eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea

Estafas cometidas a través de compras online

Estudio realizado en Donostia-San Sebastián

Grado en Criminología

Año académico: 2016/2017

Realizado por: Irene Casado Pérez

Dirigido por: Gemma María Varona Martínez

ÍNDICE.

1. INTRODUCCIÓN

Aboso y Zapata (2006) afirman que vivimos en una sociedad en la que todas o casi todas las actividades cotidianas se ven influidas por Internet y por el ciberespacio. Evans (2011) también analiza la importancia de la red en la sociedad, y afirma que:

> Internet lo cambia todo, incluso a nosotros mismos. Si bien puede parecer una declaración arriesgada, hay que tener en cuenta el impacto que Internet ha tenido sobre la educación, la comunicación, las empresas, la ciencia, el Gobierno y la humanidad. Claramente Internet es una de las creaciones más importantes y poderosas de toda la historia de la humanidad. (p.2)

Éste ha sido el motivo principal de la elección del ciberdelito –más particularmente de las estafas producidas a través de compras online- como tema principal para llevar a cabo el trabajo desarrollado a continuación.

Actualmente Internet es uno de los medios más utilizados tanto para el uso personal como para la comisión de hechos delictivos de múltiple índole, que pueden afectar a una gran variedad de derechos fundamentales -intimidad, indemnidad sexual, honor, derecho a la propiedad, etc.- (Morón, 2007).

En el 2016 el delito económico online era uno de los comportamientos ilícitos que más se llevaron a cabo junto con la corrupción, el soborno y la apropiación indebida de activos (INESE, 2016). Todo esto hace que sea necesario estudiar la ciberdelincuencia, para así poder preverla y evitar que vaya en aumento los años próximos.

El presente trabajo tiene una doble vertiente, por un lado, se realiza una exploración bibliográfica del ciberespacio, del ciberdelito en general y de los ciberdelitos económicos en particular. Y por otro lado, se desarrolla el análisis de una encuesta de percepción de inseguridad en Internet, realizada durante el transcurso de las prácticas obligatorias de la Universidad en la Guardia Municipal de Donostia-San Sebastián, entre el 25 de enero y el 18 de marzo del año 2016.

En cuanto a la primera parte de la investigación, tal y como acabo de mencionar, se comienza analizando el ciberespacio desde una visión más general, centrándose primeramente en el análisis de la influencia que tienen las nuevas tecnologías en el

comportamiento humano y qué ámbitos de su vida diaria se han visto altamente influenciados por las TIC. Posteriormente se realiza el examen del ciberespacio como un nuevo espacio para delinquir, cuyas características tanto extrínsecas como intrínsecas pueden favorecer la comisión de ciertos ciberdelitos.

Siguiendo la línea del estudio del ciberespacio, se lleva a cabo un análisis de las cibervíctimas, centrándose en uno de los debates que más importancia puede tener con relación a éstas y que puede influir en su posible no denuncia, en el foco de este debate se encuentran dos posturas, por un lado se encuentra el hecho de que las posibles víctimas tienen que llevar a cabo ciertas medidas de seguridad no automatizables –entre las que se incluyen la presencia de antivirus, de contraseñas, etc.-, además de utilizar de forma juiciosa sus datos bancarios en la red, con el objetivo de disminuir la posibilidad de convertirse en víctima de un ciberdelito en el futuro. Todo ello frente a la postura contradictoria, que se centra en el hecho de que la víctima no tiene que sufrir todo el peso de la comisión de un ciberdelito, ya que como consecuencia de todas las características que tiene el ciberespacio, que se comentarán posteriormente, los posibles ciberdelincuentes pueden ver favorecidas las posibilidades de comisión de un delito online.

Para acabar con el análisis del ciberespacio, se examinan los perfiles de las posibles cibervíctimas y de los ciberdelincuentes de hoy en día.

Continuando con la primera parte del trabajo, para ir especificando más en el objeto de la investigación, se comienza con el análisis del ciberdelito en general. Primeramente se realiza un estudio de las distintas diferenciaciones que existen dentro de los ciberdelitos. También se analizan las teorías de la oportunidad y de las actividades cotidianas como posibles explicaciones del delito online. Y se continúa examinando el “efecto iceberg” que tienen los ciberdelitos, es decir, la gran cifra negra de denuncias que ostentan los delitos cometidos a través del ciberespacio.

Finalmente, el análisis de los ciberdelitos no podría estar completo sin un examen de los mismos dentro del Derecho Penal. Por un lado, se realiza el estudio de los diferentes bienes jurídicos a proteger para poder castigar de forma correcta este tipo de delitos, y por otro lado, se examina cómo están recogidos en el actual Código Penal los diferentes tipos de delitos que se pueden cometer a través de la red. Siguiendo esta misma línea, también se analiza una de las características más

importantes de los ciberdelitos, que es la transnacionalidad, es decir, como consecuencia de la universalidad del ciberespacio, el emisor y el receptor de una acción en la red pueden estar separados por miles de kilómetros (Wall, 2007).

Se acaba el estudio del ciberdelito en general con dos conceptos que son muy importantes dentro de la comisión de un acto ilícito a través de Internet. Estos conceptos son el miedo al ciberdelito y la percepción de inseguridad en la red –este último se encuentra en el centro de la investigación-.

Para finalizar la primera parte del estudio, se comienza por analizar los ciberdelitos económicos, pero más particularmente las estafas o fraudes cometidos a través de la red. También se examina la estafa informática realizada por medio del uso fraudulento de las tarjetas bancarias. Este es el punto principal del presente trabajo, y a partir de este momento todo irá orientado a este tipo de delitos.

Se estima como uno de los puntos claves para este trabajo el hecho de poder analizar, por un lado, tres encuestas realizadas a grandes empresas con el fin de conocer si han sido víctimas de algún tipo de delito económico, de saber cómo regulan las actividades que realizan en Internet y más en general, de averiguar cuál es su grado de ciberseguridad. La primera de las encuestas se efectuó por Muñoz y Aranda (2011) en 72 países. La segunda de ellas por López, Muñoz y Aranda (2014) en 99 países. Y la última de ellas también por López, Muñoz y Aranda (2016) en 115 países. Por otro lado, también se otorga importancia al estudio de una encuesta de ciberseguridad realizada por Gómez y Urueña (2014) a 3074 hogares españoles, con el fin de conocer si han sufrido o no algún tipo de fraude o estafa a través de la red, y de examinar qué hábitos utilizan tanto para la seguridad de su equipo como para la de sus datos bancarios o personales a la hora de llevar a cabo compras online.

Los fines principales por los que se decide realizar el análisis de estas encuestas son, primeramente, para apoyar la versatilidad del papel de Criminólogo, que puede trabajar tanto en grandes empresas como con personas de a pie, otra de las razones guarda relación con el hecho de resaltar que la ciberseguridad es importante tanto en grandes empresas y en la economía de mercado, como en el conjunto de la ciudadanía –que pasa a ser el objeto de estudio- y finalmente, para poder contextualizar la segunda parte del trabajo, que es una encuesta de percepción de inseguridad en Internet realizada a ciudadanos de Donostia-San Sebastián.

Tal y como se acaba de mencionar, en la segunda parte del presente trabajo, se analiza una encuesta semiestructurada realizada durante la ejecución de las prácticas obligatorias de la Universidad en la Guardia Municipal de Donostia-San Sebastián, entre el 25 de enero y el 18 de marzo de 2016, en la que se tiene como objetivo general conocer qué grado percepción de inseguridad tienen los ciudadanos de esta ciudad con respecto a Internet. Asimismo el sondeo contará con una serie de objetivos específicos que son:

- Conocer para qué tipo de acciones utilizan más los usuarios encuestados Internet.
- Si los sujetos encuestados saben diferenciar entre una página web legal y una ilegal –entendiendo como una página web ilegal cualquier portal creado única y exclusivamente para captar los datos bancarios de los usuarios y poder utilizarlos sin su consentimiento-.
- Qué problemas ven los usuarios encuestados al uso diario de la red.
- Si los sujetos encuestados creen que Internet es un entorno seguro para adquirir bienes y/o contratar servicios.
- Si los usuarios encuestados realizan las transferencias bancarias a través de la red o prefieren ir directamente al banco.
- Determinar qué métodos de pago son los más utilizados por los sujetos encuestados.
- Si estos usuarios encuestados confían en la protección de sus datos personales a través del ciberespacio.
- Si creen que por medio de la red a veces se ve vulnerado su derecho a la intimidad.
- Y por último, si los sujetos encuestados creen necesaria una regulación de Internet en el ámbito de protección de sus datos personales.

Finalmente la encuesta se efectuó a 73 sujetos que residían en los diferentes barrios de Donostia-San Sebastián, por lo que el estudio no es representativo de la población total de dicha ciudad, sino que los resultados solamente se pueden englobar a los sujetos encuestados. La metodología utilizada es cuantitativa, ya que se usa una técnica de encuesta que busca operacionalizar o traducir realidades sociales en datos numéricos. Asimismo el sondeo cuenta con preguntas abiertas, cerradas y semicerradas, pero en su mayoría está compuesto por preguntas cerradas. Las

respuestas son de tres tipos, de elección rápida –en la que los sujetos tienen que marcar con una X-, respuestas dicotómicas –en los que se debe responder si o no- y escala Likert de 1 a 5 puntos, que tiene la misma puntuación en toda la encuesta, 1 = nada o poco seguro y 5 = mucho o muy seguro.

Finalmente, además de las conclusiones principales que suscita el análisis de los resultados de la encuesta, se recogen una serie de planes de mejora que, si tanto los usuarios de Internet, como la plataformas del Gobierno las llevasen a cabo, cabe pensar que para los potenciales infractores sería más difícil poder efectuar ciertos ciberdelitos, ya que las oportunidades de comisión se verían reducidas.

2. MARCO TEÓRICO

2.1 CIBERESPACIO: CONTEXTUALIZACIÓN

Miró (2011) en uno de sus estudios, se planteó la posibilidad de determinar si el ciberespacio se ha convertido en un nuevo espacio para delinquir, y también quiso examinar en qué medida las teorías de la oportunidad y las teorías criminológicas de las actividades cotidianas pueden explicar éste nuevo concepto de ciberdelincuencia.

Las TIC y la evolución de Internet han hecho que en los últimos años se haya creado una nueva forma de delincuencia a través de un nuevo medio, conocida como cibercrimen o ciberdelito (Solano, 2013). Éste se entiende como todo tipo de delitos que se cometen en el ámbito de Internet o que se ayudan de la red para ser perpetuados. Se ha requerido este término de cibercrimen o ciberdelito frente a otros, como puede ser el término "delitos informáticos", ya que según Di Piero (2013) no determina la verdadera importancia del uso de la red.

Tal y como afirma Wall (2007) esta nueva forma de delinquir es tan preocupante porque se lleva a cabo desde el ciberespacio, donde hay una gran universalidad, y donde el emisor y el receptor pueden estar separados por miles de kilómetros de forma simultánea. También resulta muy alarmante el hecho de que a través del ciberdelito pueden estar afectados bienes jurídicos de muchos tipos penales, tales como la intimidad, el patrimonio, el honor, la indemnidad sexual, la propiedad, etc. (Rayón y Gómez, 2014).

En este sentido y según Agustina (2014):

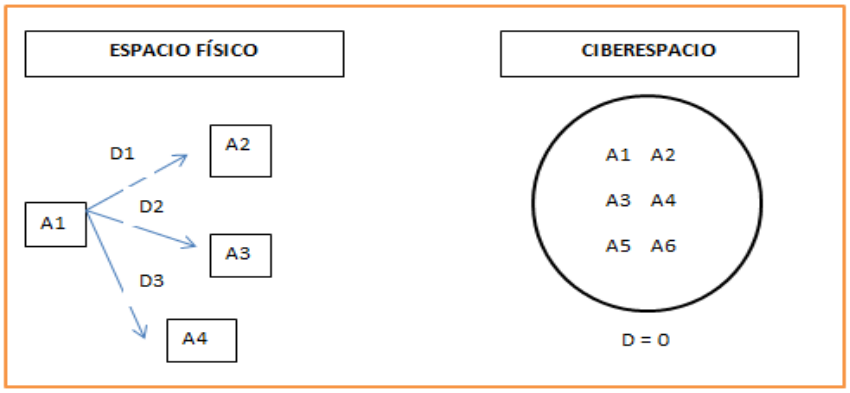
> La red es tanto un lugar criminógeno, en el sentido de que por sus mismas condiciones genera delincuencia, como un espacio propicio que atrae al delincuente a cometer sus delitos, en el que existen menos riesgos de ser detectado y abundan distintos objetivos altamente atractivos. (p.148)

El crimen cambia en Internet (Tamarit, 2016) y siguiendo la teoría de las actividades rutinarias de Cohen y Felson (1979) un crimen se va a producir cuando coinciden en el tiempo y en el espacio, un objetivo, un delincuente y la inexistencia de un guardián que pueda evitar que ese delito se lleve a cabo. En la red este hecho no se va a

producir de la misma manera que en el espacio físico, y por ello pasaré a analizar las particularidades principales que hacen que el ciberespacio sea un nuevo espacio para delinquir.

La red tiene una serie de caracteres, tanto intrínsecos como extrínsecos, que voy a analizar a continuación. Comenzando por los primeros he de afirmar que en la red cambian tanto el espacio como el tiempo en la comisión de los delitos. He ahí la diferencia entre el espacio físico y el ciberespacio. En la red no existe una naturaleza física en la comunicación entre individuos, y por tanto se determina que nos enfrentamos a un tipo de espacio que es totalmente invisible a nuestros sentidos, ya que, como he comentado anteriormente, el sujeto emisor y el receptor pueden estar separados por miles de kilómetros (Miró, 2011).

La relación entre el espacio y el tiempo es directa, porque cuando uno se contrae el otro lo hará de la misma forma. Es decir, lo que en el espacio físico pueden ser horas o incluso días, en el ciberespacio puede ocurrir en pocos minutos, en pocos segundos o de forma inmediata. Lo mismo ocurre con el espacio, lo que en el espacio físico está dividido por mucha distancia, en ciberespacio no se va a apreciar, tal y como se ve reflejado en el siguiente gráfico:



[1]*Gráfico 1: Contracción de la distancia en el ciberespacio y expansión de la capacidad comunicativa:* A1 necesita d=0 para comunicarse con A2, A3, A4, etc.

[1] 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, 13(7)*, 1-55.

En el ciberespacio es muy complejo determinar el espacio y el tiempo de comisión de los delitos, y esto a su vez afecta al hecho de que hay una gran dificultad a la hora de delimitar el ámbito geográfico-espacial que puede tener cualquier tipo de acción en la red. Es decir, no se puede especificar con exactitud el instante temporal en el que comienza una acción en el ciberespacio.

Otra de las características del ciberespacio es que el sujeto que comenzó siendo sujeto pasivo, se puede convertir en sujeto activo en cualquier momento, ya que cuando una persona genera una acción en Internet, ésta es susceptible de ser manejada por un sujeto diferente al que la creó (Miró, 2011). Puede que un usuario realice alguna acción en Internet, como puede ser, por ejemplo, "colgar" un trabajo o un vídeo en alguna página, y en el mismo instante en el que el sujeto ha realizado dicha acción, cualquier otro individuo que se encuentre en la red puede localizar dicho trabajo o dicho vídeo y realizar con él la acción que desee –siempre que el sujeto activo de la actuación no haya prohibido a través de cualquier plataforma que dicho comportamiento se pueda repetir por otra persona- y de esta forma, el sujeto pasivo se puede convertir en sujeto activo.

A continuación detallaré los caracteres extrínsecos del ciberespacio. Comenzaré analizando la deslocalización de Internet. Una de las singularidades básicas de la red es la dificultad para poder localizar de una forma concreta al autor o emisor de una acción. Está claro que se puede definir con facilidad la IP del ordenador transmisor, pero no la persona que está utilizando dicho ordenador. Otra característica que va unida a la deslocalización es la transnacionalidad del ciberespacio –que analizaré posteriormente- puesto que en Internet no existen fronteras como ocurre en el espacio físico (Rayón y Gómez, 2014). Por lo tanto, la comunicación y la interacción se producen entre individuos de diferentes Estados con total simultaneidad. La siguiente peculiaridad está relacionada con la no centralización de Internet, es decir, en este espacio prima la distribución tanto de individuos como de contenidos, lo que fomenta la globalización.

Pero sin duda la singularidad más importante de la red es la neutralidad, que abarca tanto la libertad de expresión de cualquier tipo de usuario, como el anonimato. Esto ocurre ya que el control de información y de contenidos es muy complejo en el ciberespacio (Miró, 2011). Además, el grado de ocultación del que estoy hablando es

tal que, es muy difícil poder determinar al autor de ciertos delitos con la "facilidad" con la que se puede determinar en el espacio físico. Cuando utilizo la palabra "facilidad" para el espacio físico me estoy refiriendo al hecho de que, en este espacio, el autor de un crimen puede dejar huellas, pelo, saliva o cualquier otro vestigio mediante el cual puede ser identificado. En cambio en el ciberespacio esto no puede ocurrir.

La universalidad y la popularización de la red también se deben tener muy en cuenta. Hace unos años Internet solo lo utilizaban las industrias y las empresas para llevar a cabo su trabajo. Hoy en día cualquier persona tiene un móvil o un ordenador con el que conectarse a la red, con un bajo coste, lo que impulsa aún más el consumo masivo de las TIC. Por consiguiente, cabe pensar que, tanto la popularización del ciberespacio, como las facilidades para adquirirlo, han hecho que actualmente los medios electrónicos sean los medios más utilizados tanto para la información como para la comunicación e incluso para la comisión de crímenes, como fraudes o estafas.

Por último, para acabar con las características de la red, cabe destacar que las TIC están abiertas a una evolución permanente y esto hace que también tengan que cambiar las leyes a medida que avanzan las tecnologías. Es decir, en el ciberespacio el derecho no está tan definido como en el espacio físico, y a veces se ve altamente influido por todos estos factores que he analizado hasta el momento e incluso a veces el crimen se ve favorecido por ellos.

2.1.1 INFLUENCIA DE LAS TIC EN EL COMPORTAMIENTO Y DESARROLLO HUMANO

El crecimiento y la rápida evolución de las TIC ha hecho que se haya producido un cambio en el modelo de sociedad, desde la revolución tecnológica que se llevó a cabo en el siglo XX hasta la sociedad en la que vivimos actualmente (Dubois y Cortés, 2005). Según Dubois y Cortés (2005):

> Una simple enumeración de los ámbitos que, en primera instancia, quedan modificados por las TIC incluye la difusión de los conocimientos, el comportamiento social, las prácticas económicas y empresariales, el compromiso

> político, los medios de comunicación, la educación, la salud, el ocio y el entretenimiento. (p.6)

Actualmente Internet es el motor principal de nuestra sociedad denominada "sociedad red" (Castells, 2014), aunque esa denominación no es la única existente para remarcar la importancia de las TIC en nuestro día a día. Asimismo otras de las designaciones existentes son "sociedad del conocimiento" o "sociedad de la información" (Arias, 2011). A través de estas nomenclaturas se puede apreciar claramente que en la sociedad actual se le da una gran importancia al conocimiento como base para todo tipo de procesos, ya sean sociales, económicos, culturales, políticos, etc.

Gracias a Internet y a las conexiones inalámbricas podemos realizar interacciones y comunicaciones sin ningún tipo de límite espacial, lo que puede fomentar que la sociedad red sea una sociedad de redes globales. Sin duda el ámbito de nuestra vida diaria que más ha evolucionado gracias a Internet es el de las comunicaciones "hasta el punto de llegar a convertirse en un medio global de comunicación hoy día cotidiano en nuestras vidas" (Dentzel, 2014, p.9). Pero tal y como afirma Castells (2014) esta sociedad es una "sociedad egocéntrica" en la que el proceso de individualización ocupa un lugar muy importante, siendo éste "el resultado material de las nuevas formas de organización de la actividad económica, la política y la vida social" (p.13). Pero con esto no se quiere afirmar que individualización sea sinónimo de marginación o aislamiento, ya que en esta nueva sociedad se combinan comportamientos individuales y en comunidad, con interacciones tanto virtuales como físicas. También es importante determinar que las nuevas tecnologías no es que nos conviertan en otra persona, aprovechándose de la individualización que éstas pueden generar, sino que nos hacen aprovechar las oportunidades de diferente manera a como lo haríamos en un mundo sin TIC, en realidad éstas nos ayudan a ser nosotros mismos en un espacio lleno de nuevas oportunidades para realizar lo que a nosotros no gusta de una forma fácil y cómoda (DiMaggio, 2014).

Desde la creación de Internet hasta nuestros días ha habido una gran revolución que está marcando la actividad que los usuarios realizan en la red. Esta revolución es referente a las redes sociales que actualmente según Castells (2014):

> Se han convertido en las plataformas de preferencia para todo tipo de fines, no solo para relacionarse y charlar con amigos, sino también para *marketing*, comercio electrónico, enseñanza, creatividad cultural, medios de comunicación y ocio, aplicaciones médicas y activismo sociopolítico. (p. 17)

Cuando las redes sociales comenzaron a utilizarse su uso era básicamente la comunicación con individuos tanto amigos como desconocidos, lo que fomenta la socialización, pero actualmente el uso masivo de este tipo de redes ha hecho que las empresas, los medios de comunicación, la política, etc. tenga un perfil con el que poder plasmar ideales y noticias a tiempo real con personas reales. Por ello la "realidad virtual" ya no es una realidad ficticia creada a través de Internet, sino que es un tipo de "virtualidad real" en la que "prácticas sociales, como compartir, mezclarse o vivir en sociedad se ven facilitadas por la virtualidad" (Castells, 2014, p.18).

Tal y como he comentado anteriormente, una de las características del ciberespacio más importantes es que gracias a éste nos podemos liberar de las barreras tanto espaciales como temporales que pueden marcar la comunicación social a través del medio físico. Esta singularidad de la red, sumada a la instantaneidad que ostentan las nuevas tecnologías, hacen que los sujetos nos comuniquemos con individuos de diferentes países y continentes de forma simultánea. Esto se puede ver claramente referido a través de las redes sociales que, desde su creación, han cambiado la forma de comunicarse con los seres queridos, y según Dentzel (2014) han llegado a transformar incluso las relaciones afectivas, ya que actualmente todos estamos conectados a los demás de una forma más inmediata y más directa a través tanto de la pantalla del ordenador, como del teléfono móvil o tablet. Esto puede generar una gran dependencia directa con la pareja, familia, amigos, etc. lo que no tiene por qué ser negativo, ya que dependerá del grado de dependencia emocional que se suscita en cada individuo.

Otro de los ámbitos principales que se han visto alterados por la creación de Internet ha sido la educación. El ciberespacio es un entorno lleno de información que ha creado una nueva forma de aprendizaje, el "aprendizaje en red". "En Internet las personas pueden colaborar para crear y compartir conocimientos, y desarrollar nuevas maneras de enseñar y aprender" (Dentzel, 2014, p.12). Esto se encuentra totalmente ligado con otro de los caracteres del ciberespacio, que hace referencia al

hecho de que el sujeto pasivo se puede convertir en sujeto activo en cualquier momento, llevándonos esto a la práctica, el individuo que está realizando la búsqueda de cualquier tipo de información puede seleccionarla parcialmente e incluso decidir si quiere seguir informándose o no hacerlo, de esta forma se convierte en sujeto activo.

