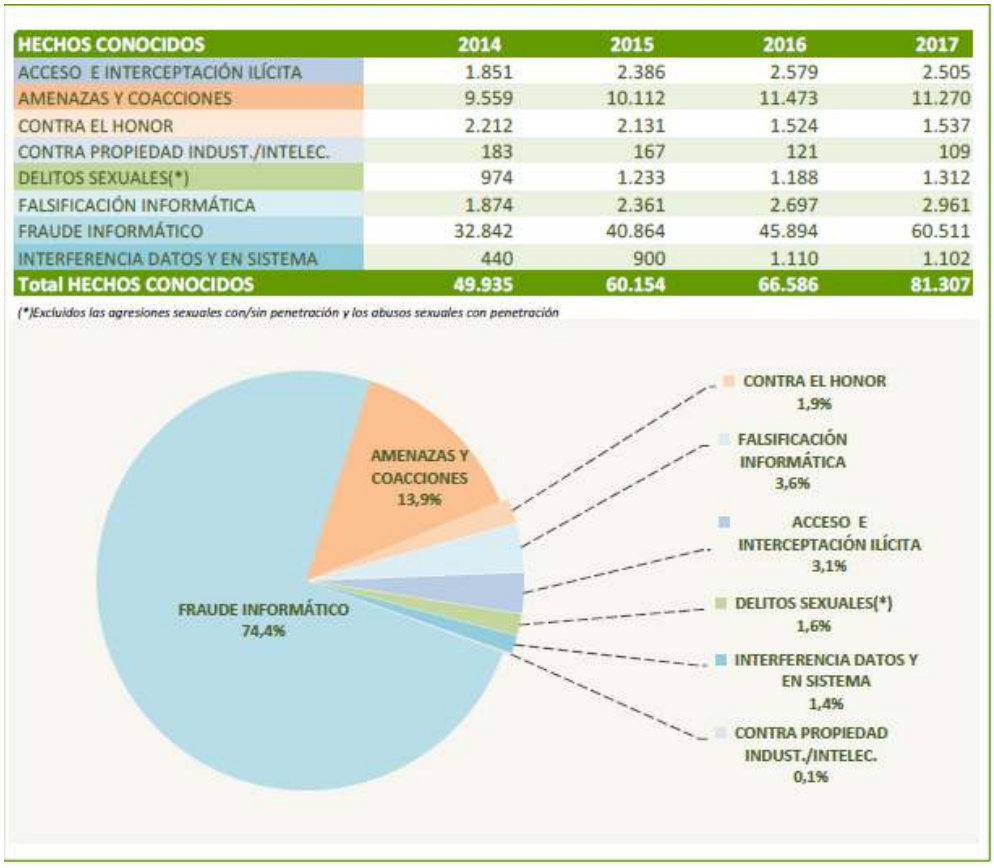
Entendiendo como **desempleados o parados** la definición dada por la RAE: "*que se halla en situación de paro forzoso*" y concretando con los datos sacados del INE que los describen como aquellos que forman parte de la población activa (que se encuentra en edad de trabajar, es decir, personas de 16 o más años) y que cumplen estos tres requisitos: se encuentran sin trabajo, están en busca de trabajo y están disponibles para trabajar. Esto se diferencia de la población inactiva que también se encuentra en edad de trabajar en que estas son personas sin trabajo, disponibles para trabajar y que no buscan empleo, donde se encuentran estudiantes, jubilados, incapacitados para trabajar y personas que perciben una pensión distinta de la de jubilación y prejubilación entre otros.

En cuanto a los objetivos específicos, serán:

1. Conocer qué actividades realizan en internet los desempleados que les convierte en más vulnerables. Como ya se ha mencionado anteriormente, este colectivo ha de interactuar, en primer lugar, para que sea visible al potencial agresor. Y

a través del estudio de esta, se pretende demostrar que estas actividades llevan a cabo en internet que las hacen más vulnerables a los ciberdelitos.