La cultura también se ve altamente influida por la evolución de la red. A través del ciberespacio se pueden dar a conocer de una forma fácil y sencilla múltiples propuestas, obras de arte, ideas, música, cine, conocimientos, etc. Según Dentzel (2014): "Internet no es solamente una tecnología, sino que es una producción cultural en sí misma" (p.16), fomentando la innovación en todos los aspectos mencionados anteriormente.

El siguiente de los ámbitos de la sociedad que se han visto altamente influidos por la rápida evolución de las TIC son las empresas. Como consecuencia de dicho desarrollo éstas han cambiado la relación con sus clientes, la forma de comunicarse con sus proveedores, los métodos de pago, las formas de marketing, los métodos de compra, etc. (Castells, 2001). Actualmente existen empresas puramente online que sólo venden productos a través de la red como son: Amazon, Ebay, Privalia, entre otras. Estas empresas han sabido aprovechar las oportunidades que generan tanto Internet como el gran número de compradores que ven a la red una forma rápida y cómoda de realizar transacciones. De esta manera se han creado empresas-red en las cuales "la red es la empresa" (Castells, 2001, p.4), con esta afirmación quiero determinar que en este tipo de empresas la mayoría de las acciones empresariales se llevan a cabo a través de la red.

El último de los ámbitos de cambio de los que voy a hablar en mi trabajo, como consecuencia de la creación y evolución de Internet, está muy relacionado con el punto anterior, éstos son los hábitos de consumo. A través de la red se pueden adquirir todo tipo de bienes –muebles, casas, ropa, alimentos, accesorios, coches, etc.-. Éste es el ámbito fundamental en el cual me voy a basar en mi estudio. Actualmente el comercio online puede facilitar "el acceso a todo tipo de comparativas y listas de productos, opiniones y valoraciones de usuarios, recomendaciones de *bloggers* reconocidos, etc.", todo ello "configura un nuevo escenario para el consumo, el comercio y la economía" (Dentzel, 2014, p.17).

Realmente cabe pensar que hay una relación directa entre la creación de las empresas-red y la evolución del comercio electrónico, ya que considero que cuantas más empresas haya facilitando la adquisición de bienes a través de Internet, mayor será el número de demandantes de dichos bienes, y viceversa.

2.1.2 CIBERAGRESOR MOTIVADO, OBJETIVOS ADECUADOS Y FALTA DE GUARDIANES EN EL CIBERESPACIO

Como he comentado anteriormente el ciberespacio tiene una serie de características que pueden favorecer la comisión de ciertos ciberdelitos. Una de ellas hace referencia al hecho de que a través de los medios electrónicos no se aprecia el espacio –tal y como he descrito varias veces con anterioridad-. Esto ocurre al contrario que en el espacio físico, que para que un individuo se convierta en posible víctima de algunos delitos, debe estar en contacto directo con un agresor; por ejemplo, en los casos de homicidio, robo, hurto, agresión, abuso, etc. En el ciberespacio no pasa igual, y las dos personas implicadas en un delito pueden estar separadas por miles de kilómetros, como he recalcado varias veces a lo largo de este trabajo. Este hecho se encuentra impulsado por el anonimato y por la rápida evolución de las TIC, y por ello considero que existen muchas más probabilidades de que los cibercrímenes aumenten en número los próximos años.

Tal y como afirma Miró (2011) una característica que puede hacer que un potencial infractor se encuentre motivado para cometer un ciberdelito es el hecho de que, con una única actuación criminal, se puede tener más de una víctima. Esto es también una de las singularidades de las estafas o de los fraudes informáticos. No obstante, tampoco nos confundamos, ya que en el espacio físico también se puede producir este hecho, pero en el ciberespacio las facilidades son mayores. Otra singularidad que puede motivar al potencial infractor, es el hecho de que a través de la red se puede ocultar y puede llevar a cabo actuaciones ayudándose del anonimato. El anonimato provoca que el agresor tenga menos miedo de ser identificado, y consecuentemente, menos miedo de ser detenido. Con la globalización de Internet aumentan las situaciones en las que coinciden en el ciberespacio un agresor motivado y un objetivo adecuado, y por lo tanto, aumentan las posibilidades de que se cometa un crimen o un ciberdelito.

Para poder comprender lo que es un objetivo -adecuado o no- en el ciberespacio, desarrollaré un ejemplo: en el contacto directo entre un potencial agresor y una víctima en el espacio físico, todos los bienes de la víctima se encuentran expuestos al agresor -por lo tanto, en este caso, los objetivos serán estos bienes-. Pero en el ciberespacio solamente se encuentran expuestos los bienes que la víctima quiere exponer, esa es una de las diferencias entre el ciberespacio y el espacio físico. En éste último la víctima muestra al infractor todas las pertenencias que tenga en ese momento –por ejemplo: en los casos de hurto o robo- pero en el caso de la red es la víctima la que decide exponer, por ejemplo, su cuenta bancaria a cualquier potencial infractor que esté dispuesto a receptarla. La posibilidad de que el objetivo se convierta en adecuado o no, depende del infractor y de la valoración que haga del mismo.

Analizando esta última idea Felson desarrolló los posibles condicionantes que pueden hacer que un objetivo se convierta en adecuado para un infractor. Estos condicionantes se pueden determinar dentro del acrónimo VIVA (Vozmediano y San Juan, 2010). Estas cuatro letras determinan que para que un infractor convierta un objetivo en adecuado es importante el Valor del objeto –que debe ser elevado-, la Inercia –que hace referencia al peso del objeto, por ello los artículos de gran valor y poco peso son los más elegidos entre los infractores-, la Visibilidad –el objeto debe estar a la vista del potencial infractor- y el Acceso al mismo –es relativo a la posible cercanía del objeto a la puerta del salida del establecimiento, por ejemplo-. Este acrónimo se utiliza más en el espacio físico, en el ciberespacio es diferente.

El acrónimo utilizado en la red es IVI (Miró, 2011) y hace referencia a las características que pueden hacer que un ciberinfractor convierta un ciberobjetivo en adecuado. La primera de las letras define el hecho de que el objetivo sea Introducido en el ciberespacio –por ejemplo, cuando un sujeto introduce sus datos bancarios en la red-, la segunda determina el Valor del objeto, que debe ser apetecible para el potencial infractor –en el caso de la cuenta corriente del usuario, el infractor debe tener una predisposición para recoger datos personales en la red de terceras personas- y por último, el bien debe Interaccionar con el agresor de forma telemática –en el ejemplo que estoy desarrollando, la cuenta bancaria del usuario tiene que entrar en contacto con el infractor para que éste la pueda adquirir-.

Para finalizar con el análisis del ciberdelito falta una característica que puede fomentar el aumento del crimen en Internet. Hasta ahora hemos analizado el potencial infractor y la posibilidad de que los objetivos se conviertan en adecuados para él. Falta el estudio de la ausencia de guardianes que puedan evitar la comisión del crimen. Todas las características del ciberespacio que he comentado anteriormente pueden favorecer la ausencia de guardianes, que son los que tienen la función de proteger a la posible víctima. No es que en Internet no haya límites ni leyes, lo que ocurre es que la incidencia de éstas parece tener menos fuerza. En el caso del ciberespacio es la víctima la que va a incorporar sus propios guardianes capaces, es decir, es la propia víctima la que en ocasiones determina su propia autoprotección –siempre refiriéndome a los delitos contra la propiedad, como estafas informáticas a través de compras online, por ejemplo, ya que en éstos casos es la propia víctima la que va a realizar acciones en la red que la pueden perjudicar-.

En conclusión, el hecho de que las TIC estén en constante desarrollo y evolución puede hacer que los usos que los individuos hacen hoy en día de las nuevas tecnologías cambien. Y por ello, todos los análisis que se hacen del ciberespacio y del ciberdelito pueden quedarse anticuados en unos años.

2.1.3 VICTIMIZACIÓN EN EL CIBERESPACIO

Miró (2013a), en otros de sus estudios, quiso determinar cómo aumenta o disminuye el riesgo de victimización en el ciberespacio. En esta investigación se plasma la idea de que la víctima juega un papel importante en la creación de algunos tipos de delitos llevados a cabo en Internet. Esto es así puesto que a veces es la propia persona la que elige qué datos plasma en la red, con qué personas habla o qué tipo de contraseñas son las que protegen sus datos personales. En general podríamos afirmar que el papel de la víctima constituye un componente significativo para la posible creación de un futuro ciberdelito, es decir, es la propia víctima la que en ocasiones tiene que llevar a cabo ciertas conductas de autoprotección para reducir las oportunidades de sufrir un delito online (Agustina, 2014). Con ello me refiero a conductas tales como: utilización juiciosa de datos bancarios para realizar compras, cambio de contraseñas

temporalmente, presencia de antivirus, evitar la interacción con ciertos individuos, etc.

Éste dato abre un gran debate existente actualmente sobre la posible culpabilización de la víctima en ciertos ciberdelitos económicos. Éste tipo de delitos son de índole ocupacional y en ellos los ciberdelincuentes aprovechan ciertas oportunidades existentes en ciertos espacios para tomar la decisión de cometer el delito. Para poder aprovechar todas las oportunidades que les brinda el ciberespacio, los ciberdelincuentes tienen que hacer un balance sobre lo que para ellos son buenos ciberobjetivos, tal y como he mencionado en el punto anterior. Es en este momento en el que la contribución de la víctima en la creación de las oportunidades óptimas para la comisión del ciberdelito es importante (De la Cuesta y Pérez, 2010).

Este es uno de los puntos principales de las teorías de la prevención situacional del delito que en ciertas ocasiones pueden definir la ciberdelincuencia. El objetivo principal de estas teorías es "influir en las actitudes de las potenciales víctimas con la finalidad de reducir las oportunidades delictivas y hacer más difícil la comisión del delito" (De la Cuesta y Pérez, 2010, p.112). Hay varias técnicas de prevención situacional que pueden entorpecer la comisión de ciertos delitos, estas son (Summers, 2009):

1) Aumentar el esfuerzo: control de accesos, control de salidas, etc.
2) Aumentar el riesgo: aumento de guardianes, vigilancia natural y formal, reducción del anonimato, etc.
3) Disminuir las ganancias: ocultar o eliminar objetivos, identificar la propiedad, etc.
4) Reducir las provocaciones: evitar disputas, disuadir imitaciones, eliminar estrés y frustraciones, etc.
5) Eliminar excusas: establecer reglas, incrementar los sentimientos de culpabilidad del infractor, facilitar la toma de decisiones no delictivas, etc.

En el caso de los ciberdelitos solamente caben destacar los tres primeros grupos de técnicas de prevención situacional que, según De la Cuesta y Pérez (2010), hacen referencia a:

1) Aumentar el esfuerzo: endurecimiento de los objetivos –estrategias de protección de los datos-, control de acceso –contraseñas-, desviación de transgresores –evitar que haya muchos individuos problemáticos en el mismo lugar a la misma hora-.
2) Aumentar el riesgo: vigilancias, control de objetivos.
3) Reducción de ganancias: ocultar o eliminar los objetivos –no colocar cierta información personal en cualquier lugar del ciberespacio-.

Ahora bien, muchos de los estudios sobre cibercriminalidad han determinado que la mayoría de los ciberdelitos se cometen por la ineficacia o por la inexistencia de ciertos sistemas de seguridad. Asimismo las empresas o los particulares deben llevar a cabo "la adopción de ciertas medidas preventivas adecuadas para la seguridad del sistema informático que permitieran disuadir al potencial delincuente cibernético de la comisión del ilícito" (De la Cuesta y Pérez, 2010, p.114). Por lo tanto, con el hecho de evitar la comisión de ciertos ciberdelitos económicos, "la modificación del comportamiento de la víctima consigue, por ende, una reducción de los riesgos derivados de las oportunidades espaciales" (De la Cuesta y Pérez, 2010, p.115).

Según la teoría de la prevención situacional del delito, es importante el hecho tanto de que la víctima tenga un buen sistema de seguridad, como de que las contraseñas que protejan sus datos personales sean tales que puedan disuadir a ciberdelincuente para evitar que acceda dentro de su sistema operativo. Por ello, en los ciberdelitos es muy significativo influir en el comportamiento de la posible víctima en el ciberespacio, para poder reducir los riesgos y las oportunidades de comisión de ciertos ciberdelitos económicos (De la Cuesta y Pérez, 2010).

Otro dato muy importante referente a la cibervictimización es que, a mayor interacción con personas tanto conocidas como desconocidas y a mayor uso de la red, cabe pensar que hay mayor riesgo de ser víctima de ciberdelitos (Álvarez, 2009). Y si a esta afirmación se suma el hecho de que la persona no lleve a cabo conductas de autoprotección, el riesgo de victimización puede ser mucho mayor.

Pero no hay que inculcar en la víctima el único peso de sufrir la comisión de ciberdelitos, analizando la cibervictimización desde la rama de la Victimología y según el autor Agustina (2014):

> La relación entre el ofensor y la víctima, mediada por "máscaras virtuales", facilita al ofensor el recurso a apariencias engañosas, técnicas de camuflaje y de manipulación, y potencian en la víctima una serie de déficits cognitivo-conductuales que incrementan notablemente los riesgos de victimización. (p.158)

Estas "máscaras virtuales" pueden hacer que el ofensor parezca otra persona totalmente diferente a la que es en el mundo físico y pueda utilizar el engaño como factor principal para cometer un hecho ilícito hacia un individuo concreto, que pasará a convertirse en la víctima del ciberdelito.

A continuación comenzaré a desarrollar las características de las víctimas en el ciberespacio según Agustina (2014). Antes de comenzar a describirlas, he de afirmar que no es la única clasificación existente para definir a la posible víctima de un ciberdelito, ya que existen muchos sujetos que tienen una personalidad más fuerte que otros y tienen menos posibilidades de ser influenciados por las TIC.

La primera de las características que puede definir a las posibles víctimas de ciberdelitos en la red es la desinhibición que ésta puede generar. Es decir, los usuarios cuando se encuentran navegando por Internet pueden realizar conductas que en el mundo físico no llevarían a cabo, y esto se puede ver reforzado por el anonimato que origina el ciberespacio y por las "máscaras virtuales" de las que he hablado en el punto anterior, que pueden hacer que se cree un "yo virtual" muy diferente al "yo real" en el mundo físico. La desinhibición que genera la red puede ser tan elevada que los usuarios pueden realizar conductas arriesgadas para su integridad y de esta forma tener más riesgo de ser victimizados en el futuro.

La segunda de las características de las que habla este autor está relacionada con los jóvenes de la actualidad, los cuales han crecido en la era digital y desarrollan todas sus actividades diarias en la red. Según Agustina (2014):

> El efecto desinhibidor en la persona genera una aceleración de la conducta en una dinámica en el uso de las TIC (…) y se traslada a la esfera decisional del sujeto en términos de una mayor confianza o relajación en sus interacciones (ingenuidad) y en una ausencia de reflexividad en sus procesos de toma de decisiones (irreflexividad). (p.166)

Y esos son los dos caracteres que, junto con la desinhibición ocasionada por Internet, pueden tener grandes efectos en el autocontrol del individuo, que se verá en gran

medida disminuido a causa de las TIC. Consecuentemente a esto el sujeto tiene muchas más posibilidades de realizar conductas arriesgadas y de convertirse en potencial víctima de un ciberdelito. Por todo ello se debería inculcar a la sociedad una educación basada en ciberdelincuencia, sobre todo a las personas jóvenes del siglo XXI, que son los que más utilizan los medios electrónicos y los que menos peligro ven a las redes (Agustina, 2014).

Según Montiel (2016), en relación con los jóvenes de la actualidad:

> Numerosos estudios empíricos basados en la perspectiva teórica de la victimología del desarrollo revelan que los menores de edad son el grupo más vulnerable en el ámbito victimológico y su victimización es más frecuente que aquella que experimentan los adultos. (p.120)

Se ha creado un nuevo término denominado "cibercriminalidad social" en el que existen diferentes formas de violencia interpersonal que no hace falta que ocurran a través del contacto físico entre dos o varias personas como ocurría hasta el momento, sino que con la rápida evolución de las TIC basta con una mínima conexión al ciberespacio a través de cualquier tipo de dispositivo para llevarlas a cabo. Varios ejemplos claros de este tipo de cibercriminalidad son: el cyberbullying –abuso de poner continuado frente a un menor sobre otro realizado a través de las TIC (Miró, 2013b)-, el happy slapping –agresiones y abusos de poder grabadas a través de cualquier medio electrónico-, el grooming –acciones realizadas por un adulto hacia un menor con el fin de poder abusar sexualmente de él- y el sexting –envío de imágenes de carácter sexual a través del teléfono móvil-.

En esta misma línea Montiel (2016) afirma que "los resultados de numerosos estudios de cibervictimización y ciberdelincuencia apuntan que la adolescencia es la etapa del ciclo vital de mayor riesgo de victimización y agresión en línea" (p.127) y por ello debe ser el colectivo en el que se debe inculcar mayor educación en ciberdelitos.

Para finalizar el apartado de cibervictimización me gustaría concluir con una frase que afirma Agustina (2014) en uno de sus artículos que debería ser la base principal para realizar cualquier actuación en Internet, ésta es: "no hacer en el mundo virtual lo que no haría en el mundo real" (p.178).

2.1.4 PERFIL DE POSIBLES CIBERDELINCUENTES Y CIBERVÍCTIMAS

Comenzaré por analizar el perfil del ciberdelincuente actual, que ha sufrido una modificación en los últimos años (De la Cuesta y Pérez, 2010). Anteriormente un delincuente informático era un joven que quería obtener ciertos conocimientos, cierto poder y una reputación entre sus compañeros, o por el contrario era un simple trabajador que quería vengarse de alguna empresa en particular, sin ningún tipo de ánimo de lucro. En los últimos años, tal y como he comentado anteriormente, este perfil ha sufrido una serie de modificaciones que ha hecho que el ciberdelincuente haya evolucionado a la vez que lo han hecho las nuevas tecnologías. Actualmente el perfil del ciberdelincuente es un "sujeto varón, de entre 25 y 35 años de edad" (Mateos, 2013, p.20) con ciertos conocimientos técnicos previos que persigue fines económicos o lucrativos y que dirige sus acciones hacia grandes plataformas del Estado, "afectando gravemente a la seguridad, integridad y fiabilidad de la información de los datos que la representan" (De la Cuesta y Pérez, 2010, p.101).

En nuestra sociedad siguen existiendo los sujetos que individualmente se aprovechan de ciertos problemas en algún sistema de seguridad para adquirir la información interna existente en él y poder lucrarse con ella, pero lo que más define a la cibercriminalidad de hoy en día es la criminalidad organizada, es decir, grandes grupos de personas que utilizan ciertos conocimientos técnicos cualificados para poner en riesgo la seguridad de grandes plataformas del Estado, y de esta forma obtener grandes cantidades de dinero.

Antes de comenzar con el análisis del perfil de las posibles cibervíctimas, es importante poder analizar el perfil del defraudador español que realizan López, Muñoz y Aranda (2016) en la encuesta sobre fraude y delito económico. En ésta, López, Muñoz y Aranda (2016) afirman que:

> La mayoría de los infractores son hombres de entre 41 y 50 años (…) la antigüedad media en la empresa de los diferentes actores de los delitos es mayoritariamente más de 10 años (…) cerca de la mitad de los infractores ostentan cargos intermedios (…) los delitos han sido cometidos en un 59% de los casos por trabajadores en posesión de un título universitario. (pp. 11-12)

En segundo y último lugar voy a analizar los perfiles de las víctimas de ciberdelincuencia, en este sentido "se establece el hecho de que cualquier ciudadano, empresa o Gobierno que tenga presencia en el ciberespacio se encuentra expuesto a las miradas de los ciberdelincuentes" (Mateos, 2013, p.28). Según Mateos (2013) en lo referente a las personas de a pie, los individuos que tienen más riesgo de sufrir un ciberdelito, y por ende, pueden responder al perfil actual de las cibervíctimas, son los jóvenes de entre 16 y 24 años de edad, que responden a los sujetos que más utilizan y más se apoyan en la red para cualquier tipo de acción en su día a día. "Este hecho podría ser debido a la falta de preparación y educación, en cuanto a las medidas de seguridad necesarias para el uso de la red" (Mateos, 2013, p.30).

El segundo perfil de posible víctima de un ciberdelito son las empresas, claramente se puede pensar que éstas son un blanco muy importante para los ciberdelincuentes por el gran volumen de economía que algunas de ellas pueden generar. Según Mateos (2013) el hecho de que la mayoría de los individuos trabajen en el sector servicios hacen de éste un sector vulnerable a la hora de sufrir un ciberdelito, ya que la mayoría de los ciberdelincuentes buscan adquirir información confidencial de la empresa comprometiendo así la seguridad tanto de la misma como de los clientes que ésta pueda tener.

La última de las posibles víctimas potenciales de un ciberdelito que he mencionado anteriormente son los Gobiernos, "centrales energéticas, redes de suministro eléctrico y cualquier otra infraestructura gubernamental relacionada con las tecnologías de la información, suponen puntos vulnerables para los Gobiernos y sus ciudadanos" (Mateos, 2013, p.39). Actualmente se encuentran a la orden del día las bandas organizadas que utilizan el ciberterrorismo para captar individuos, plasmar sus ideales radicales y realizar ataques masivos, todo ello puede generar una amenaza tanto nacional como internacional. Pero a veces, en el caso del Gobierno, es muy difícil poder determinar con exactitud cuando éste actúa como ciberdelincuente o como cibervíctima (Mateos, 2013).

2.2 CIBERDELITO: CONTEXTUALIZACIÓN

Morón (2007) afirma que la delincuencia a través de la red puede tener dos tipos de consecuencias delictivas: la primera de ellas puede afectar a bienes jurídicos fundamentales que el Código Penal protege de forma principal –patrimonio, intimidad, derechos de autor, propiedad, etc.-. Estos bienes jurídicos se ven vulnerados por los medios informáticos a través de programas espías, Phishing, Pharming, distribución de pornografía infantil, sexting, grooming, etc.

La segunda de las consecuencias afecta al buen funcionamiento de la red, que se puede ver perjudicado cuando estas plataformas son atacadas con accesos no autorizados, difusión de virus, troyanos, etc.

Di Piero (2013) define el cibercrimen como todo tipo de conductas que están impulsadas o beneficiadas por Internet y que afectan a uno o a varios bienes jurídicos de múltiple índole. Hay dos grandes grupos de cibercrímenes según Di Piero (2013).

El primero hace referencia a la función que han cumplido las TIC dentro del comportamiento criminal y el segundo a la incidencia de ese comportamiento en la sociedad. Dentro del primer grupo hay dos tipos, por un lado se encuentran los comportamientos que solamente se pueden llevar a cabo con ayuda de las TIC -denominados ciberataques puros-; y por otro lado se encuentran los actos que ya tenían su existencia en el mundo físico pero que también se han producido en el mundo telemático –designados como ciberataques réplica-.

Cuando hacemos referencia a la incidencia que han tenido los comportamientos criminales en la sociedad, los ciberataques se denominan cibercriminalidad social, económica o política, dependiendo de qué objetivo sea prioritario en el ataque criminal. A continuación plasmaré una tabla para entender mejor dichos tipos de cibercriminalidad:

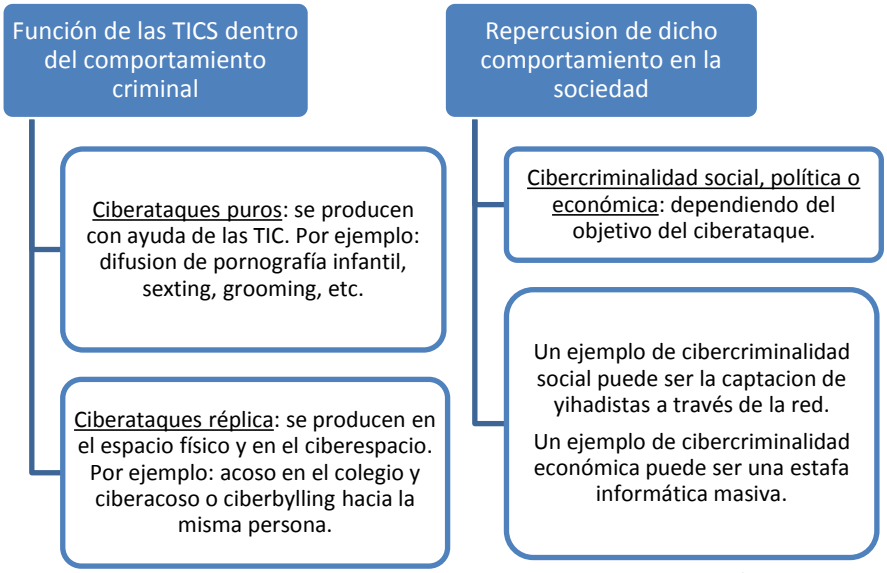


Gráfico 2: Tipos de ciberdelitos según Di Piero[2].

Mata y Martín (2007) también establece dos tipologías para dividir los ciberdelitos. La primera hace referencia a los hechos criminales que solamente se pueden llevar a cabo a través de algún medio informático, dentro de este grupo se encontrarían las estafas informáticas –de las que hablaré más adelante-, la difusión de material pornográfico, el ciberterrorismo, el ciberbullying, el sexting y el grooming.

Dentro de la segunda de las tipologías están los delitos que recaen sobre el sistema informático pero que no necesitan de él para ser cometidos. Este tipo de ciberdelitos son, entre otros, la alteración de daños en algún tipo de archivo informático, los daños a un servidor o la copia o falsificación de una obra protegida por derechos de autor.

2.2.1 TEORÍAS DE LA OPORTUNIDAD Y DE LAS ACTIVIDADES COTIDIANAS COMO POSIBLES EXPLICACIONES DEL CIBERDELITO

Gran parte de los estudios criminológicos sobre la cibercriminalidad y el ciberdelito tienen un punto común. Este punto común es la afirmación de la existencia de una correspondencia entre el cibercrimen y las teorías tanto de la oportunidad como de las actividades cotidianas de Cohen y Felson (1979).

[2] Di Piero, C. (2013). El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. *Revista para el análisis del derecho, (3)*, 1-6.

La Criminología Ambiental es una rama de la Criminología que estudia la relación entre el delito y el ambiente, centrándose en la elección racional del delincuente y en la prevención situacional del delito (Vozmediano y San Juan, 2010). La elección racional hace referencia al conjunto de hechos que van a determinar que un delincuente cometa un delito o decida no hacerlo, siempre teniendo en cuenta que el ambiente está lleno de oportunidades para la comisión de acciones ilegales. En la elección racional, el delincuente evalúa los posibles resultados positivos que puede tener la comisión del delito, comparándolos con los posibles riesgos de ser detenido por las fuerzas y cuerpos de seguridad. De esta forma va a llegar a la conclusión de cometer el acto o no hacerlo. Pero hay que determinar que esta teoría tiene ciertas limitaciones a la hora de explicar el ciberdelito, ya que muchos delincuentes no son racionales, y a la hora de cometer un delito no tienen la capacidad para poder evaluar los posibles riesgos que puede conllevar dicha comisión.

La segunda de las teorías mencionadas anteriormente es la prevención situacional del delito, ésta afirma que la posibilidad de delinquir no se encuentra solamente en la decisión del delincuente, sino que el ambiente está plagado de oportunidades que provocan nuestra posible elección de delinquir y afectan a esta toma de decisiones.

Las Teorías de las Actividades Cotidianas pueden explicar el fenómeno del cibercrimen (Miró, 2011) ya que afirman que, con la evolución tecnológica y la globalización, se producirá el aumento de la criminalidad relacionada con las TIC. Esto ocurre porque se van a poder unir un mayor número de potenciales infractores y de posibles víctimas en un contexto en el que habrá muy pocos o ningún guardián que pueda evitar la comisión del hecho delictivo, y es justamente lo que ocurre en el ciberespacio.

2.2.2 EFECTO “ICEBERG”

El efecto “iceberg” en los ciberdelitos hace referencia a la existencia de una gran cifra negra (De la Cuesta y de la Mata, 2010), es decir, que el número de denuncias existentes sobre ciberdelitos es mucho menor que el número real de delitos. La falta de denuncias que ocasionan los ciberdelitos se pueden ver favorecidas por las características de la red que he comentado anteriormente, entre las que se pueden

encontrar tanto el anonimato como la baja probabilidad de castigar a los autores de los delitos debido a la dificultad para poder detenerlos.

La gran cifra oculta que existe en los ciberdelitos también se debe a que éstos son un tipo de acciones ilícitas que necesitan un elevado nivel de investigación para poder conseguir detener al culpable del delito. Según Agustina (2014) "la investigación policial en el ciberespacio es especialmente compleja debido, en ocasiones, a la alta sofisticación con que cuentan los ciberdelincuentes; y/o que el delito se comete mediante sistemas o canales que dificultan la identificación del ofensor" (p.150).

Pero actualmente el delito online con el número de cifra negra más elevado es la cibercriminalidad social juvenil (Montiel, 2016). Normalmente este tipo de conductas no se denuncian por el miedo que tienen las víctimas a las posibles represalias que puede tener el hecho de acusar al agresor ante las autoridades del colegio, instituto, tutores legales o incluso ante la policía. Además este tipo de conductas entre adolescentes se ven en ocasiones como un "juego de niños" que no tiene la gravedad suficiente como para ser un delito que debe ser perseguido, investigado y castigado. Según Montiel (2016) "modificar estos esquemas cognitivos es imprescindible si se quiere reducir la elevada cifra negra en estos fenómenos y conocer la magnitud real del problema" (p.127).

2.2.3 CIBERDELITO Y DERECHO PENAL

Para poder estudiar qué tipo de conductas ilícitas, llevadas a cabo en Internet, deben ser castigadas lo primero que hay que hacer es determinar qué bien jurídico debe ser protegido. En este aspecto hay dos criterios que apuntan información totalmente contradictoria: el primero de ellos advierte que se debe crear un nuevo apartado dentro del Código Penal en el que se castiguen individualmente los ciberdelitos; y el segundo de los criterios es partidario de agotar primero todos los bienes y delitos castigados en el Código Penal vigente, y luego anotar en ellos las modificaciones concretas necesarias (González, 2007).

La posición doctrinal mayoritaria es la que afirma que se deben estudiar nuevos bienes jurídicos a proteger para poder castigar de forma correcta los ciberdelitos.

Según González (2007) estos bienes jurídicos son: la seguridad informática, la libertad informática y la invulnerabilidad de los datos informáticos.

En el caso de la seguridad informática es un bien jurídico colectivo que puede hacer referencia tanto a un individuo en particular, como a la red en general. Lo voy a explicar claramente en dos casos diferentes: en el caso de referirse a un individuo, la seguridad informática engloba, por ejemplo, el acceso a un ordenador ajeno aunque no sea para cometer un delito, ya que esto puede afectar de manera directa a otro tipo de bienes del individuo como serían la intimidad, el patrimonio, la libertad, etc. En el caso de la red en general, se puede hacer referencia, por ejemplo, a las conductas ilícitas relacionadas con la creación de un virus que se puede adentrar en cualquier ordenador o incluso afectar a la buena circulación de la red.

Refiriéndonos a la libertad informática hacemos referencia a la autodeterminación que tiene cada individuo para poner los datos personales que él quiera tanto de su familia, amigos, pareja, como de él mismo, en Internet. Tiene mucha relación con el derecho a la privacidad, y por lo tanto será castigada cualquier persona que afecte a la intimidad de otro individuo, por ejemplo, divulgando información que el usuario no quiera que aparezca en la red.

El último de los bienes a proteger es la invulnerabilidad de los datos informáticos, con ella también hacemos referencia al artículo 264 del Código Penal. En este artículo se denominan los daños como la "destrucción, deterioro o menoscabo de bienes ajenos". Esto se convierte en delito de daños informáticos al demostrarse una conducta dolosa, es decir, intencionada. El artículo 264 del Código Penal ha sufrido un cambio en julio de 2015 en relación con la cantidad dañada, ésta no debe exceder los 400 euros, lo cual en la práctica supone un endurecimiento de las penas en tanto que desde entonces se considera delito a algo que antes estaba tipificado como falta.

Asimismo una vez analizados los bienes que se deben de proteger para poder saber qué delitos se deben castigar y de qué manera, y una vez introducida la reforma que sufrió el Código Penal el año 2015[3], voy a reflejar como aparecen los ciberdelitos

[3] España. Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (Ley Orgánica 1/2015, 30 de marzo). Boletín oficial del Estado, nº 77, 2015, 31 marzo.

después de dicho cambio en el actual Código Penal español. En dicha reforma se produjeron numerosas supresiones de artículos –en concreto 32- y se modificaron otros 252. A mi parecer en el ámbito de los ciberdelitos se necesitaba una modificación de artículos, ya que en esta sociedad, conocida como la sociedad de la información y de la tecnología, hay muchas maneras de delinquir en el ámbito de Internet que necesitaban una articulación más específica.

El Ministerio del Interior (2015) en su anuario estadístico establece cómo quedan divididos los diferentes tipos de delitos que se pueden llevar a cabo a través del ciberespacio, asimismo estos ciberdelitos quedan expuestos de la siguiente manera:

TÍTULO VI, CAPÍTULO II, de las amenazas:

- Artículos 169 a 171 (incluido): regulan las amenazas por medio de cualquier TIC tanto a una persona concreta, a su familia o a cualquier otra persona con la que esté íntimamente vinculada, como a un grupo étnico, cultural o religioso.

TÍTULO VI, CAPÍTULO III, de las coacciones:

- Artículos 172, 172 bis y 172 ter (incluido): son referentes a las coacciones a través de las TIC, cuando un individuo o bien obligue a otro a hacer algo que no quiere o bien le impida realizar lo que él desee utilizando violencia o intimidación. El artículo 172 ter regula el acoso informático de forma reiterada.

TÍTULO VIII, CAPÍTULO II, de los abusos sexuales:

- Artículo 181: hace referencia a cualquier individuo que, por medio de cualquier TIC, realice actos que pongan en riesgo la libertad e indemnidad sexual de otra persona, sin consentimiento y sin violencia ni intimidación.

TÍTULO VIII, CAPÍTULO II BIS, de los abusos y agresiones sexuales a menores de dieciséis años:

- Artículo 183: es referente al individuo que, a través de cualquier TIC, realice cualquier acto de carácter sexual con un menor de dieciséis años.

- Artículo 183 bis: afecta a cualquier sujeto que, a través de una TIC, obligue a un menor de dieciséis años a participar o a presenciar actos de carácter sexual.
- Artículo 183 ter: hace referencia al que, a través de Internet o de cualquier otra TIC, contacte con un menor de dieciséis años y le proponga concertar un encuentro sexual, un acercamiento o simplemente intente embaucarle para que le facilite material pornográfico.

TÍTULO VIII, CAPÍTULO III, del acoso sexual:

- Artículo 184: afecta a cualquier sujeto que solicite, de forma reiterada, favores de naturaleza sexual a través de cualquier medio informático o TIC.

TÍTULO VIII, CAPÍTULO IV, de los delitos de exhibicionismo y provocación sexual:

- Artículo 185: hace referencia al sujeto que, utilizando cualquier TIC, ejecute u obligue a ejecutar a cualquier individuo actos de exhibición obscena ante menores de edad o incapaces.
- Artículo 186: afecta al sujeto que, a través de cualquier TIC, venda, difunda o exhiba material pornográfico entre menores de edad o incapaces.

TÍTULO VIII, CAPÍTULO V, de los delitos relativos a la prostitución y a la explotación sexual y corrupción de menores:

- Artículo 189: afecta a cualquier persona que capte, a través de Internet o de cualquier TIC, a menores o incapaces para explotarles sexualmente. También se castigará al que suministre, difunda o exhiba pornografía infantil a través de cualquier medio informático o TIC.

TÍTULO X, CAPÍTULO I, del descubrimiento y revelación de secretos:

- Artículos 197 a 201 (incluido): en ellos se regulan la difusión y el acceso de datos de terceras personas sin su consentimiento con el fin de descubrir sus secretos o vulnerar su intimidad. En ellos también será castigado el que, a través de cualquier TIC, revele secretos de terceros sin su consentimiento.

- Artículo 197 bis: relativo al acceso no autorizado a sistemas informáticos. Hace referencia tanto a la intromisión a sistemas informáticos de personas que no tienen licencia para ello, como a la obstaculización de las transmisiones de datos informáticos.
- Artículo 197 ter: relativo a la adquisición y entrega a terceras personas de contraseñas y datos personales de usuarios sin el consentimiento del titular de los datos.

TÍTULO XI, CAPÍTULOS I Y II, de la calumnia y de la injuria:

- Artículos 205 a 210 (incluido): regulan las calumnias e injurias a través de cualquier medio informático o TIC.

TÍTULO XIII, CAPÍTULO VI, de las defraudaciones, sección 1ª de las estafas:

- Artículo 248 a 251 bis (incluido): en estos artículos se castigan las estafas bancarias, las estafas con tarjetas de crédito, débito y cheques de viajes y otras estafas tales como la fabricación o facilitación de programas informáticos con el fin de cometer fraudes informáticos.

TÍTULO XIII, CAPÍTULO IX, de los daños:

- Artículos 263 a 267 (incluido): estos artículos son relativos al individuo que, por cualquier medio informático o TIC, borre o dañe datos informáticos, programas informáticos o documentos electrónicos ajenos.

TÍTULO XIII, CAPÍTULO XI, de los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores, sección 1ª de los delitos relativos a la propiedad intelectual:

- Artículos 270 a 272 (incluido): hacen referencia a los ciberdelitos de la propiedad intelectual. Particularmente en el artículo 270 se castiga a quien, con la intención de obtener un beneficio económico, plagie o distribuya cualquier tipo de información de prestaciones literarias, artísticas o científicas, siempre sin el consentimiento del titular de las mismas. También se encontraría en el artículo 270.2 cualquier persona que distribuya enlaces para llegar a las obras anteriormente indicadas, sin el consentimiento del titular y con intención de lucrarse o de lucrar a terceras personas. En el

artículo 270 básicamente se protegen los derechos de autor, castigando a cualquier persona que intente vulnerarlos a través de cualquier medio informático o TIC. En los artículos siguientes se encuentran los agravantes y atenuantes correspondientes.

TÍTULO XIII, CAPÍTULO XI, de los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores, sección 2ª de los delitos relativos a la propiedad industrial:

- Artículo 273: hace referencia a los ciberdelitos de la propiedad industrial. En él será castigado el que fabrique, utilice u ofrezca en el comercio objetos sin el consentimiento del titular.
- Artículo 274: afecta al sujeto que, con fines industriales y sin el consentimiento del titular, ofrezca o distribuya al por menor o al por mayor productos que se encuentran registrados por otros.
- Artículo 275: se castiga a los sujetos que utilicen el tráfico económico para distribuir un objeto protegido por otro.
- Artículo 276: hace referencia al individuo que haya ganado elevadas cantidades de dinero con la falsa distribución o se encuentre en el seno de una organización criminal.
- Artículo 277: es referente al sujeto que intencionadamente haya divulgado un objeto con una patente secreta.

TÍTULO XIII, CAPÍTULO XI, de los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores, sección 3ª de los delitos relativos al mercado y a los consumidores:

- Artículo 278: en este artículo se castiga al sujeto que se apodere de cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos con el fin de descubrir un secreto de empresa.
- Artículo 279: se sancionará la difusión o cesión de un secreto de empresa producida por el sujeto que tiene el deber de guardarlo a través de cualquier medio informático o TIC.

- Artículo 280: hace referencia al sujeto que realice las acciones descritas anteriormente con conocimiento de su origen ilícito y sin haber tomado parte en el descubrimiento del secreto.
- Artículo 281: el hecho de eliminar del mercado productos de primera necesidad con el fin de desabastecer a un sector de la ciudadanía también será castigado.
- Artículo 282: es referente a los fabricantes o comerciantes que en su publicidad, a través de cualquier medio informático o TIC, hagan alegaciones falsas.
- Artículo 282 bis: el sujeto que falsee la información económica de una empresa a través de cualquier TIC será condenado.
- Artículo 283: en este artículo se castiga al individuo que, en perjuicio del consumidor, facture cantidades superiores por productos o servicios.
- Artículo 284: hace referencia al sujeto que, mediante violencia o engaño, altere los precios de mercancías, productos, títulos, valores o instrumentos financieros, servicios o cualesquiera otras cosas muebles o inmuebles que sean objeto de contratación. En este artículo también se castiga a quien difunda noticias o rumores falsos con el fin de alterar el precio de un valor o instrumento financiero, siempre queriendo obtener para sí mismo o para un tercero un beneficio económico. Por último será condenado el que utilizando información privilegiada, realice transacciones con el fin de proporcionar engaños sobre la oferta, demanda o precio de valores o instrumentos financieros.
- Artículo 285: es referente al sujeto que, de forma directa o indirecta, utilice alguna información para la cotización de valores o instrumentos negociados en algún mercado organizado, siempre que obtenga para sí mismo o para un tercero un beneficio económico superior a 600.000 euros o causando un perjuicio de idéntica cantidad.
- Artículo 286: en este artículo será castigado el que, sin el consentimiento del prestador de servicios y con fines comerciales, facilite el acceso a un servicio de radiodifusión sonora o televisiva, a servicios interactivos por vía electrónica o suministre el acceso a los mismos.

TÍTULO XVIII, CAPÍTULO I, de la falsificación de moneda y efectos timbrados:

- Artículo 386 a 388 (incluido): a lo largo de estos artículos se castiga al sujeto que, mediante cualquier TIC, altere una moneda o fabrique una falsa, introduzca en el país una moneda falsa o modificada y transporte o distribuya una moneda falsa o modificada con conocimiento de su falsedad.
- Artículo 389: hace referencia al individuo que, a través de cualquier medio informático o TIC, falsifique o distribuya sellos de correos o efectos timbrados falsos o los introduzca en España con conocimiento de su falsedad.

TÍTULO XVIII, CAPÍTULO II, de las falsedades documentales, sección 4ª de la falsificación de tarjetas de crédito y débito y cheques de viaje:

- Artículo 399 bis: en este artículo se castiga al individuo que, mediante cualquier TIC, altere o copie cualquier tarjeta de crédito o débito o cheques de viaje. También será condenado el sujeto que tenga tarjetas de crédito, de débito o cheques de viaje falsos listos para distribuir. Y por último se impondrá una pena al sujeto que, con conocimiento de su falsedad, utilice tarjetas de crédito, de débito o cheques de viaje en perjuicio de otro.

TÍTULO XVIII, CAPÍTULO III, disposiciones generales:

- Artículo 400: hace referencia a la fabricación, obtención o tenencia de útiles, materiales, instrumentos, sustancias, datos y programas informáticos, aparatos, elementos de seguridad u otros medios destinados a la comisión de los delitos anteriormente mencionados.

TÍTULO XVIII, CAPÍTULO IV, de la usurpación del estado civil:

- Artículo 401: es referente al sujeto que, mediante cualquier TIC o vía informática, usurpe el estado civil de otro.

También hubo una reforma de la Ley de Enjuiciamiento Criminal en 2015[4] que tiene una gran repercusión en los ciberdelitos, ya que según la nueva redacción del artículo 284 de dicha ley:

> Cuando no exista autor conocido del delito, la Policía deberá conservar el atestado, a disposición del Ministerio Fiscal y de la autoridad judicial, sin enviárselo, salvo que concurra alguna de las siguientes circunstancias: que se trate de delitos contra la vida, contra la integridad física, contra la libertad e indemnidad sexuales o de delitos relacionados con la corrupción; que se practique cualquier diligencia después de transcurridas setenta y dos horas desde la apertura del atestado y éstas hayan tenido algún resultado; o que el Ministerio Fiscal o la autoridad judicial soliciten la remisión.

Por lo tanto al ser de gran dificultad obtener un posible autor de los delitos –como consecuencia de todas las características de la red que he comentado en puntos anteriores- la mayoría de las denuncias no pasarán de comisaría y será mucho más difícil resolver el delito.

2.2.4 CIBERDELITO COMO PROBLEMA TRASNACIONAL

> Es evidente que para hacer frente a esta forma de delincuencia se precisa realizar un enfoque supranacional, con unidades policiales de investigación especializadas y dotadas de los medios técnicos necesarios para la efectividad de su trabajo, e igualmente, se hace preciso un enjuiciamiento rápido y especializado de este tipo de conductas. (Rayón y Gómez, 2014, p.212)

La delincuencia en el ciberespacio siempre va un paso por delante de las leyes penales (Rayón y Gómez, 2014). En nuestra sociedad, denominada la sociedad de las nuevas tecnologías, éstas evolucionan constantemente y siempre va a haber nuevas formas de delinquir dentro de éste gran espacio que es la red.

---

[4] España. Ley de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal y el fortalecimiento de las garantías procesales (Ley 41/2015, 5 de octubre). Boletín oficial del Estado, nº 239, 2015, 6 octubre.

> El ciberespacio ha generado la aparición de nuevas conductas delictivas (…) al tiempo que ha aumentado considerablemente la vulnerabilidad de determinados bienes jurídicos, señaladamente los relacionados con la intimidad, el honor, la propiedad, la autodeterminación informática, la libertad sexual y la seguridad del mercado o del consumo. (Flores, 2015, p.6)

Por todo ello sería muy importante que la ley penal tuviera "tipos penales abiertos" (Rayón y Gómez, 2014, p.230). Estos tipos penales dan una visión más flexible y dinámica para poder castigar este tipo de delitos tan cambiantes.