2. Demostrar que los fraudes informáticos son los ciberdelitos que más sufren los desempleados. Mediante este objetivo se pretende demostrar que esto es así debido a que los fraudes informáticos son unos de los delitos que más se dan en el ciberespacio, según el Observatorio Español de Delitos Informáticos, el cual establece que este año se han dado 60511 fraudes informáticos (entendemos como fraudes informáticos los tipificados en el Código Penal en los artículos del 248 al 251 y 623.4. Dichos artículos se refieren a las estafas bancarias, con tarjetas de crédito, débito y cheques de viaje y otras estafas realizadas). Atendiendo a la información ofrecida por el Estudio sobre la Cibercriminalidad en España (2017) realizado por el Ministerio del Interior, también podemos decir que el fraude informático representa el 70.4% del total de ciberdelitos conocidos (IMAGEN I). Por tanto, queremos demostrar la correlación entre el hecho de ser desempleado y sufrir un fraude informático.



HECHOS CONOCIDOS	2014	2015	2016	2017
ACCESO E INTERCEPTACIÓN ILÍCITA	1.851	2.386	2.579	2.505
AMENAZAS Y COACCIONES	9.559	10.112	11.473	11.270
CONTRA EL HONOR	2.212	2.131	1.524	1.537
CONTRA PROPIEDAD INDUST./INTELEC.	183	167	121	109
DELITOS SEXUALES(*)	974	1.233	1.188	1.312
FALSIFICACIÓN INFORMÁTICA	1.874	2.361	2.697	2.961
FRAUDE INFORMÁTICO	32.842	40.864	45.894	60.511
INTERFERENCIA DATOS Y EN SISTEMA	440	900	1.110	1.102
Total HECHOS CONOCIDOS	**49.935**	**60.154**	**66.586**	**81.307**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración

Imagen 1
Estudio sobre la cibercriminalidad en España.
Ministerio de Interior

3. C**onocer qué tipos de fraudes informáticos son los que más sufren los desempleados.** Esto se llevará a cabo para poder realizar un programa de prevención en un futuro.

III. **Hipótesis**

Nuestro proyecto de investigación parte de la siguiente hipótesis teórica: **las actividades que realizan en la red los desempleados les hacen más vulnerables a ser víctimas en el ciberespacio**. Según Miró (2015) es importante tener en cuenta que los ciberdelitos engloban tanto delitos relacionados con sistemas o por medios de sistemas informáticos como delitos que afectan a la integridad de la persona (injurias, amenazas, acoso sexual, etc.) en el ciberespacio. Un error común es denominar delincuencia informática en vez de ciberdelitos, ya que este alude a delitos complejos, técnicos y sofisticados realizados sobre sistemas informáticos.

Esta hipótesis se desarrollará a partir de la investigación realizada por Fernando Miró donde comprobó que mayor interacción, introducción y menos autoprotección, en inglés el acrónimo, ISI (*Introduction*, *self-protection, interaction*) conlleva un mayor riesgo de victimización por *online harassment* [1]. Al final de su trabajo incluye una propuesta de futuro, en donde recomienda verificar si las tres variables ISI se cumplen en otro aspecto como en delitos que perjudican en el ámbito patrimonial de los individuos.

Por consiguiente, la variable dependiente de este proyecto de investigación es "la victimización por delitos de fraude informático" y las **variables independientes** que **se medirán y estudiarán son las siguientes:** 1) actividades realizadas en internet por los desempleados en la búsqueda de trabajo y 2) actividades imprudentes en el manejo de las TIC´s. Estas dos variables independientes permitirán poder diferenciar qué individuos son vulnerables por desconocimiento del manejo de las TIC`s y qué individuos son vulnerables por la búsqueda de trabajo (acentuada por su situación de necesidad).

En primer lugar, se pretende conocer las actividades que realizan los desempleados en el ciberespacio, por lo tanto:

H1-1. La situación de desempleo de los individuos está asociada con que realicen actividades que les hagan propensos a sufrir delitos que afecten a su patrimonio.

En esta hipótesis, se operativiza "actividades" de la siguiente manera:, entrar o inscribirse en páginas web de empleo no oficiales, respuesta a correos sospechosos (entendemos "sospechosos": correos de emisores desconocidos, correos spam y correos de entidades bancarias no oficiales), abrir o contestar correos sospechosos de ofertas de empleo; seguir enlaces o descargar ficheros adjuntos que se encuentran en los correos sospechosos de ofertas de empleo.