Unas de las características más importantes de la red y del ciberespacio son la ausencia de fronteras, de límites temporales y espaciales y la supraterritorialidad –esta característica hace referencia al hecho de que la información existente en la red circula a gran velocidad alrededor de todo el mundo- (Flores, 2015). La transnacionalidad de los ciberdelitos, sumada al anonimato que genera la red, hace aún más difícil la persecución, investigación y enjuiciamiento del presunto culpable y por ello es que muchos de los ciberdelitos quedan impunes (Rayón y Gómez, 2014). Asimismo la comisión de un ciberdelito puede llevarse a cabo en uno o varios países de forma simultánea, por una o varias personas que a veces difícilmente se pueden detener. "Obviamente esto afecta a la competencia jurisdiccional, a la ley aplicable y al procedimiento que se tramitará para su investigación y enjuiciamiento" (Rayón y Gómez, 2014, p.215).

El ciberespacio tiene una serie de problemas que claramente entorpecen la posible investigación y enjuiciamiento del presunto culpable, y según Rayón y Gómez (2014) algunos de estos problemas son:

- Cuando un sujeto realiza una acción ilícita en la red, parece que lo hace en un entorno que está totalmente al margen del Derecho, ya que no hay un cuerpo judicial jerarquizado dentro del ciberespacio.
- El hecho de que no haya un cuerpo judicial jerarquizado dentro del ciberespacio fomenta que sea más difícil supervisar todas las acciones tanto lícitas como ilícitas que se pueden realizar en la red.
- El siguiente de los problemas hace referencia a la extraterritorialidad que tienen este tipo de delitos, "lo que conlleva problemas de jurisdicción, de

operatividad policial y judicial, de determinación de la ley y del procedimiento aplicable" (Rayón y Gómez, 2014, p.232).

- La comisión de la ciberdelincuencia tiene que fomentar que todos los Estados tengan una armonización legislativa para que sea más fácil investigar los ciberdelitos. Por lo tanto lo que se debería hacer es "la suscripción de tratados internacionales que intensifiquen la colaboración internacional para hacer frente a la ciberdelincuencia" (Rayón y Gómez, 2014, p.233).

Para poder determinar qué tribunal y en qué país se van a llevar a cabo la investigación y enjuiciamiento del presunto culpable hay que determinar en qué país se ha cometido el ciberdelito, hecho que es muy difícil de concretar como consecuencia de todas las características de la red que llevo comentando hasta el momento. En numerosas ocasiones este hecho produce que se creen supuestos de litispendencia internacional, y esto es, según Flores (2015):

> Un escenario que debe ser evitado porque los conflictos internacionales de jurisdicción provocan, entre otros efectos negativos, tensiones entre los Estados, perjudican una persecución eficaz de este tipo de delincuencia, impiden de ordinario una adecuada satisfacción de la víctima y pueden, en último término, afectar a garantías básicas como el derecho a la tutela judicial efectiva o al principio *non bis in ídem*. (p.10)

Para finalizar con este apartado es de gran importancia poder especificar algunas de las estrategias internacionales de solución de este tipo de delincuencia. Según Flores (2015) algunas de estas son:

- Creación de un Tribunal penal internacional en materia del ciberdelincuencia: la idea es poder crear un Tribunal que solucione algunos de estos problemas internacionales que sufre la comisión de un ciberdelito.
- Utilización de sistemas de ADR para la solución de conflictos de jurisdicción internacional: los sistemas ADR son sistemas de resolución alternativa de conflictos entre los que se encuentran la mediación, el arbitraje y la conciliación.

> Estos métodos tienen, y tendrán en el futuro, una importancia capital en el terreno de los conflictos jurídicos disponibles, dado su bajo coste, su rapidez, la complejidad de las soluciones judiciales en los conflictos transnacionales y la garantía de conocimiento especializado que proporciona un árbitro específicamente elegido. (Flores, 2015, p.21)

- La cooperación internacional y el juez internacional: tal y como he mencionado anteriormente sería de gran importancia que todos los Estados cooperasen entre ellos para poder luchar contra la ciberdelincuencia. Sería muy significativo que todos los Estados tuvieran una armonización legal para que fuera mucho más sencillo investigar y enjuiciar a los posibles culpables de un ciberdelito.
- Modelo del Convenio sobre Ciberdelincuencia de 2001 del Consejo de Europa: este modelo se denomina Convenio sobre la prevención y castigo de la criminalidad informática. El punto más importante de dicho Convenio es la homogeneización de todas las normas relacionadas con la criminalidad informática a nivel internacional.

2.2.5 LÍNEAS DE FUTURO Y NECESIDAD DE ESTUDIO

Tal y como he explicado durante todo el trabajo vivimos en una sociedad cada vez más cibernética. Las TIC en general, y el uso del ciberespacio en particular, va aumentando a gran velocidad (Agustina, 2014).

Consecuentemente a esto si aumenta el número de personas que utilizan la red, cabe pensar que aumentará el número de ciberdelitos, ya que habrá mayor número de potenciales infractores dispuestos a encontrar en ciertos usuarios los objetivos adecuados para ellos; con lo cual se necesitan de forma constante trabajos y estudios sobre estas conductas ilícitas y sobre las posibles víctimas potenciales, además de cambios actualizados en la legislación sobre este ámbito.

Según un estudio de los autores De la Cuesta y San Juan (2010) hay un espacio dentro de la ciberdelincuencia que aún no está estudiado y tiene gran importancia, este ámbito es el miedo al ciberdelito.

En el espacio físico las personas que tienen miedo a sufrir un delito van a intentar reprimir alguna conducta o van a llevar a cabo otro comportamiento con el fin de evitar ser víctima del delito en cuestión. En el espacio cibernético pasará lo mismo y habrá personas que tengan miedo al ciberdelito y personas que no lo tengan. Asimismo las personas que no lo tengan o no lo perciban van a llevar a cabo conductas arriesgadas para su integridad, evitando cualquier tipo de autoprotección y poniendo muchos de sus bienes en riesgo de potenciales infractores (San Juan, Vozmediano y Vergara, 2009).

Para poder comprender lo que es el miedo al ciberdelito debemos diferenciarlo de otro concepto muy similar pero a su vez muy diferente que es la percepción de inseguridad en la red. Conforme a las definiciones que hacen Serrano y Vázquez (2007) de estas dos ideas, podemos afirmar que el miedo al delito es el pánico que tiene una persona a ser víctima de un delito; a su vez la percepción de inseguridad es un concepto más amplio y hace referencia al temor al delito en general, en cuanto a problema social.

Trasladando estos conceptos a mi investigación tener miedo al ciberdelito puede provocar que los usuarios realicen conductas de autoprotección constantemente –como pueden ser: cambio de contraseñas temporalmente, presencia de antivirus, uso responsable de datos bancarios en la red, etc.- ya que el propio individuo tiene un cierto temor a ser víctima de un posible ciberdelito, y cabe pensar que llevará a cabo cualquier tipo de comportamiento que tenga como fin evitar convertirse en posible víctima. La percepción de inseguridad en Internet, tal y como he comentado anteriormente, es un concepto más amplio y todos los individuos que utilizan la red conocen que es un espacio en el cual hay que prestar mucha atención a la hora de realizar conductas arriesgadas para su integridad tanto física como patrimonial, entre otros derechos fundamentales.

Hay algunos autores que sí han estudiado el miedo al delito pero no existe un consenso a la hora de definir este término. La mayoría tienen en común una idea y es que este temor es una experiencia emocional subjetiva (Vozmediano, San Juan y Vergara, 2008).

Llevándonos este último concepto al terreno cibernético, podemos definir el miedo al ciberdelito como la estimación que un usuario hace cada vez que utiliza la red, es

decir, la persona valora tanto los resultados positivos como las consecuencias de sus actos y llega a la conclusión de si tiene la posibilidad de ser víctima de un ciberdelito, y será en este punto donde exista o no exista el miedo al delito online.

Siguiendo esta línea y según un estudio de Vozmediano, San Juan y Vergara (2008), en el ámbito de la ciberdelincuencia hay un matiz que llama mucho la atención. Cuando nos fijamos en las diferentes situaciones resultantes a la hora de combinar los distintos niveles de delito objetivo o delito real con el miedo al delito, llegamos a una conclusión: en el caso de los ciberdelitos, cuando existe una criminalidad objetiva elevada, es decir, cuando hay un gran número de ciberdelitos –como ocurre en nuestra sociedad de hoy en día- hay un miedo al delito bajo. Con esto cabe pensar que a la hora de utilizar Internet, da igual si el número de denuncias es elevado o no, ya que los usuarios van a seguir utilizando la red indistintamente.

[5]*Gráfico 3: Situaciones resultantes de la combinación de diferentes niveles de delito objetivo y de miedo al delito.*

[5] Vozmediano, L. & San Juan, C. (2010). *Criminología Ambiental: ecología del delito y de la seguridad.* Barcelona: UOC y De la Cuesta, J.L. & San Juan, C. (2010). La Cibercriminalidad: interés y necesidad de estudio. Percepción de seguridad e inseguridad. En *Derecho penal informático* (pp. 57-78). España: Cívitas.

En conclusión, el miedo al ciberdelito es una rama de la ciberdelincuencia que tiene mucho interés a la hora de conocer y explicar los ciberdelitos, además de ayudar a la prevención de los mismos. El estudio de la víctima es muy importante en este ámbito ya que, como he comentado en puntos anteriores, es la persona lesionada la que expone sus bienes y la que en ocasiones es la dueña de su autoprotección en Internet. Por lo tanto hay una necesidad de estudio de las personas dañadas por actos llevados a cabo a través de la red, tanto para poder definir los límites del delito informático, como para poder ayudar a su concepción y prevención.

2.3 CIBERDELITOS ECONÓMICOS: CONTEXTUALIZACIÓN

Junto con el aumento de las TIC se ha producido una gran revolución en cuanto al empleo de Internet, esta innovación está relacionada con el uso del ciberespacio para llevar a cabo conductas de carácter económico o financiero, lo que ha provocado que existan muchas personas que utilizan la red para lucrarse con el dinero de los usuarios (San Juan, Vozmediano y Vergara, 2009).

Siguiendo con uno de los estudios de Fernández (2007), hay diferentes tipos de delitos cometidos en el ámbito informático que van a provocar el crecimiento económico de infractores que se lucran con el dinero de terceros. Se pueden dividir en cuatro grupos: mails, comercio electrónico, conexiones telefónicas y obtención de claves de acceso. A continuación analizaré brevemente cada uno de ellos como forma de contextualización.

El envío de mails falsos consiste en mandar de forma intensiva correos electrónicos a los usuarios prometiéndoles ganar muchas cantidades de dinero con premios de lotería, apuestas deportivas, etc. En estos mails aparece escrito de forma muy difícil de captar el hecho de que, si se plasma el número de la cuenta bancaria, se van a llevar a cabo grandes cargos de dinero en dicha cuenta. Además puede darse la opción de que en el mail aparezca un número de teléfono por si el usuario tuviera cualquier tipo de problema o de duda. Este número es internacional por lo que aparte de tener un elevado coste normalmente se suele retener a los usuarios muchos minutos en espera para poder beneficiarse de ellos lo máximo posible.

Los fraudes en comercio electrónico hacen referencia a dos tipos de actividades: la primera está relacionada con la falsa compra de objetos –siempre pagados con antelación- que posteriormente o no llegarán al domicilio o llegarán cambiados por otro objeto; y la segunda está relacionada con el precio del objeto adquirido, que puede ser mucho mayor del prometido en la página donde se lleva a cabo la compra. En este tipo de fraude puede haber dos tipos de víctimas, tanto el particular en sí, como la empresa encargada de colocar el objeto a disposición de terceras personas dispuestas adquirirlo –por ejemplo Ebay, Amazon, Privalia, etc.-.

El tercer tipo de fraude es el que se lleva a cabo a través de conexiones telefónicas ilícitas mediante las cuales a un usuario se le llama desde un número de teléfono con un elevado coste, no informando adecuadamente al individuo de las consecuencias de la instalación del servicio que se quiere prestar y con el fin de que el usuario lo adquiera. Una vez que la víctima ha adquirido el servicio, se le descargará una aplicación en el ordenador denominada "espejo" con el fin de que el estafador se introduzca con total libertad en el historial de actividades del particular y recolecte datos personales del mismo.

Por último el cuarto tipo de fraude está relacionado con la sustracción de las claves de acceso y de los datos bancarios de la víctima con el fin de lucrarse de todos sus bienes económicos. Se puede llevar a cabo de dos formas diferentes: la primera a través de la dirección IP de la víctima y la segunda es el denominado Phishing.

En el primero de los casos, el infractor se aprovecha de que sabe que el cliente utiliza la cuenta bancaria para realizar compras o adquirir servicios a través de Internet. Posteriormente se introduce dentro del ordenador de la persona para adquirir dicho número de cuenta y hacerse pasar por la víctima mediante suplantación de identidad para realizar compras masivas con un elevado coste. La filtración al ordenador del particular se suele hacer a través de aplicaciones que se introducen dentro del mismo y que envían información al infractor de todos los datos personales de la víctima sin que ésta lo sepa.

En los últimos años ha aumentado mucho el número de denuncias sobre el segundo tipo de estafa denominado Phishing (Fernández, 2007). Éste consiste en enviar correos electrónicos de forma masiva a la víctima, en los cuales se manifiestan logotipos y textos aparentemente fiables de páginas web legales para que el cliente se

fíe de ellos. En estos mails se pide al individuo que introduzca su número de cuenta y sus claves de acceso e incluso pueden enviar al sujeto a una página web aparentemente legal, pero creada solamente para recabar datos personales de los usuarios –página web ilegal-. De esta forma estos datos ya están en manos de terceras personas que están dispuestas a lucrarse con su dinero.

Hay una variante del Phishing que es el Pharming, y está relacionado con redireccionar estos correos electrónicos a páginas web aparentemente lícitas, como he comentado anteriormente. En esta otra forma de estafa, que es totalmente complementaria al Phishing, se modifican las direcciones DNS –estas direcciones son las encargadas de llevar a un usuario de Internet a la página que quiere visitar- de tal forma que el estafador creará unas páginas web aparentemente originales con el fin de recabar los datos bancarios de las víctimas.

Normalmente los infractores tienen un modus operandi muy claro, y es el abrir otros números de cuenta y hacer una rápida transferencia ingresando pequeñas cantidades de dinero en todas ellas -el patrimonio procede de las cuentas de los usuarios-. También puede existir una tercera persona que se deja ingresar algo de patrimonio con el fin de enviar al autor de la estafa el dinero, pero no en su totalidad, ya que esta tercera persona se quedará una comisión.

2.3.1 ESTAFAS INFORMATICAS Y USO FRAUDULENTO DE LAS TARJETAS DE PAGO

Son una de las manifestaciones del denominado “lucro ilícito” gracias al dinero de terceros y es consecuencia de una gran innovación que ha sufrido la red en la cual se pueden llevar a cabo actividades de tipo económico y financiero de forma fácil y sencilla (Fernández, 2007).

Las estafas –convencional e informática- se encuentran tipificadas en el Código Penal en el Título XIII, Capítulo VI y Sección I, denominada *de las estafas*, a través de los artículos 248 al 252 bis (incluido). Según el artículo 248 del Código Penal “cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio

propio o ajeno". Es muy importante para mi trabajo poder reproducir el punto 2 de dicho artículo, ya que en él aparece la red como medio de estafa:

> También se consideran reos de estafa: a) los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro; b) los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo; c) los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realizaren operaciones de cualquier clase en perjuicio de su titular o de un tercero.

Hay muchos autores que han estudiado la posible diferencia entre la estafa convencional y la estafa informática. Algunos de ellos creen que son dos modelos de estafa totalmente diferentes entre sí, y que por lo tanto se deben tipificar por separado. Sin embargo otro autor como Javato (2008) tiene otro tipo de pensamiento, éste cree que el delito genérico es el de estafa convencional y que la estafa informática solamente es una adaptación de la anterior a otro tipo de medio de comisión que es Internet.

Como comentaré posteriormente, la estafa convencional se basa en el engaño y en el error, asimismo la estafa informática cambia estos dos términos por el de manipulación informática, entendida por Javato (2008) como "cualquier alteración del resultado de un procesamiento electrónico de datos" (p.5). Este autor hace unas diferenciaciones entre los tipos de manipulaciones informáticas, dependiendo del momento en el que se van a producir. De esta forma podemos distinguir entre: manipulaciones previas, del programa y posteriores. Solamente cabe destacar la manipulación previa, puesto que es una de las más importantes en esta sociedad ya que engloba uno de los fenómenos que más ha aumentado en los últimos años que he comentado anteriormente como es el Phishing –método para conseguir de forma fraudulenta información personal de los usuarios con el objetivo de lucrarse con su dinero-. Dentro de este tipo de manipulación previa nos encontramos también con el acuerdo entre dos personas que compran y venden bienes o servicios en Internet –este método también es clave a la hora de analizar la estafa informática, ya que muchas de ellas se llevan a cabo dentro de los establecimientos comerciales online-.

Otro de los elementos que diferencian la estafa convencional de la estafa informática es “la producción no consentida de la transferencia de activos patrimoniales” (Javato, 2008, p.6). Lo que en la modalidad genérica de estafa el hecho de intercambiar bienes o servicios por bienes patrimoniales se hace de forma activa y personal, en la estafa informática se hace online, de ahí el término “transferencia”, que es relativo a un intercambio no personal.

El tercer y último elemento está muy relacionado con el segundo, y es que ésta transferencia de activos debe de originar en el titular del patrimonio una pérdida no consentida que debe ser “real y efectiva” (Javato, 2008, p.7).

2.3.1.1 UTILIZACION FRAUDULENTA DE TARJETAS DE PAGO

Las tarjetas de pago, ya sean de crédito o de débito, se han convertido en uno de los medios de pago más masivamente utilizados de todos los tiempos (Mata y Martín, 2007). Este uso se produce tanto en el espacio físico –comprando en supermercados, centros comerciales, etc.- como en el espacio cibernético, donde la tarjeta es el método de pago estrella frente a otros métodos de pago como puede ser el contrareembolso entre otros (López, Mata y Bernal, 2010). El hecho de que las tarjetas se utilicen tanto afecta de forma directa a la creación de diferentes tipos de delitos que tengan como objeto la recaudación de los datos personales de las mismas para poder lucrarse con el dinero existente en ellas.

El delito central que se produce cuando una persona, con el número de la tarjeta de otra, adquiere objetos o servicios sin el consentimiento del titular, es el denominado delito de “estafa convencional” –artículo 248 CP-. Para que este delito se produzca se tienen que cumplir determinadas acciones (Mata y Martín, 2007): la primera de ellas es que el autor del hecho debe llevar a cabo una conducta de engaño, la segunda es que el engaño debe causar en el receptor una situación de error y por último, esta situación de error debe tener como consecuencia una pérdida patrimonial del titular de la tarjeta, en este caso.

Cuando nos encontramos con un posible delito de “estafa convencional” en un comercio, por ejemplo, el dueño de la tienda puede pedir el carnet de identidad a

cualquier persona que vaya a pagar con dicha tarjeta, ya sea de crédito o de débito. Pero en los últimos tiempos, como he comentado anteriormente, se ha producido un aumento masivo de los pagos con tarjeta en Internet, lo que provoca desconcierto ya que hay menos posibilidades de saber si la persona que está utilizando este método de pago es realmente el titular o no lo es. Esto ha hecho que se cree una nueva tipología dentro del delito de estafa denominada "estafa informática". En nuestra sociedad, este tipo de estafa ha aumentado tanto en las formas de llevarlo a cabo, como en el número objetivo de delitos, o lo que es lo mismo, en el número de personas que quieren lucrarse con el dinero de terceros (Mata y Martín, 2007).

El legislador quiso crear otro tipo de estafa –artículo 248.2 CP- ya que en la "estafa informática" el engaño y el error que he comentado anteriormente se van a producir de una forma diferente de como se llevan a cabo en la "estafa convencional". El engaño y el error pasan a denominarse manipulación informática, y mediante dicha manipulación el autor del delito quiere conseguir un beneficio económico a través de un tercero sin su consentimiento. La manipulación que acabo de mencionar no se produce a través del engaño de la víctima, como ocurre en el delito de "estafa convencional", sino que "es el propio sujeto activo quien a través de artificios tecnológicos y medios informáticos consigue llevar a cabo tal acción" (González, 2014, p. 35).

2.3.1.2 ESTAFA INFORMÁTICA: CONCRECIÓN FINAL

Una vez que ya conocemos la definición de "estafa informática" y su diferencia con el delito genérico de estafa –"estafa convencional"-, lo siguiente es conocer qué tipo de bien jurídico es el que se protege para poder tipificar este tipo de delito dentro del Derecho Penal.

Está claro que los ciberdelitos pueden vulnerar una serie de bienes jurídicos de múltiple índole, como pueden ser el honor, la intimidad, la libertad, etc., pero refiriéndonos particularmente al delito de estafa informática, hay un bien jurídico que prevalece ante otros mencionados anteriormente, éste es el patrimonio, y según afirma Sánchez (2009):

> Entendido siempre de forma amplia, es decir, como conjunto de derechos, bienes y relaciones jurídicas que puede ser titular un sujeto; encuadrando, por tanto, este tipo delictivo, dentro de la categoría genérica de delitos económicos de enriquecimiento, con la particularidad de tratarse de un tipo de delitos de apoderamiento. (p.121)

En conclusión, cabe pensar que cuanto más vaya evolucionando el uso de Internet, más van a ir evolucionando a su vez los delitos relacionados con el enriquecimiento gracias a uso ilícito de medios de pago online. Según los estudios analizados, se podría considerar que la comisión del delito de estafa informática va a ir aumentando, lo que debe provocar que se endurezcan los medios para adquirir servicios o bienes en Internet, para que las personas que intentan lucrarse con el dinero de los usuarios no tengan facilidades para ello.

Antes de comenzar con la segunda parte de mi trabajo, analizaré varias encuestas realizadas, tanto a empresas como a hogares españoles usuarios de Internet, con el fin de realizar un estudio más completo del ciberdelito.

2.3.2 ENCUESTA ESPAÑOLA SOBRE FRAUDE Y DELITO ECONÓMICO 2011/2014/2016

A continuación voy a realizar un breve análisis referente a las encuestas que se realizaron en los años 2011, 2014 y 2016 sobre fraudes y delitos económicos, centrándome más particularmente en el examen que hacen las mismas sobre este tipo de delitos en España.

La primera de ellas se realizó a nivel mundial –en particular se efectuó en 72 países- por Aranda y López (2011). Según el sondeo "del total de los encuestados, el 53% eran miembros del Comité de Dirección o alta dirección de las organizaciones, el 36% de organizaciones cotizadas y el 38% representantes de las organizaciones con más de 1000 empleados" (Aranda y López, 2011, p.4).

La segunda de las encuestas también se realizó a nivel mundial –particularmente a 99 países- por López, Muñoz y Aranda (2014). A través del sondeo se puede determinar que:

> Del total de los encuestados, el 55,70% eran miembros de Comités de dirección o pertenecían a la alta dirección de las organizaciones, el 32,90% desempañaban su labor en organizaciones cotizadas y el 62% correspondía a representantes de organizaciones con más de 1000 trabajadores. (López, Muñoz y Aranda, 2014, p.5)

La última de las encuestas también fue realizada a nivel mundial en 115 países por López, Muñoz y Aranda (2016). Según lo establecido en el sondeo:

> Del total de los encuestados a nivel nacional, el 47% son miembros de comités de dirección o pertenecen a la alta dirección; el 36,10% desempeña su labor en empresas cotizadas y el 56,60% corresponde a representantes de organizaciones con más de 1000 trabajadores. (López, Muñoz y Aranda, 2016, p.5)

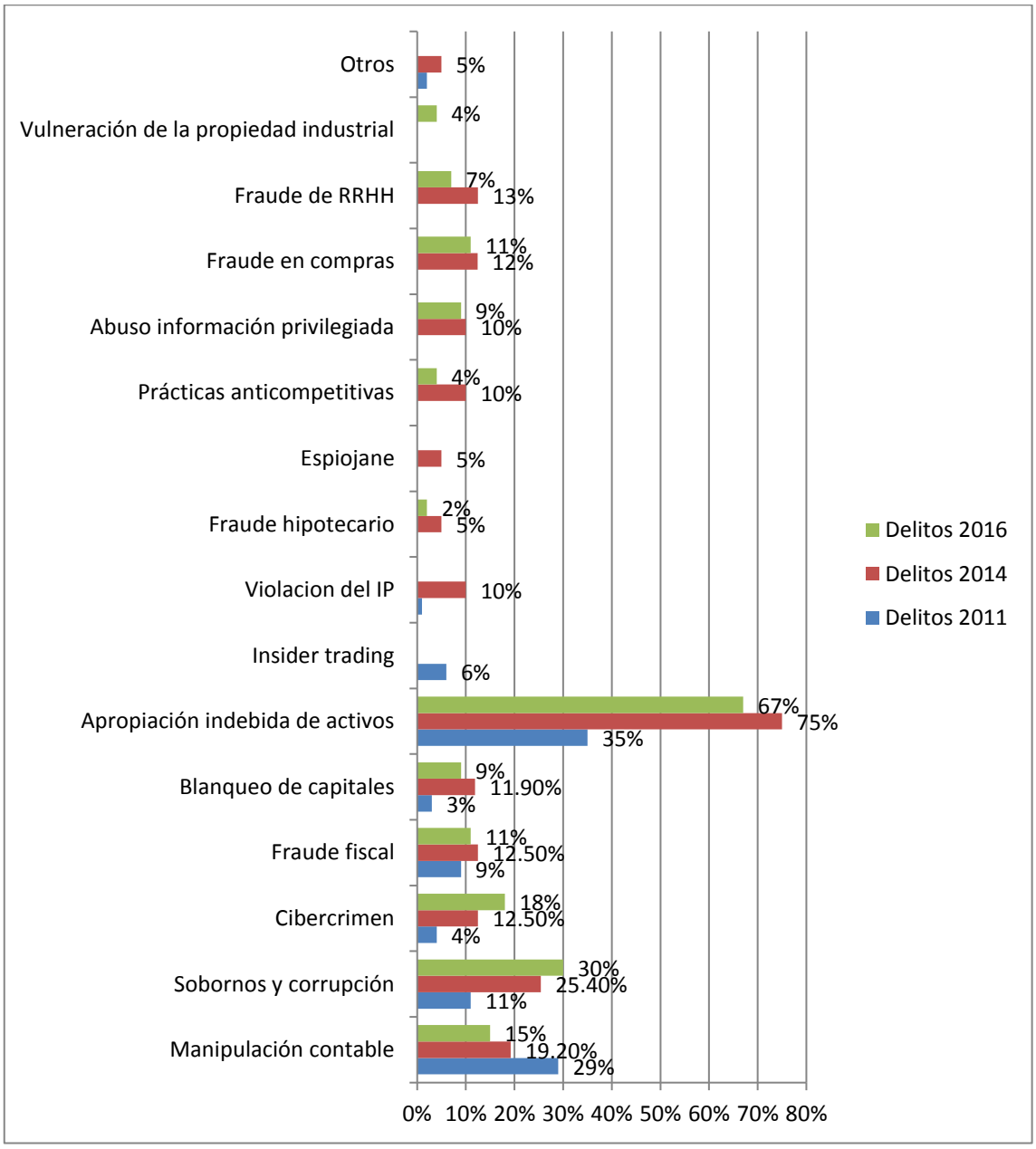
Con la representación de dichas encuestas lo que quiero afirmar es que uno de los ámbitos en los que la ciberseguridad tiene una importancia es en la economía de mercado y en las empresas. Pero la ciberseguridad también tiene especial significación en el conjunto de la ciudadanía, donde puede existir este tipo de sentimiento en la red y éste es mi objeto de estudio. Por ello primero realizaré un análisis de la ciberseguridad en las grandes empresas, para continuar con un pequeño análisis de ésta en los individuos de a pie. De esta forma contextualizaré la posterior encuesta de percepción de inseguridad en la red realizada durante el transcurso de las prácticas obligatorias de la Universidad.

Otra de las razones por las que realizo el análisis de las encuestas de las empresas y de los individuos de a pie es para resaltar el hecho de que la Criminología puede enfocarse en ambos aspectos. Por un lado, un criminólogo puede formar parte de una gran empresa y por otro lado, su labor también se puede enfocar con los sujetos de a pie, analizando sus conductas y sus miedos para poder extraer de ahí conclusiones dirigidas a realizar campañas de prevención segmentadas por grupos de vulnerabilidad, por ejemplo. Ésta última sería una de las estrategias que propongo con mi posterior encuesta de percepción de inseguridad en la red.

Ahora bien, centrándome en analizar las encuestas mundiales sobre fraude y delito económico de 2011, 2014 y 2016 –pero centrándome en los resultados que han obtenido estas en España-, he de especificar que trazaré una serie de tendencias y comparaciones de cada encuesta en una misma gráfica, para que de esta forma sea

más sencillo comprender el cambio o la posible evolución del fraude y del delito económico desde 2011 hasta 2016.

La primera de las gráficas a analizar es la correspondiente a los delitos económicos que han sufrido las empresas encuestadas a lo largo de los últimos 12 meses.



[6]*Gráfico 4: ¿Qué tipo de delitos económicos ha sufrido su organización en los últimos 12 meses? Tendencias de respuesta del 2011 al 2016.*

[6] Fuente: Encuesta mundial sobre fraude y delito económico 2011, 2014 y 2016.

En el año 2011 España se encontraba en el centro de una inmensa crisis económica, con lo cual la mayoría de las empresas españolas encuestadas no se encontraban en su mejor momento, en términos económicos. Esto se ve claramente reflejado en la gráfica anterior, ya que los delitos sufridos por las empresas en 2011 fueron como consecuencia de la posible influencia de la crisis económica que en ese año estaba en su máximo auge. Siguiendo con el año 2011, en el caso de los ciberdelitos, solamente se produjeron en el 4% de las empresas encuestadas, cifra que despierta interés ya que la mayoría de las empresas ya utilizaban Internet para llevar a cabo la contratación de servicios y la realización de sus tareas diarias.

Analizando la gráfica número 4 lo que más me ha llamado la atención es que aumentaron el tipo de delitos económicos que se llevaron a cabo entre el 2011 y el 2016. Mientras que en la primera de las encuestas había 9 tipos de fraudes, en 2014 la cifra aumenta hasta 14 y en 2016 se mantuvo en 12.

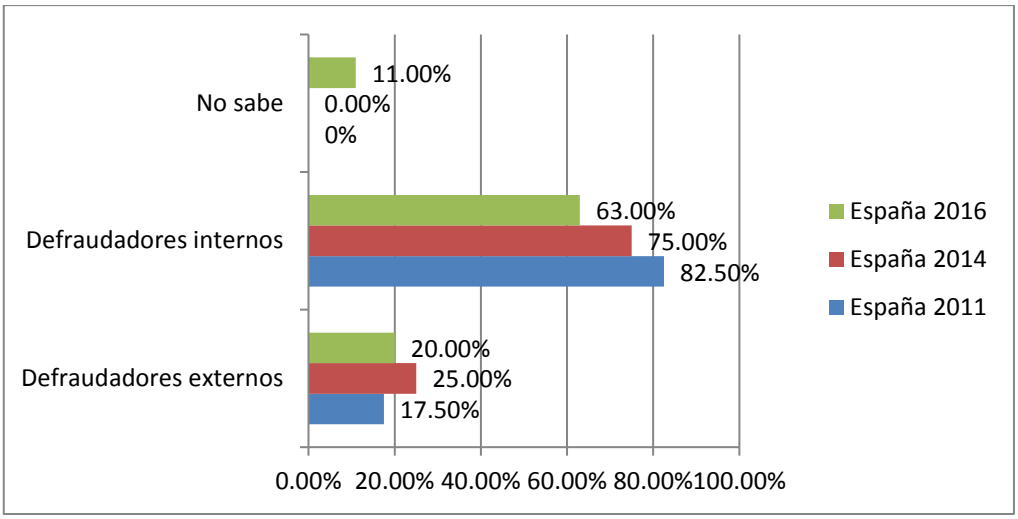
En el caso del año 2014 es donde hay mayor número de tipología de delitos, esto se puede deber por un lado a la Reforma que sufrió el Código Penal en diciembre de 2010. Según la encuesta del año 2014 podemos determinar que cuatro años después de dicho cambio en el Código Penal "el 41,80% de las organizaciones en España implantaron un Modelo de Prevención y Detección de Delitos y un 51,90% realizaron algún tipo de evaluación de riesgo de fraude en los últimos 24 meses" (López, Muñoz y Aranda, 2014, p.36). Por otro lado también es de gran importancia mencionar el Proyecto de Ley de reforma del Código Penal –que en 2014 estaba en vías de ser aprobado- en el cual "la persona jurídica podrá evitar la responsabilidad penal si prueba que cuenta con un modelo de prevención eficaz" (López, Muñoz y Aranda, 2014, p.36). Por lo tanto si muchos de los responsables jurídicos de las empresas que hubieran cometido algún tipo de fraude demostraran que tienen un modelo de prevención mediante el cual no se ha demostrado que dicho delito se haya cometido, cabe pensar que podrían quedar exentos de toda responsabilidad penal.

Tal y como vemos representado en el gráfico anterior la apropiación indebida de activos fue el delito que más se produjo en España tanto en 2011, como en 2014 y 2016, pero la cifra creció considerablemente siendo en el año 2014 donde se encontraba en el punto más elevado -en 2011 la apropiación indebida ocupaba el 35%, en 2014 ocupaba el 75% y en 2016 el 67%-. En el caso de los ciberdelitos la

diferencia de porcentajes entre el año 2011 y el 2016 es evidente, es más la tendencia ha sido aumentar en porcentaje de una encuesta a otra –en 2011 la cifra era de 4%, en 2014 de 12,50% y en el año 2016 los ciberdelitos suponían el 18% del total de los delitos económicos que se cometieron en las empresas españolas encuestadas-. Lo mismo ocurría con los delitos de soborno y corrupción, la tendencia ha ido aumentando a medida que han avanzado los años, en 2011 el porcentaje se encontraba en el 11%, tres años más tarde en el 25,40% y el año pasado el porcentaje aumentó hasta el 30%.

Por último el delito que ocupaba en 2011 el segundo puesto de fraude económico que más se había producido –el delito de manipulación contable-, en el 2014 pasaba a ocupar el tercer puesto, después de la apropiación indebida de activos y de los sobornos y la corrupción e inmediatamente seguido de los ciberdelitos, sin embargo en el año 2016 pasó a ocupar el cuarto puesto, ya que los ciberdelitos han ido ganando terreno a medida que han avanzado los años tal y como he comentado anteriormente.

La segunda de las gráficas que me ha llamado mucho la atención es en la que se plasman los datos sobre qué tipo de defraudadores existían en las organizaciones encuestadas. Me parece muy interesante plasmarla y poder determinar la tendencia de respuesta entre el año 2011 y el 2016 ya que gracias a esta se puede conocer quién ha defraudado más a la empresa, si los individuos que trabajan en ella o sujetos externos a la misma.



[7]Gráfico 5: En relación con el delito económico de mayor gravedad que ha sufrido su organización en los últimos 12 meses, ¿quién fue el principal autor? Tendencias de respuesta del 2011 al 2016.

En el año 2011 el delito de corrupción y/o soborno tenía unas cifras extremadamente preocupantes ya que el porcentaje de defraudadores internos suponía el 82,50%. Es más, según la encuesta, estos delitos de corrupción y/o soborno se llevaron a cabo por los altos y medios cargos.

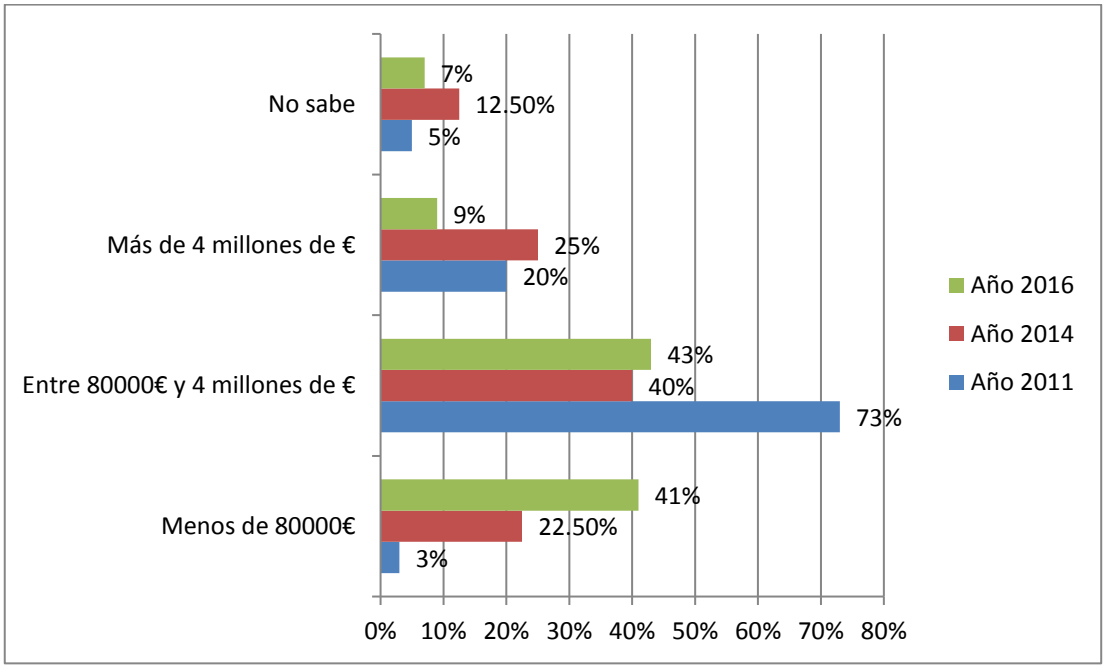
En el caso del 2014 la línea sigue muy parecida a la encuesta de 2011, incluso con menor número de cifras -aunque eran prácticamente similares- el 75% de los defraudadores fueron internos. Todo esto está muy relacionado con la gráfica número 4 ya que es lógico que delitos como sobornos, corrupción, apropiación indebida y manipulación contable hayan sido cometidos por personas que trabajan en la empresa víctima de estos fraudes. Según la encuesta de 2014 "este hecho nos mostraba la necesidad de incrementar las medidas de control establecidas dentro de las organizaciones" (López, Muñoz y Aranda, 2014, p.14).

En el caso del año 2016 el porcentaje de defraudadores internos disminuyó hasta el 63%, pero el porcentaje de la respuesta "lo desconozco" o "no sabe" aumentó del 0% -respuestas producidas tanto en el año 2011 como en el año 2014- hasta el 11% en el año 2016. Además de esto en este último año se estableció un nuevo tipo de respuesta denominada "prefiero no decirlo" que tenía un porcentaje del 7%, lo que hace pensar que, el hecho de que el porcentaje de defraudadores internos haya

[7] Fuente: Encuesta mundial sobre fraude y delito económico 2011, 2014 y 2016.

disminuido, no quiere decir que realmente esto haya ocurrido sino que hay que tener en cuenta que las respuestas "lo desconozco" y "prefiero no decirlo" también pueden hacer referencia a defraudadores internos.

La siguiente gráfica a analizar es en relación a la cantidad de dinero que ha sido defraudada en las empresas encuestadas en los últimos 24 meses.



[8]*Gráfico 6: En términos financieros, aproximadamente, ¿cuánto cree que ha sido el impacto económico para su organización derivado de los delitos económicos sufridos en los últimos 24 meses? Tendencias de respuesta del 2011 al 2016.*

Como se aprecia claramente en el gráfico las cantidades defraudadas de menos de 80.000 euros han tenido una tendencia ascendente a medida que han pasado los años –en el año 2011 el porcentaje era del 3%, en 2014 del 22,50% y el año pasado la cifra llego a ser del 41%-.

Asimismo las pérdidas de más de 4 millones de euros han sido cada vez menores, siendo en el año 2016 solamente del 9%, en comparación con el 2011 y 2014 que eran del 20% y 25% respectivamente. En el caso de las pérdidas de entre 80.000 euros y 4 millones de euros también han disminuido notablemente, lo que en el año 2011 era una cifra increíblemente elevada -75%-, en los años posteriores el

[8] Fuente: Encuesta mundial sobre fraude y delito económico 2011, 2014 y 2016.

porcentaje disminuyó hasta el 40% en el año 2014 y el 43% en el 2016. Es más según la encuesta del año 2016:

> Estos datos ponen de manifiesto cómo, cada vez más, las organizaciones afectadas son más conscientes e invierten más recursos en analizar y determinar el impacto de los delitos ya acontecidos para conocer en profundidad la huella que los mismos dejan en sus estados financieros. (López, Muñoz y Aranda, 2016, p.10)

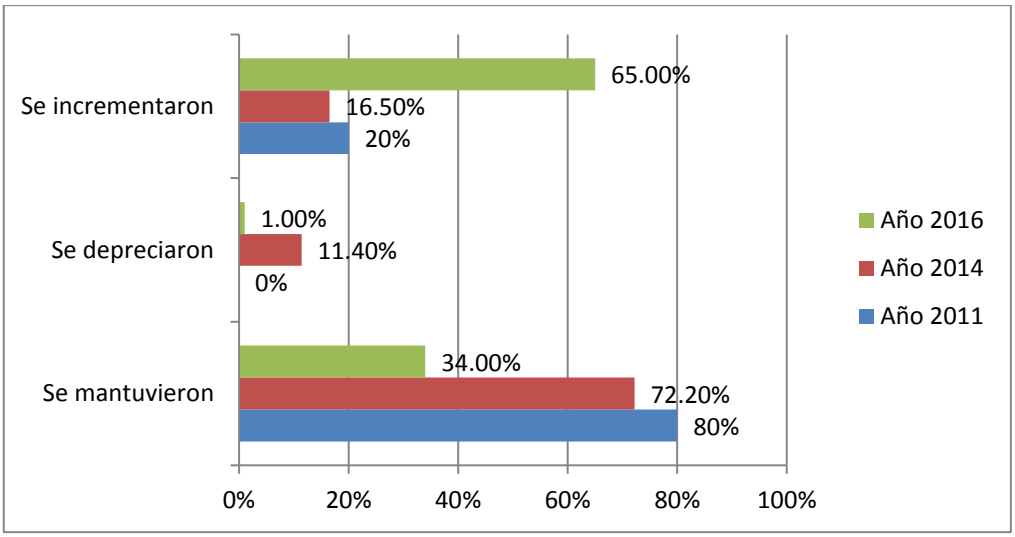
Pero el impacto que tienen las pérdidas financieras en las empresas no solamente tienen este carácter económico, sino que también pueden influir en la vida empresarial de forma muy notoria, asimismo en la encuesta del año 2016 aparecen porcentajes que expresan que:

> Los delitos económicos que han experimentado han producido un impacto negativo medio-alto en otros aspectos no financieros de la sociedad: en un 56% de los casos la moral de los empleados se ha visto afectada, un 35% afirma que ha repercutido en las relaciones empresariales y un 33% indica que han sufrido consecuencias en la reputación y la fuerza de la marca. (López, Muñoz y Aranda, 2016, p.10)

Ahora bien, centrándonos a partir de ahora en los ciberdelitos, a las empresas encuestadas se les realizaron preguntas sobre el impacto del cibercrimen y sobre las posibles realizaciones de evaluaciones del riesgo de sufrir algún tipo de ciberdelito –que son las gráficas expuestas a continuación-. Según los datos del sondeo y según el gráfico número 4 los ciberdelitos han ido aumentado su número a medida que han ido avanzando los años, lo que afirma que la tendencia ha sido ascendente con el paso del tiempo.

En el año 2011 el crimen online no era tan importante como lo fue en el año 2016, pero según los resultados desde ese año ya se preveía un gran auge de este tipo de delitos ya que “las empresas cada vez tenían mayor interacción en la red y aumentaba el comercio electrónico en las organizaciones” (Aranda y López, 2011, p.21).

Los gráficos que voy a analizar a continuación son en relación con el ciberdelito. El primero de ellos hace referencia a la importancia que las empresas encuestadas le daban a los ciberdelitos.



[9]*Gráfico 7: ¿Ha cambiado la percepción del riesgo de cibercrimen en su organización durante los últimos 12 meses? Tendencias de respuesta del 2011 al 2016.*

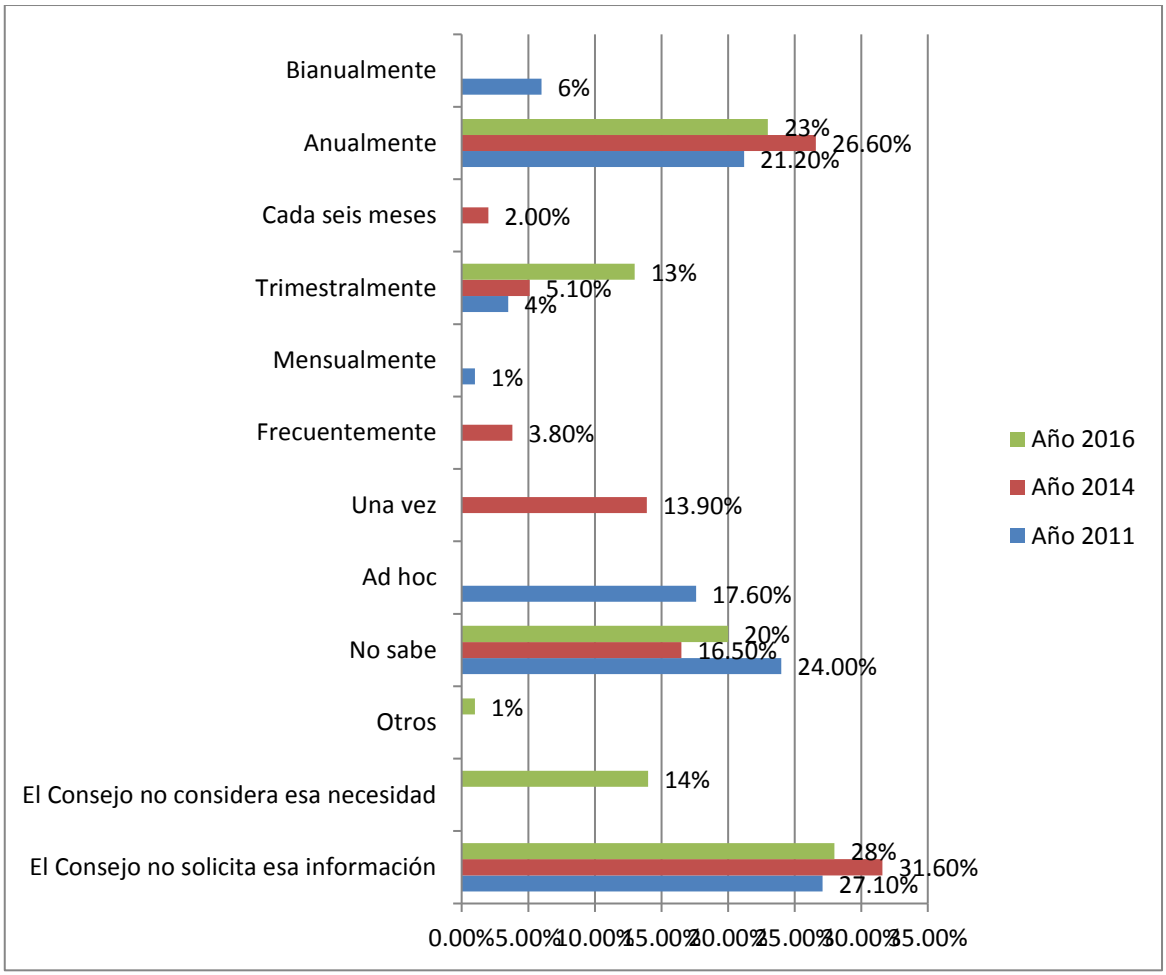
Claramente lo que más llama la atención de la gráfica número 7 es que en el año 2016 el 65% de las empresas españolas encuestadas han incrementado su percepción del riesgo con respecto a los ciberdelitos. Esto guarda relación con el gráfico número 4 ya que el hecho de que este tipo de delitos hayan tenido una tendencia ascendente con el paso de los años, puede hacer que las empresas lo vean como un delito real que les puede ocurrir en cualquier momento, y más aún si no toman las medidas de seguridad correspondientes.