En segundo lugar, una de las variables del ISI que Miró estudia es *self-protection* que hace alusión a la propia protección que el sujeto realiza. Este término se sustituirá por "el uso inadecuado de las TIC´s" que se operativizará a continuación. La utilización de este término se justifica en que un uso incorrecto de las TIC´s afecta a la probabilidad de ser más victimizado en el ciberespacio.

Estas Tic´s se engloban en diferentes instrumentos electrónicos como la televisión, el teléfono, el vídeo, el ordenador. Por ende, nuestro proyecto de investigación se centrará en:

H1-2. El uso inadecuado de las TIC´s por parte de los desempleados está asociado con que sufran fraudes informáticos.

Esta hipótesis, se operativiza a través de las siguientes actividades: no actualizar frecuentemente el sistema operativo, poseer un antivirus ilegal o no actualizarlo de manera constante, contestar a correos de entidades bancarias falsas; no verificar si accedemos a la página oficial de nuestro banco, descargar ilegalmente de archivos (Tanto archivos mp3, mp4 o libros), entrar en páginas web no seguras, acceder a cuentas bancarias a través de un conexión WIFI que no conocemos o no estamos seguros de su total fiabilidad; abrir correos sospechosos; contestar a estos correos; seguir enlaces o descargar ficheros adjuntos que se encuentran en los correos de contactos conocidos.

IV. Estrategias de investigación

Tras lo explicado anteriormente, consideramos que se debería utilizar una metodología cuantitativa debido a que consiste en la demostración o falsación de la hipótesis anteriormente explicada. Por tanto, se debería utilizar una encuesta, puesto que, es un método que permite la obtención de información de manera estructurada y a gran escala. Por otro lado, es el método de excelencia entre las Ciencias Sociales. Para la realización se tomará como población a los desempleados residentes en el Reino de

España, a través de un muestreo probabilístico aleatorio simple para que los datos puedan ser representativos a nivel nacional.

Bibliografía

AGUILAR CÁRCELES, M. (2015). "Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido". Nº 15: 15 páginas.

CASCALES, M. J. (2015). *La prevención situacional del delito desde el ámbito de la psicología .Elche.*

FAWN T. NGO y RAYMOND P. (2011). "Cybercrime Victimization: An examination of Individual and Situational level factors". International Journal of Cyber Criminology. Nº5: 20 páginas.

GÓMEZ, J. A. (2011). *Cómo se hace un trabajo de investigación en sociología.*

INE. (28 de julio de 2016). *Encuesta de Población Activa (EPA) Segundo trimestre de 2016.*

INE. *Encuesta de Población Activa (EPA) Segundo trimestre de 2016.*

MEDINA SARMIENTO, J; AGUSTINA SANLLEHÍ, J.R; MIRÓ LLINARES, F. y SUMMERS, L. (2015). Crimen, oportunidad y vida diario. Libro homenaje al profesor Marcus Felson., Madrid, Dykinson.

MESEGUER GONZÁLEZ, J.D. (2013). "Los nuevos modi operandi de los Ciberdelincuentes durante la crisis económica". Revista de Derecho UNED, Nº 12.

MINISTERIO DEL INTERIOR. (2017). Estudio sobre la cibercriminalidad en España. En la red: http://www.interior.gob.es/documents/10180/7146983/Estudio+Cibercriminalidad+2017.pdf/a937823d-8af5-4baa-86fa-7f085f7cac07. (Visto el 20/10/2018)

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". Revista Electrónica de Ciencia Penal y Criminología. Nº 13.
Id. (2012). El cibercrimen, Fenomenología y criminología de la delincuencia en el ciberespacio, Madrid, Marcial Pons.

Id. (2013). "La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio". Revista Española de Investigación Criminológica: REIC, Nº 11: 35 páginas.

MIRÓ LLINARES, F.; GARCÍA GUILABERT, N. (2012). "La victimización en el ciberespacio. Modelo explicativo de la ciber-victimización a partir de las teorías de la prevención situacional del delito". Revista Electrónica de Ciencia Penal y Criminología, Nº 55 páginas.

REDONDO ILLESCAS, S.; GARRIDO GENOVÉS, V. (2013). Principios de Criminología. Valencia, Tirant lo blanch.