Es muy sorprendente que en el año 2014 el 11,40% de las empresas encuestadas afirmasen que su percepción de riesgo había disminuido, ya que con respecto al año 2011 el número real de denuncias por ciberdelito habían aumentado, con lo cual si la percepción del riesgo había disminuido, cabe pensar que España no le daba ninguna importancia al hecho de ser una posible víctima de este tipo de conducta ilícita, pese a que haya aumentado el número de delitos objetivos. Es más según el sondeo de 2014 "la actitud de España tenía que cambiar y aproximarse a la opinión del resto del mundo, de manera que aumentara la preocupación de las organizaciones por este tipo de delitos" (López, Muñoz y Aranda, 2014, p.28). Y esto es lo que ocurrió en el año 2016 tal y como he mencionado anteriormente.

[9] Fuente: Encuesta mundial sobre fraude y delito económico 2011, 2014 y 2016.

Por último, en cuanto a la respuesta "se mantuvieron", notoriamente hay una tendencia negativa desde el año 2011 al 2016, ya que ésta en el número de delitos ha sido ascendente, y por lo tanto es lógico que con el paso de los años la percepción del riesgo no se mantuviera.

El siguiente esquema que analizaré es en relación con la frecuencia en la que el Consejo de Administración de las empresas encuestadas regula una evaluación del riesgo de fraude informático.



[10]*Gráfico 8: ¿Con qué frecuencia los miembros del Consejo de Administración piden información sobre el estado de preparación de la organización para hacer frente a los incidentes cibernéticos? Tendencias de respuesta del 2011 al 2016.*

Se ve claramente reflejado que la mayoría de las empresas españolas encuestadas no llevan a cabo este tipo de análisis de la evaluación del riesgo de ser víctimas de un ciberdelito, ya que el porcentaje de respuestas desde el año 2011 al 2016 es más o

[10] Fuente: Encuesta mundial sobre fraude y delito económico 2011, 2014 y 2016.

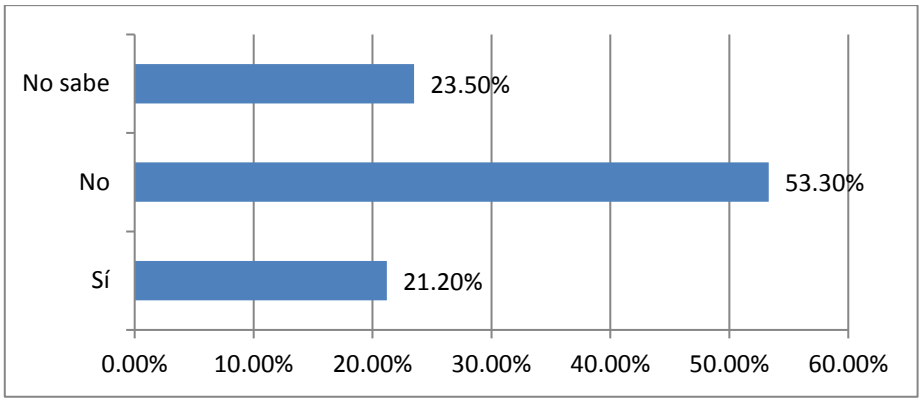
menos similar –en el año 2011 el porcentaje era del 27,10%, en el año 2014 era del 31,60% y en el año 2016 era del 28%-. Esto refleja la necesidad de realizar este tipo de análisis para poder corregir los errores que se pueden cometer y de esta forma poder reducir las oportunidades de convertirse en víctima de este tipo de delitos.

El siguiente porcentaje que llama mucho la atención es con respecto a la respuesta "no sabe" ya que afirma más aun el hecho de que las empresas españolas encuestadas no le dan la importancia que se merece a este tipo de análisis. La tendencia es más o menos similar en ambas tres encuestas: en el año 2011 nos encontramos con un porcentaje del 24%, en el año 2014 éste es del 16,50% y en el año 2016 del 20%.

En cuanto a la respuesta "anualmente" la tendencia es más o menos similar a lo anteriormente expresado, el 21,20% de las empresas encuestadas afirmó en el año 2011 que realizaba este análisis una vez al año, lo mismo respondió el 26,60% en el año 2014 y el 23% en el año 2016. Claramente este tipo de respuestas son más positivas que las anteriores ya que, aunque en un año los errores que se pueden llegar a cometer una empresa en la red pueden ser bastantes, el hecho de realizar el análisis aunque sea anualmente puede disminuir el riesgo de ser una posible víctima en el futuro.

Para finalizar con el análisis del gráfico número 8, un punto positivo de las respuestas analizadas es que la tendencia a realizar las evaluaciones trimestralmente ha ido evolucionando de forma ascendente a medida que han ido avanzando los años, de manera que en el año 2011 el porcentaje de este tipo de respuesta fue del 4%, en el año 2014 el porcentaje aumentó hasta el 5,10% y finalmente el año pasado éste era del 13%.

Para acabar con las encuestas me ha llamado la atención una de las preguntas que se realizaron en el año 2011 que, aunque no se puede comparar con las realizadas en 2014 y 2016 –ya que no se encuentra plasmada en dichos sondeos-, sí me parece que es importante analizarla aunque sea solo a nivel general. Creo que es una pena que no hayan propuesto este tipo de preguntas en las encuestas posteriores, puesto que vivimos en una sociedad en la que las redes sociales están en el centro de las relaciones interpersonales de todo el mundo tanto entre particulares como entre empresas.



[11]*Gráfico 9: ¿Controla su organización las redes sociales como Facebook o Twitter como factor de riesgo en su organización?*

Según la encuesta "en España las organizaciones aún no eran conscientes de la necesidad de supervisar las redes sociales" (López y Aranda, 2011, p.35). Esto era así puesto que el 53,3% de las empresas encuestadas había respondido que no controlan las redes sociales habitualmente, algo que creo que es indispensable puesto que, un control tanto del tráfico interno como del externo, es importante para evitar poner en riesgo tanto la seguridad de la empresa –en cuanto a ciberdelito se refiere- como la reputación de la misma.

En el siguiente punto voy a analizar un estudio realizado con el objetivo de determinar el grado de ciberseguridad existente en las personas de a pie, para de esta forma poder contextualizar el punto número 3 del marco teórico que es una encuesta de percepción de inseguridad en Internet realizada a 73 ciudadanos de Donostia-San Sebastián.

Más particularmente la investigación que analizaré a continuación es un estudio sobre ciberseguridad y confianza en los hogares españoles realizado por el Instituto Nacional de Tecnologías de la Comunicación (INTECO) y el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) (Gómez y Urueña, 2014).

[11] Fuente: Encuesta mundial sobre fraude y delito económico 2011, 2014 y 2016.

2.3.3 ESTUDIO SOBRE CIBERSEGURIDAD Y CONFIANZA EN LOS HOGARES ESPAÑOLES

El estudio se ha realizado a 3074 hogares, más particularmente "a usuarios españoles de Internet mayores de 15 años con acceso frecuente a Internet desde el hogar (al menos una vez al mes)" (Gómez y Urueña, 2014, p.70).

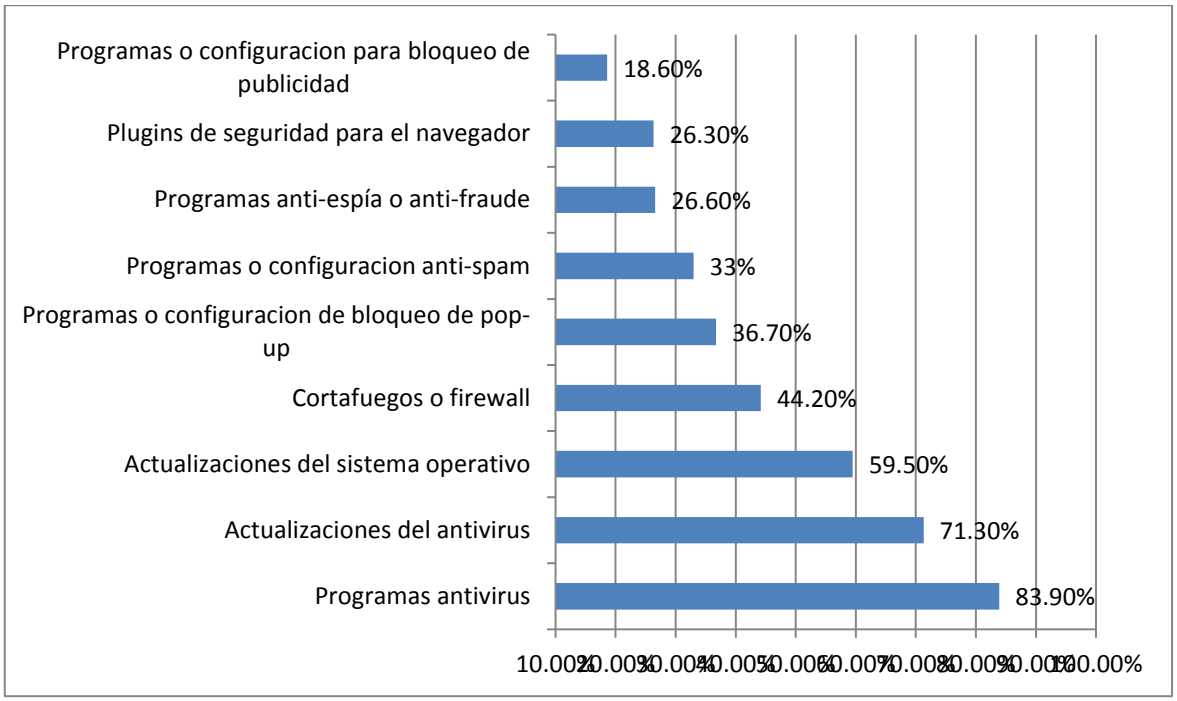
El motivo de elección de un estudio con estas características, tal y como he comentado anteriormente, es por un lado buscar una conexión entre las anteriores encuestas en grandes empresas y la posterior en las personas de a pie –que son mi objeto de estudio- y por otro lado poder contextualizar y dar sentido a la siguiente investigación realizada en Donostia-San Sebastián durante la ejecución de las prácticas obligatorias de la Universidad.

A partir de ahora comenzaré a examinar algunas de las gráficas existentes en dicho estudio sobre ciberseguridad en los hogares españoles, pero plasmaré solamente los gráficos que más tienen que ver con mi posterior investigación sobre estafas a través de compras online.

Las primeras de las gráficas a examinar son referentes al tipo de medidas de seguridad que los usuarios encuestados han seleccionado como protectoras de su ordenador y de los datos personales existentes en el mismo.

Es importante poder diferenciar entre dos tipos de medidas de seguridad: las automatizables y las no automatizables. Según la encuesta las automatizables "son aquellas medidas de carácter pasivo que, por lo general, no requieren de ninguna acción por parte del usuario, o cuya configuración se pone en marcha automáticamente" (Gómez y Urueña, 2014, p.7). Entre estas medidas se encuentran los antivirus, los programas anti-spam, etc. Asimismo, según la investigación, las medidas de seguridad no automatizables "son aquellas medidas de carácter activo que, por lo general, sí requieren una actualización especifica por parte del usuario para su correcto funcionamiento" (Gómez y Urueña, 2014, p.7). Entre éstas se encuentran las contraseñas, las copias de seguridad, etc.

Ambos dos tipos de medidas de seguridad se encuentran expuestas en las siguientes gráficas:

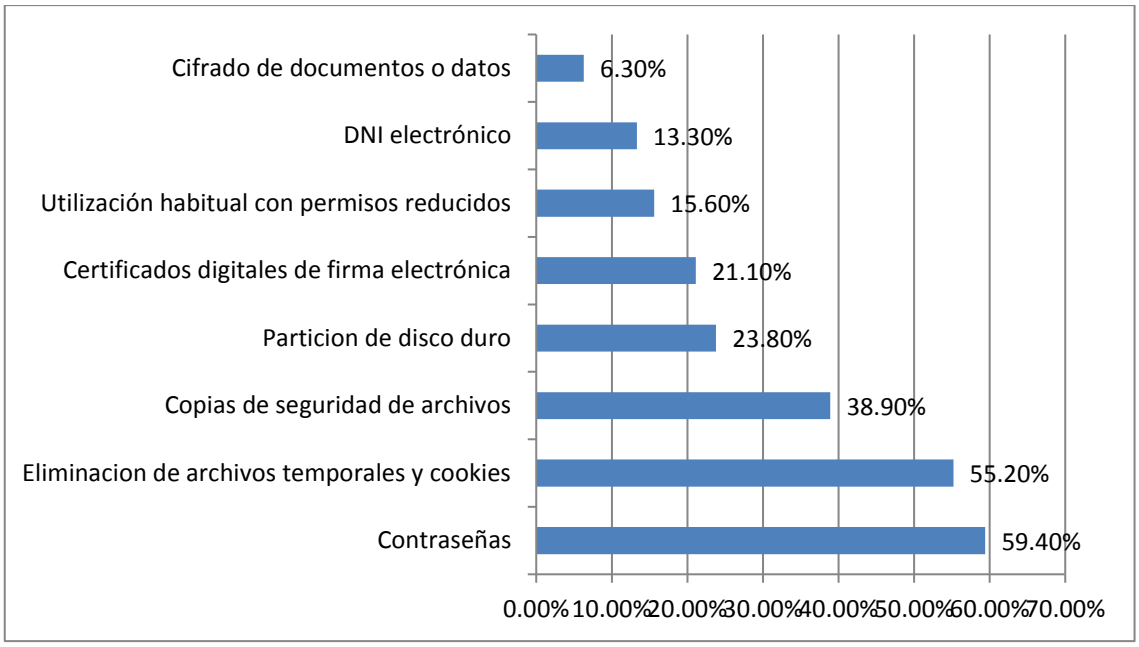


[12]*Gráfico 10: Porcentajes de utilización de medidas de seguridad automatizables por los hogares españoles encuestados.*

En la gráfica anteriormente expuesta se aprecia que la medida de seguridad automatizable, es decir, la que por regla general no requiere ningún tipo de acción por parte del usuario, más utilizada por los hogares españoles encuestados, es el programa antivirus con un 83,90% de respuesta. Seguido de las actualizaciones del mismo y del sistema operativo con un 71,30% y un 59,50% respectivamente.

Asimismo la medida de seguridad que menos se utiliza en los hogares encuestados es el uso de programas para el bloqueo de la publicidad que cuentan solamente con un 18,60% de respuesta. Los demás porcentajes van en aumento considerablemente hasta llegar a lo anteriormente mencionado, es decir, a las actualizaciones del sistema operativo y del antivirus y a los programas antivirus.

[12] Fuente: Estudio sobre ciberseguridad y confianza en los hogares españoles 2014.



[13]*Gráfico 11: Porcentajes de utilización de medidas de seguridad no automatizables por los hogares españoles encuestados.*

A simple vista se aprecia que, en comparación con el gráfico anterior, los porcentajes de utilización son muy bajos. Más particularmente la medida de seguridad no automatizable, es decir, la que necesita acciones de actualización por los usuarios, más utilizada en los hogares españoles es la contraseña con un 59,40% de respuesta. Este porcentaje es mucho más bajo que la medida de seguridad automatizable más utilizada, que era el antivirus y contaba con un 83,90% de respuesta.

La siguiente medida de seguridad no automatizable que tiene un porcentaje más o menos similar a las contraseñas es la eliminación de archivos temporales y cookies que cuentan con un 55,20%. Las demás medidas de seguridad tienen unos porcentajes de respuesta muy bajos, por lo que cabe pensar que los hogares españoles deberían replantearse el hecho de llevar a cabo conductas más activas para proteger su sistema operativo y los datos personales existentes dentro de su ordenador.

Las siguientes dos tablas a analizar son en las que los hogares españoles encuestados alegan por qué motivos no utilizan ciertas medidas de seguridad. Las tablas se dividen en dos ya que una de ellas corresponde a los motivos de no utilización de medidas de seguridad automatizables y la otra a las no automatizables.

[13] Fuente: Estudio sobre ciberseguridad y confianza en los hogares españoles 2014.

Comenzare por plasmar la tabla de motivos de no utilización de las medidas automatizables:

MEDIDAS	No Conoce	No Necesita	Precio	Entor-pecen	Descon-fía	Ineficaz	Otros
Programas antivirus	8,30%	27,40%	**24,50%**	9,60%	5,90%	**6,70%**	17,60%
Actualizaciones del antivirus	8,30%	25,90%	**23%**	9,10%	5,30%	5,50%	**22,90%**
Actualizaciones del sistema operativo	13,20%	28,40%	14,20%	9,60%	4,60%	4%	26%
Cortafuegos o firewall	24,70%	26,90%	9,40%	**12,70%**	4,60%	3,90%	17,90%
Programas o configuración de bloqueo de pop-up	**28,90%**	27,80%	6,10%	**12,20%**	4,60%	5%	15,40%
Programas o configuración anti-spam	19,30%	**36,30%**	6%	10,20%	**6,60%**	5%	16,60%
Programas anti-espía o anti-fraude	25,20%	27,10%	11,90%	8,10%	**7,80%**	4,50%	15,40%
Plugins de seguridad para el navegador	**36,50%**	26%	5,50%	10,70%	5%	3,20%	13,10%
Programas o configuración para bloqueo de publicidad	**37,30%**	25,20%	6,30%	9,70%	5,60%	3,60%	12,30%

[14]Gráfico 12: Motivos alegados por los hogares españoles encuestados para no utilizar medidas de seguridad automatizables.

En la gráfica anteriormente expuesta se puede apreciar que los motivos alejados con los porcentajes más elevados son a las respuestas “no necesita” y “otros”. En la primera de ellas el porcentaje de respuesta mayor corresponde a los programas o

[14] Fuente: Estudio sobre ciberseguridad y confianza en los hogares españoles 2014.

configuración anti-spam con un 36,30%, seguido de las actualizaciones del sistema operativo con un 28,40%. En el caso de la respuesta "otros" el porcentaje más elevado corresponde a las actualizaciones del sistema operativo con un 26%, seguido de las actualizaciones del antivirus con un 22,90%.

El programa antivirus y las actualizaciones del mismo tienen los porcentajes mayores en la respuesta "precio" con un 24,50% y un 23% respectivamente.

El 36,50% de los hogares españoles encuestados no conocen los plugins de seguridad para el navegador y el 37,30% tampoco conocen los programas o configuración para bloqueo de publicidad. En el caso de los programas o configuración de bloqueo de pop-up el 28,90% de los hogares encuestados nunca han oído hablar de ellos, por lo que han marcado la casilla de "no conoce".

En el caso de las respuestas "entorpecen", "desconfía" e "ineficaz" los porcentajes de respuesta son muy bajos por lo que no considero relevante realizar un análisis más específico de los mismos.

A continuación plasmaré la tabla de los motivos de no utilización de las medidas de seguridad no automatizables:

MEDIDAS	**No Conoce**	**No Necesita**	**Entor-pecen**	**Descon-fía**	**Ineficaz**	**Otros**
Contraseñas	12,50%	**54,10%**	6,30%	5,20%	**4,60%**	17,30%
Eliminación archivos temporales y cookies	24,40%	35,90%	**7,20%**	5,70%	**3,50%**	23,30%
Copia de seguridad de archivos	14,10%	44,60%	5,50%	3,90%	2,30%	**29,60%**
Partición del disco duro	**27,10%**	42,30%	6%	3,40%	2,40%	18,80%
Certificados digitales de firma electrónica	20,80%	47%	3,60%	5%	1,80%	21,80%

Utilización habitual con permisos reducidos	20%	**49,60%**	**7,30%**	3,50%	2,50%	16,90%
DNI electrónico	9,50%	**49,40%**	3,20%	**6,30%**	1,90%	**29,70%**
Cifrado de documentos o datos	**31,50%**	45,80%	3,50%	3,60%	1,60%	14,10%

[15]*Gráfico 13: Motivos alegados por los hogares españoles encuestados para no utilizar medidas de seguridad no automatizables.*

Lo primero que se puede apreciar entre una tabla y otra es que se ha eliminado la casilla del "precio" ya que claramente este tipo de medidas de seguridad no requieren del usuario ningún tipo de contribución económica.

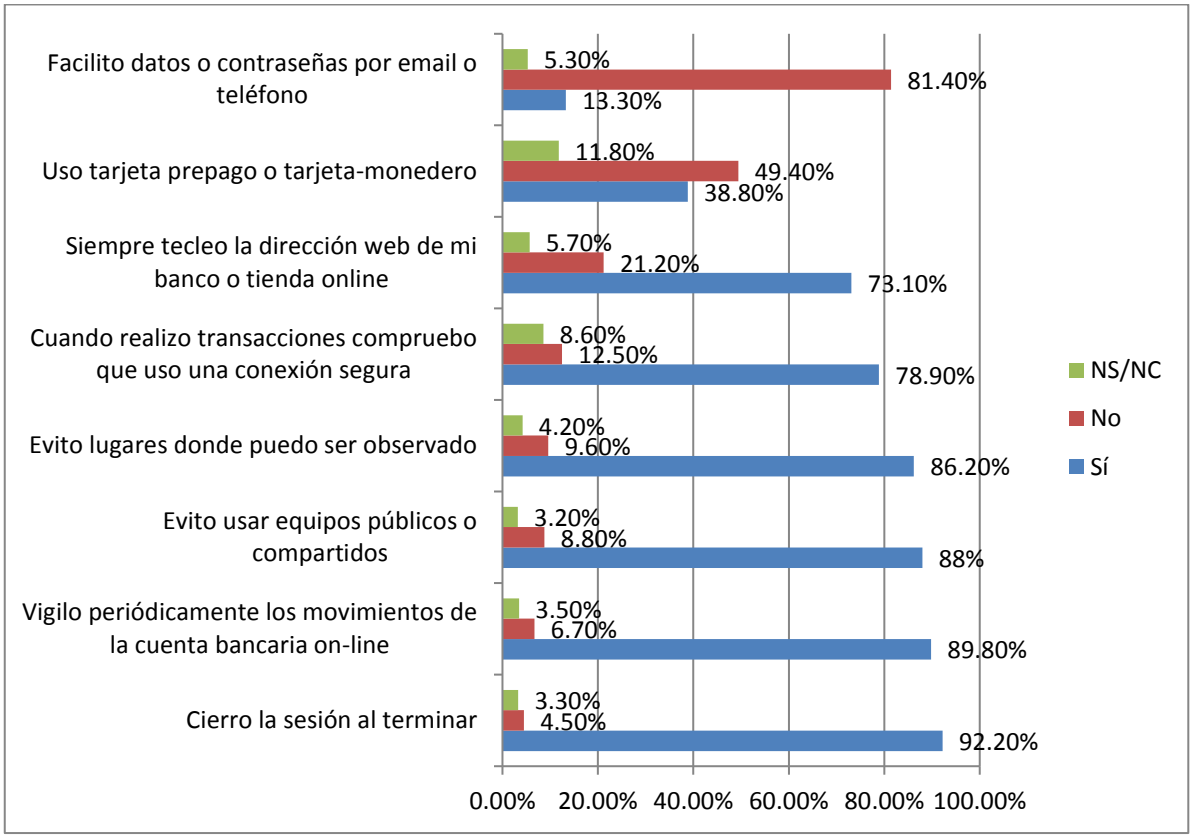
Ahora bien, analizando la tabla más específicamente vemos que la respuesta "no necesita" es la que tiene porcentajes más elevados llegando al 54,10% en el caso de las contraseñas, al 49,60% en el caso de la utilización habitual con permisos reducidos y al 49,40% en el caso del DNI electrónico. Con este hecho me remito a lo que he mencionado en el análisis del uso o no uso de las medidas de seguridad no automatizables en general, y creo que los usuarios deberían de comenzar ellos mismos por realizar ciertas conductas de seguridad, que les requieran algo de tiempo para su correcto funcionamiento, para que de esta forma comiencen ellos mismos por proteger su ordenador y los datos personales existentes en él.

La respuesta "otros" también tiene algunos porcentajes elevados como es el caso de la copia de seguridad de archivos que cuenta con un 29,60% de respuesta y del DNI electrónico que tiene un 29,70%.

En el caso de las respuestas "entorpecen", "desconfía" o "ineficaz" ocurre lo mismo que en la anterior tabla, y es que los porcentajes de respuesta son bastante bajos con lo cual considero que no es necesario realizar un análisis más específico de los mismos.

[15] Fuente: Estudio sobre ciberseguridad y confianza en los hogares españoles 2014.

En la siguiente gráfica los hogares españoles encuestados especifican qué tipo de conductas llevan a cabo a la hora de realizar una compra a través de la red. Antes de realizar el análisis el gráfico queda de la siguiente manera:



[16]*Gráfico 14: Conductas realizadas por los hogares españoles encuestados a la hora de llevar a cabo una compra online.*

A la hora de realizar el examen del gráfico anterior lo primero que llama la atención es que los porcentajes de la respuesta "si" son muy elevados en la mayoría de las conductas marcadas *a priori* en la encuesta. Más específicamente el 92,20% de los hogares encuestados cierran sesión al terminar una compra online, el 89,80% vigila periódicamente los movimientos que existen dentro de su banca online, el 88% evita utilizar conexiones públicas a la hora de adquirir un bien a través de la red, el 86,20% evita realizar la compra en cualquier lugar en el que le puedan observar, el 78,90% comprueba que la adquisición la realiza desde una conexión segura antes de llevarla a cabo y por último el 73,10% siempre teclea la dirección de su banco como forma de comprobar la seguridad del sitio web. Tal y como se puede apreciar en lo

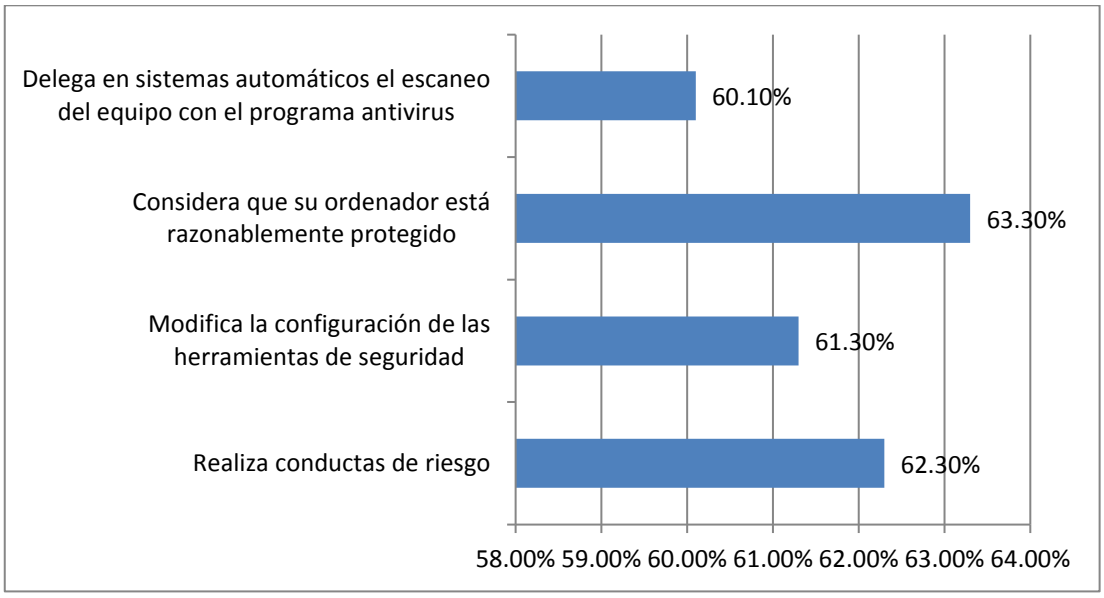
[16] Fuente: Estudio sobre ciberseguridad y confianza en los hogares españoles 2014.

anteriormente mencionado todas las conductas que los hogares españoles han especificado como reales a la hora de realizar una compra a través de Internet son bastante seguras, con lo cual cabe pensar que la mayoría de dichos hogares son bastante conscientes de la posibilidad de ser víctimas de cualquier tipo de fraude online si no llevan ciertas conductas a cabo.

Solamente el 38,80% de los hogares españoles encuestados han afirmado que utilizan tarjetas monedero o tarjetas prepago para realizar compras a través de la red, frente a un 49,40% que confirman que no utilizan estos métodos de pago online.

En el caso de facilitar datos o contraseñas por email o por teléfono, el 81,40% de los hogares españoles encuestados no realizan este tipo de conductas en Internet, lo que es muy positivo ya que cabe pensar que el hecho de desvelar este tipo de informaciones personales sin ninguna certeza puede aumentar las posibilidades de sufrir un fraude online.

La siguiente de las gráficas a examinar corresponde al hecho de si los hogares españoles encuestados han tenido algún tipo de infección en su ordenador como consecuencia de ciertas acciones que han realizado en el mismo.



[17]*Gráfico 15: Tipos de conductas realizadas en el equipo vs infección del mismo.*

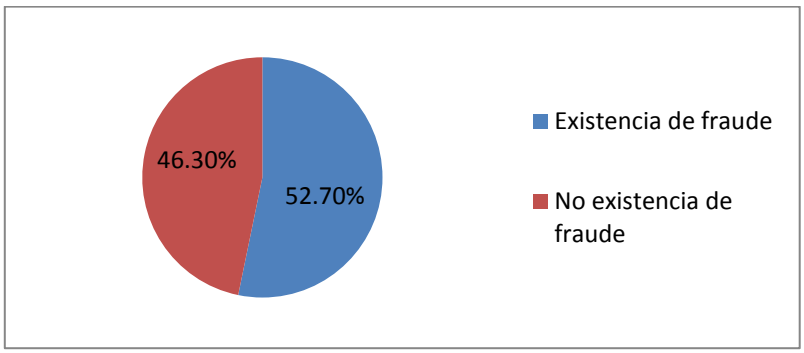
[17] Fuente: Estudio sobre ciberseguridad y confianza en los hogares españoles 2014.

Es sorprendente que para cualquier tipo de conducta de las marcadas *a priori* en la encuesta los porcentajes de infección son muy similares. También cabe expresar que los cuatro tipos de conductas son, en algunos casos inseguras, como ocurre con el caso de realizar conductas de riesgo en el ordenador.

En el caso anteriormente mencionado, el acto de realizar conductas de riesgo habitualmente en su equipo, el 62,30% de los hogares españoles encuestados afirman que han sufrido una infección. El 63,30% de los encuestados que consideran que su ordenador está totalmente protegido, también han sido víctimas de alguna infección del sistema. Asimismo los hogares encuestados que han modificado la configuración de las herramientas de seguridad de su equipo han sufrido alguna infección en el 61,30% de los casos. Y por último, el porcentaje menor, aunque prácticamente similar a los anteriores, es el de los hogares españoles que utilizan sistemas automáticos para realizar el escaneo del equipo a través del antivirus, en este caso el 60,10% de los encuestados afirman haber sido víctimas de algún tipo de infección.

Con estos porcentajes cabe pensar que, aunque éstos no sean extremadamente elevados, es importante llevar a cabo conductas seguras y medidas de seguridad tanto automatizables como no automatizables con el objeto de disminuir la posibilidad de sufrir algún tipo de infección en el sistema o de fraude a través de compras online.

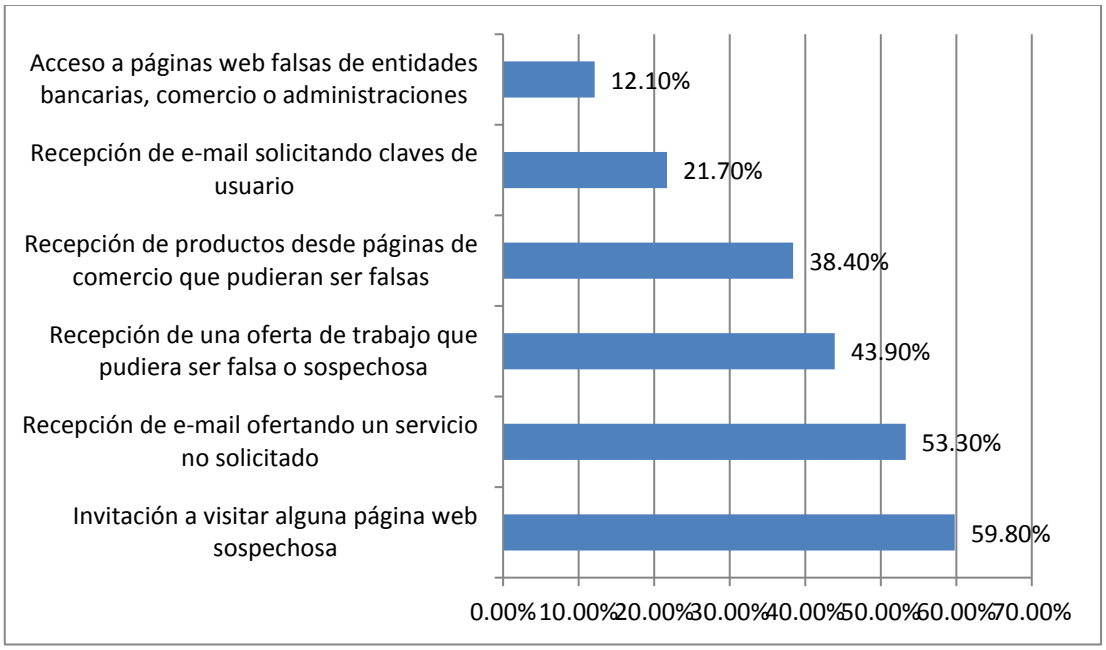
Las tres gráficas siguientes que voy a analizar hacen referencia a los fraudes online. Más específicamente las dos primeras corresponden a la existencia de una situación de fraude a través de la red y a cómo se ha manifestado esa situación y la última de ellas es referente a cómo se ha mostrado el remitente del supuesto fraude.



[18]Gráfico 16: Existencia de fraude en los hogares españoles encuestados.

[18] Fuente: Estudio sobre ciberseguridad y confianza en los hogares españoles 2014.

Tal y como se ve expresado en la gráfica los porcentajes de existencia o no de un fraude en los hogares españoles encuestados son muy similares, un 52,70% afirma que sí que ha sufrido alguna situación de fraude y un 46,30% manifiesta que no han sufrido ninguna situación que les haya hecho pensar que podrían ser víctimas de un fraude a través de la red.



[19]*Gráfico 17: Manifestaciones del intento de fraude sufrido por los hogares españoles encuestados.*

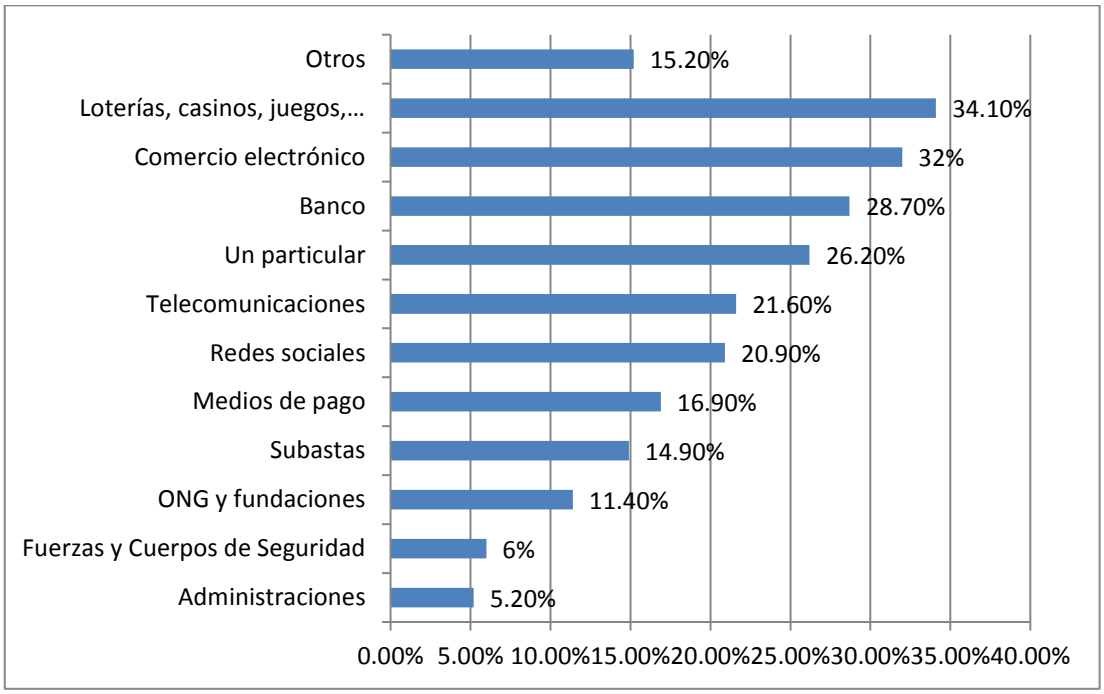
Del 52,70% de los hogares españoles encuestados que han afirmado haber sufrido alguna situación de fraude, más de la mitad, el 59,80%, han manifestado que ha sido a través de una invitación para visitar alguna página web sospechosa y el 53,30%, por medio de un e-mail en el que se le oferta un servicio que el posible afectado no ha solicitado en ningún momento.

Los demás porcentajes van disminuyendo considerablemente, el 43,90% de los encuestados declaran que el intento de fraude ha sido a través de una oferta de trabajo que aparentemente es falsa, el 38,40% por medio de la recepción de productos desde páginas de comercio que parecen ser falsas, el 21,70% afirman que el intento de fraude se ha cometido a través de un e-mail solicitando las claves de usuario existentes en su ordenador y por último, el menor de los porcentajes, un

[19] Fuente: Estudio sobre ciberseguridad y confianza en los hogares españoles 2014.

12,10% de encuestados que manifiestan que el fraude online se ha cometido por medio del acceso a páginas web falsas de bancos, comercios o administraciones.

La última de las gráficas referentes a los fraudes online es con relación a cómo se han revelado los remitentes de las posibles situaciones de fraude:



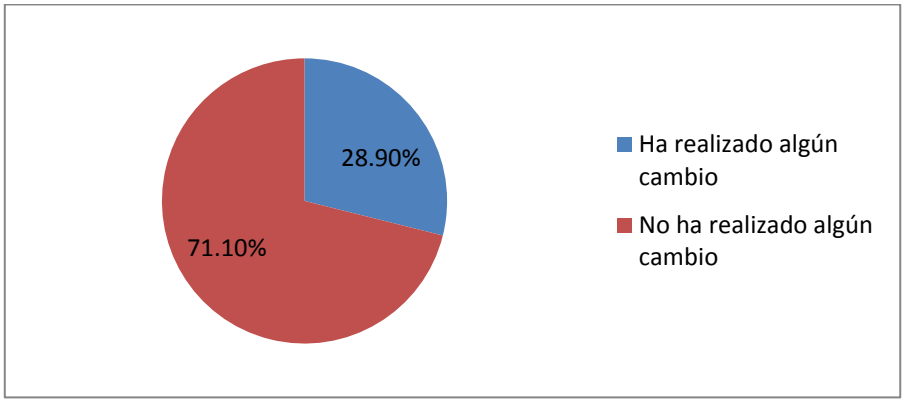
[20]Gráfico 18: Manifestaciones del remitente del supuesto fraude online.

Tal y como se expresa en la gráfica expuesta anteriormente las cuatro formas principales por las cuales los remitentes llevan a cabo situaciones de fraude a través de la red son: en el 34,10% de los casos a través de loterías, casinos, juegos, etc., en el 32% por medio de comercio electrónico, en el 28,70% con forma de entidades bancarias y por último en el 26,20% de las situaciones como si fuese un particular. Los demás porcentajes van descendiendo notablemente por lo que no considero relevante realizar un análisis más específico.

Por lo tanto y según la encuesta "de forma general, la principal forma adoptada por el remitente de la comunicación sospechosa de ser fraudulenta es la imagen de loterías, casinos y juegos online" (Gómez y Urueña, 2014, p.44).

[20] Fuente: Estudio sobre ciberseguridad y confianza en los hogares españoles 2014.

Las siguientes dos gráficas que voy a analizar hacen referencia a si los hogares españoles encuestados han realizado algún cambio en su equipo después de sufrir un incidente de seguridad o un fraude, y si los han adoptado en qué han consistido:



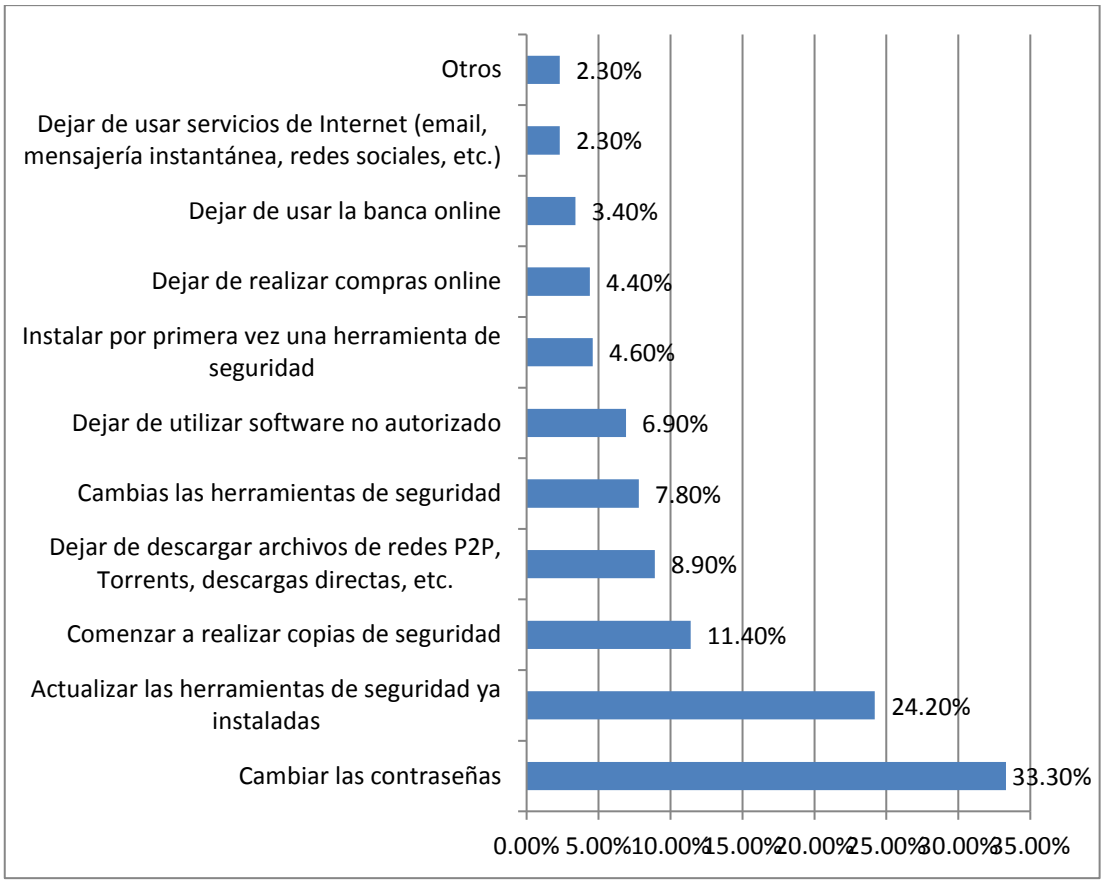
[21]Gráfico 19: Adopción de algún cambio en el equipo de los hogares españoles encuestados después de sufrir un incidente de seguridad o un fraude.

Esta gráfica llama mucho la atención ya que solamente el 28,90% de los hogares españoles encuestados han realizado alguna modificación en su equipo después de sufrir alguna situación en que la seguridad de su ordenador se ha podido ver afectada. Todo ello frente a un elevado porcentaje –un 71,10%- de encuestados que han manifestado no realizar ningún tipo de cambio después de sufrir dicha situación.

Con esto cabe pensar que casi la mayoría de los sujetos encuestados no consideran importante el hecho de modificar ciertas medidas de seguridad después de haber sido posibles víctimas de un fraude, o después de haberse enfrentado a una situación en la que se ha podido crear dicho fraude. En mi opinión solamente estimo como significativo el hecho de realizar cambios cuando se ha sufrido un incidente de seguridad, por el contrario en situaciones en las que te envían correos electrónicos que aparentan ser falsos no creo que sea importante modificar ciertas medidas de seguridad del equipo, ya que si no se responde a ese correo no considero que el equipo esté en riesgo.

Ahora bien, en la siguiente gráfica se exponen los cambios que han realizado el 28,90% de hogares españoles encuestados que han modificado alguna medida de seguridad de su ordenador tras un incidente:

[21] Fuente: Estudio sobre ciberseguridad y confianza en los hogares españoles 2014.



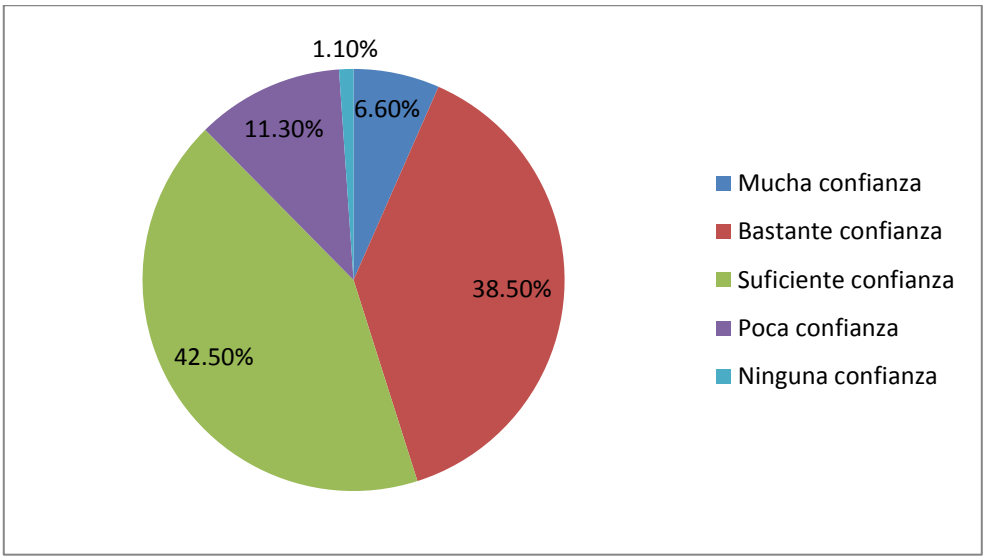
[22]*Gráfico 20: Cambios realizados por los hogares españoles encuestados después de sufrir un incidente de seguridad.*

Los dos cambios que más se han adoptado por los hogares españoles después de haber sufrido un fraude o un incidente de seguridad son: con un 33,30% el cambio de las contraseñas que protegen sus datos personales en el equipo y con un 24,20% la actualización de las herramientas de seguridad ya instaladas, todo ello con el propósito de no volver a sufrir un incidente de ese tipo.

Los demás porcentajes de respuesta son muy bajos por lo que no considero de relevancia mencionarlos.

[22] Fuente: Estudio sobre ciberseguridad y confianza en los hogares españoles 2014.

La siguiente gráfica es en relación con el nivel de confianza que tienen los hogares españoles encuestados en Internet:



[23]*Gráfico 21: Nivel de confianza que tienen los hogares españoles encuestados en Internet.*

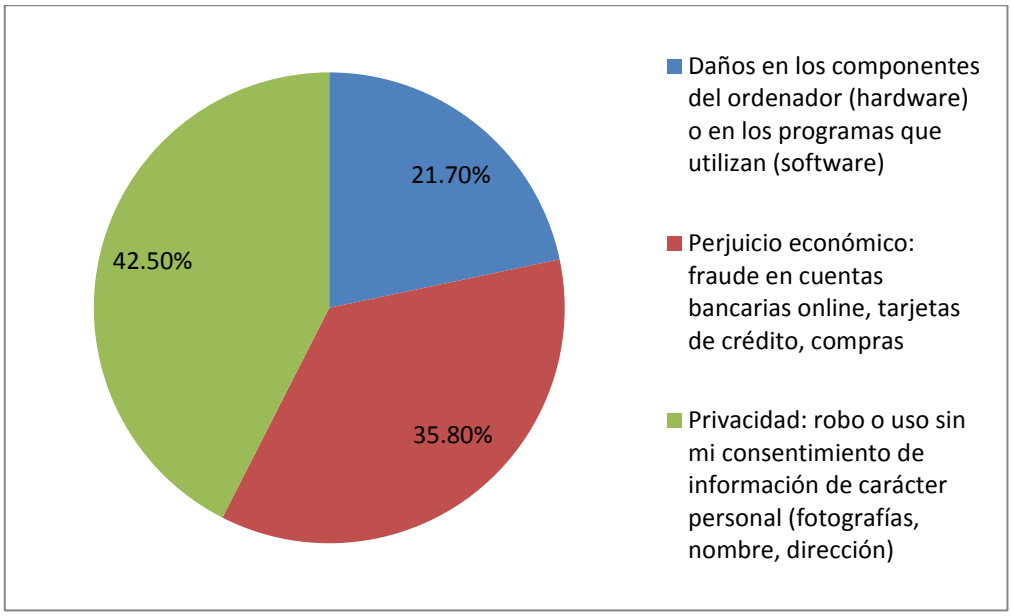
Los dos porcentajes más elevados con relación al nivel de confianza que tienen los hogares españoles encuestados en la red se encuentran entre las respuestas "suficiente confianza" y "bastante confianza", con un 41,50% y un 38,50% respectivamente.

Asimismo el 6,60% de los encuestados tienen mucha confianza en Internet, frente a un 1,10% de los hogares encuestados que no confía nada en la red.

Con estos datos se puede llegar a la conclusión de que la mayoría de los encuestados se encuentra en una situación en la que Internet le crea confianza, por lo que cabe pensar que muchos de ellos tienen una percepción de inseguridad en la red muy baja ya que consideran que Internet es un entorno bastante seguro para realizar muchas de las acciones del día a día.

[23] Fuente: Estudio sobre ciberseguridad y confianza en los hogares españoles 2014.

La penúltima de las gráficas que voy a examinar hace referencia a los riesgos que ven los hogares españoles encuestados al uso diario de Internet:



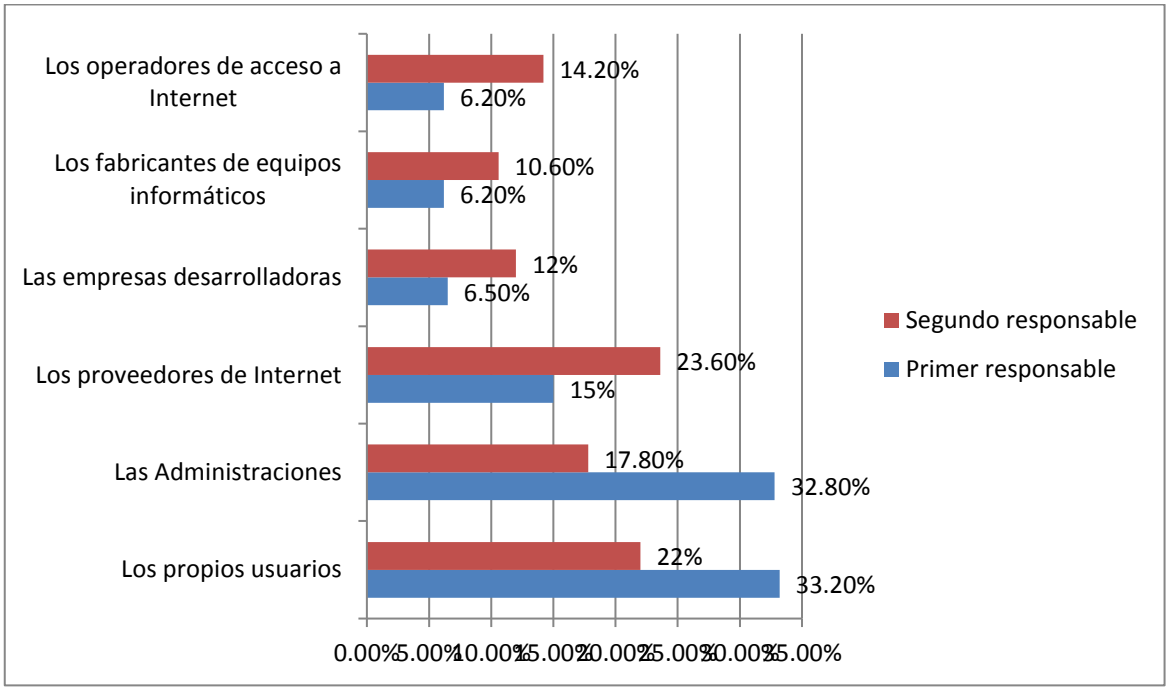
[24]*Gráfico 22: Riesgos que ven los hogares españoles encuestados con relación al uso diario de Internet.*

Los daños valorados en la encuesta *a priori* son tres: los daños al hardware o al software del equipo, el perjuicio económico y los daños relacionados con la vulneración de la privacidad de cada individuo. Ahora bien, hay dos de estos daños que tienen porcentajes más o menos similares frente a otro que se encuentra un poco más distanciado.

Con los dos porcentajes mayores, tal y como se aprecia en la gráfica, me refiero por un lado a la vulneración de la privacidad que cuenta con un 42,50% de respuesta y por otro lado al perjuicio económico que cuenta con un 35,80%. Todo ello frente a un 21,70% de encuestados que consideran que los daños al equipo también son de relevancia. En mi opinión es lógico que, aunque los daños en los componentes del ordenador también son en algunas ocasiones un perjuicio económico, considero que lo más importante es la vulneración de la privacidad y el robo o el uso de los datos personales de los usuarios sin su consentimiento.

[24] Fuente: Estudio sobre ciberseguridad y confianza en los hogares españoles 2014.

Finalmente la última gráfica es referente a donde, los hogares españoles encuestados, consideran que se encuentra la mayoría de la responsabilidad en el hecho de sufrir un fraude online:



[25]*Gráfico 23: Responsabilidad donde creen los hogares españoles encuestados que se encuentra el hecho de sufrir un fraude online.*

Tal y como se ve expresado en el gráfico los dos porcentajes de respuesta que los hogares encuestados consideran como primeros responsables al hecho de sufrir un fraude online o una incidencia de seguridad en el ordenador son: por un lado las Administraciones con un 33,80%, y por otro lado los propios usuarios, que asumen la responsabilidad de sus acciones en la red, con un 33,20% de respuesta.

El segundo responsable con el porcentaje más elevado serían los proveedores de Internet que cuentan con un 23,50% de respuesta.

Una vez finalizado el análisis de las gráficas tanto de las empresas como de los hogares españoles, en el siguiente apartado comenzaré por analizar la encuesta de percepción de inseguridad en la red creada y llevada a cabo durante el transcurso de las prácticas obligatorias de la Universidad.

[25] Fuente: Estudio sobre ciberseguridad y confianza en los hogares españoles 2014.

3 ENCUESTA DE PERCEPCIÓN DE INSEGURIDAD EN LA RED

La encuesta a la que me referiré en este apartado la llevamos a cabo Jennifer Hoyos, Marina Gomeztegui y yo para el trabajo de las prácticas obligatorias de la Universidad que realizamos en la Guardia Municipal de Donostia-San Sebastián, entre el 25 de enero y el 18 de marzo del 2016. Esta encuesta debía englobar la información suficiente como para poder realizar el trabajo de las prácticas y los trabajos de Fin de Grado de cada una de nosotras.

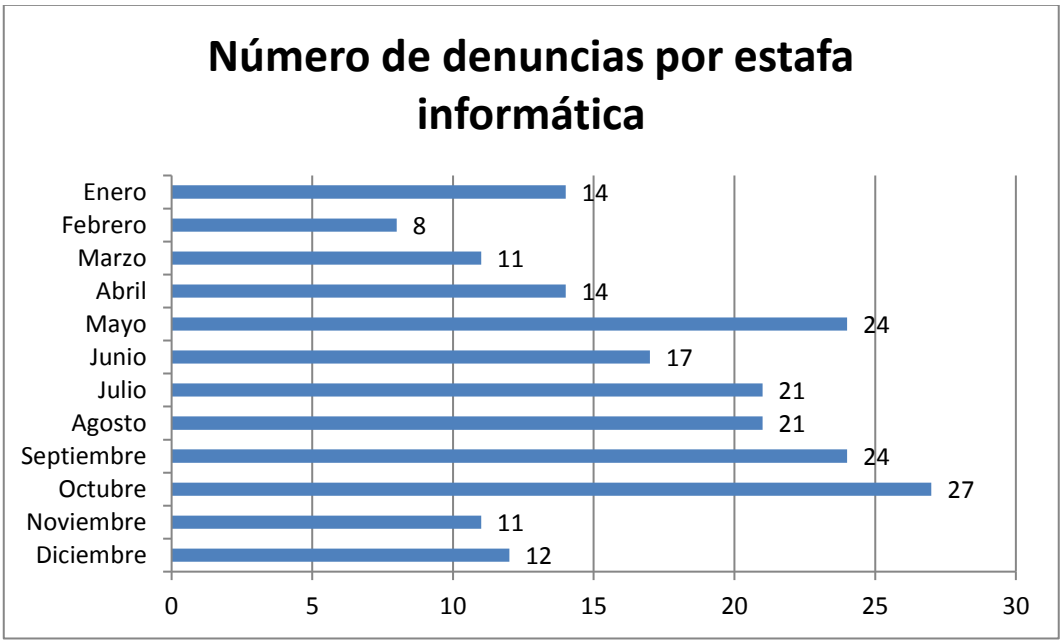
Como objetivo principal para el trabajo de prácticas establecimos la comparación de los delitos objetivos que se habían llevado a cabo en Donostia-San Sebastián en el 2015 -ayudándonos de las denuncias que la Guardia Municipal recogió ese año- con la percepción que los ciudadanos, de la misma ciudad, tenían en cuanto al miedo de ser víctimas de esos delitos. Los delitos en los que nos centramos fueron: hurtos en general, hurtos de cartera-bolso (los pusimos a parte ya que las cifras eran muy altas), agresiones sexuales, abusos sexuales, robos con violencia, robos con intimidación y por último el delito en el que yo me voy a centrar que son las estafas informáticas.

Por lo tanto la encuesta está dividida en tres partes, las dos primeras nos ayudaron a sacar adelante el trabajo de las prácticas obligatorias y eran la base principal del trabajo de Fin de Grado de mis compañeras, estas partes son: cifra negra y preguntas relacionadas con la inseguridad ciudadana. Por último la tercera parte es la que voy a analizar de ahora en adelante y es la que engloba la percepción de inseguridad en Internet. Todo esto lo explicaré a continuación cuando analice el instrumento utilizado en la metodología de la encuesta.

3.1 ESTADÍSTICAS DE ESTAFA INFORMÁTICA EN 2015

Antes de comenzar con el análisis de la encuesta es importante poder determinar cuántos fueron los delitos de estafa informática que la Guardia Municipal recogió en el año 2015 en Donostia-San Sebastián. Esta cifra fue de 204 denuncias.

Mientras realizaba las prácticas obligatorias de la Universidad recogí todas las denuncias de estafa informática por meses, para así poder realizar un análisis anual sobre esta conducta ilícita y sacar una serie de conclusiones que pueden servir como complemento a mi investigación. Estos datos los voy a plasmar en la siguiente gráfica:



[26]*Gráfico 24: Número de denuncias por estafa informática recogidas por la Guardia Municipal de San Sebastián en el año 2015.*

Tal y como vemos en el gráfico, excepto en el mes de febrero que cuenta solamente con 8 denuncias, el número de denuncias por estafa informática el resto del año es constante –van desde 11 a 27-. Todo ello frente a octubre que es el mes en el que se produjeron mayor número de denuncias en el ámbito de estafas online, las cuales obtuvieron un total de 27. Hay otros cuatro meses que tienen especial relevancia en cuanto a su número de denuncias estos son: mayo, julio, agosto y septiembre. Dichos meses comparten cantidades de dos en dos, es decir, mayo y septiembre comparten el mismo número –más en particular 24- y julio y agosto, a su vez, también tienen el mismo número –un total de 21 cada mes-.

Haciendo un análisis más global que por meses se puede afirmar que la estación del año con más número de denuncias fue verano, seguida de otoño, primavera y por último invierno. En el caso de verano, que hace referencia a los meses de junio, julio,

[26] Fuente: Base de datos de la Guardia Municipal de Donostia-San Sebastián.

agosto y septiembre, tiene un total de 83 denuncias. El hecho de que ésta fuera la estación con más número de estafas informáticas denunciadas puede deberse a que en estos meses es cuando los individuos tienden a realizar un elevado número de compras, ya que normalmente las personas suelen marcharse de vacaciones en estas fechas, alquilan apartamentos, habitaciones de hotel, adquieren bienes para dichas vacaciones, etc. Por ello hay muchas posibilidades de ser víctima de una estafa informática en verano.

A continuación determinaré los objetivos generales y específicos de mi trabajo.

3.2 OBJETIVO GENERAL Y ESPECÍFICOS

Primeramente he fijado un objetivo general que quiero cumplir una vez finalizado el análisis de la encuesta. Este objetivo es el de conocer qué grado de percepción de inseguridad tienen los sujetos encuestados en Internet. Pienso que éste es un objetivo clave para poder averiguar si los individuos ven a Internet un método seguro y fiable para navegar con total libertad y tranquilidad, y consecuentemente a esto, para adquirir bienes y/o contratar servicios, o al contrario creen que es un entorno poco seguro para navegar con total comodidad y para realizar sus tareas diarias.

Con el objetivo de crear un estudio más completo sobre la percepción de inseguridad en la red he marcado una serie de objetivos específicos que perseguiré con la realización de la encuesta y que son de gran ayuda para saber cuál es la opinión de los habitantes de Donostia-San Sebastián sobre Internet en su totalidad, abarcando varias perspectivas.

Particularmente son nueve los objetivos específicos marcados en el sondeo:

1- Analizar para qué acciones utilizan los sujetos encuestados Internet: en la encuesta aparecen una serie de ámbitos de uso de la red ya marcados *a priori* en los que los sujetos encuestados tienen que determinar si hacen uso de ellos diariamente o no. Estos ámbitos son: información sobre actualidad, compras, entretenimiento, intercambio de archivos, participación en chats y foros, intercambio de comunicación, contratación de servicios y uso de datos bancarios.

2- Conocer si las personas encuestadas saben la diferencia entre una página web legal y una ilegal. Esto hace referencia a los anteriormente mencionados en el marco teórico Phishing y Pharming en los cuales los posibles infractores crean páginas web aparentemente legales para poder adquirir los datos bancarios de los usuarios.
3- Averiguar qué problemas principales ven los usuarios encuestados al uso diario de Internet. Este objetivo nos puede ayudar a conocer en qué se fijan más los ciudadanos a la hora de utilizar la red día a día, o lo que es lo mismo, a qué dan más importancia los individuos cuando usan Internet. Los problemas fijados *a priori* en la encuesta para poder evaluar este objetivo son: velocidad, seguridad, coste, calidad del acceso –hace referencia a la legalidad y seguridad de la página-, falta de confidencialidad –relacionado con lo anterior-, demasiada publicidad, infección por virus y una última opción que es mencionar otro problema si no es ninguno de los anteriormente fijados.
4- Determinar a través de una escala Likert si los sujetos encuestados creen que Internet es un entorno seguro para realizar compras o contratar servicios.
5- Saber si los individuos encuestados utilizan las transferencias bancarias online o prefieren ir directamente al banco a llevarlas a cabo. Este objetivo es clave para conocer la confianza que los usuarios tienen a la hora de colocar sus datos personales en Internet. En el caso de que no lo hagan es importante también determinar por qué prefieren ir al banco directamente.
6- Averiguar qué método de pago utilizan los ciudadanos de Donostia-San Sebastián encuestados a la hora de adquirir bienes online. Este objetivo está muy relacionado con el anterior ya que nos ayuda a evaluar la confianza que los usuarios tienen en Internet, pero no solamente a la hora de plasmar sus datos bancarios, sino también a la hora de preferir pagar un bien antes o después de que llegue al domicilio. Los métodos de pago marcados en la encuesta para medir este objetivo son: tarjeta de crédito o débito –cabe pensar que las personas que utilicen las transferencias online también usen este método de pago-, contrareembolso, domiciliación bancaria, transferencia, a través del teléfono móvil, PayPal y similares y finalmente se encuentra la opción de que las personas encuestadas plasmen otro método utilizado si no es ninguno de los anteriores.

7- Determinar a través de una escala Likert qué grado de confianza tienen los individuos encuestados en la protección de sus datos personales en Internet.
8- Saber en qué medida las personas encuestadas creen que a través de la red a veces se viola su derecho a la intimidad.
9- Conocer si los encuestados creen necesaria una regulación de la ley en el ámbito de protección de los datos personales a través de la red. Además de averiguar si creen o no indispensable dicha regulación podrán expresar en qué ámbito creen que se debe de llevar a cabo.

A partir de aquí comenzaré a examinar la metodología de creación de la encuesta para posteriormente analizar los resultados en base tanto del objetivo general como de los específicos.

3.3 METODOLOGÍA

La metodología utilizada en la encuesta que voy a describir a continuación es la que llevamos a cabo mientras realizábamos las prácticas, por ello hay muchas partes que no son necesarias en mi investigación sobre percepción de inseguridad en la red pero creo que es importante describirlas por un lado, para poder comprender por qué ha tenido esa forma la encuesta y por otro lado, como modo de contextualización para el posterior análisis de los resultados.

Comenzaré por describir el diseño, posteriormente determinaré la muestra utilizada -diferenciándola por género, edad y barrio de residencia de los encuestados-, el procedimiento empleado para la creación de la encuesta y por último analizaré el instrumento utilizado –del que antes he hecho una breve contextualización-.

3.3.1 DISEÑO

Al principio queríamos llevar a cabo un diseño por conglomerados dividiendo toda la población de Donostia-San Sebastián por barrios ya que pensábamos que al ir a realizar la encuesta a cada barrio nos encontraríamos con individuos que eran residentes del sitio en cuestión. Pero a la hora de llevar a cabo la encuesta en el

exterior pudimos apreciar que había zonas como Gros, la Parte Vieja, Amara o Egia en las que había mucha cantidad de individuos, pero muchos de ellos no residían en el barrio donde estábamos realizando la encuesta e incluso algunos de ellos pertenecían a Bilbao, Zarautz, Irún, etc.

Todo esto unido a la falta de tiempo hizo que tuviésemos que cambiar el diseño y la muestra del estudio ya que a la hora de realizar una encuesta en el exterior, es muy difícil que todos los días se obtengan el mismo número de encuestados, de hecho hay días que no obtuvimos ninguno o porque los individuos no querían perder el tiempo y no tenían ganas o tenían prisa o porque no eran de Donostia-San Sebastián, lo que nos dificultaba mucho el trabajo.

A partir de este punto es cuando cambiamos a un muestreo no probabilístico en el cual nosotras mismas establecíamos la muestra de forma aleatoria –muestra por conveniencia-. Y fue a partir de aquí donde decidimos finalmente ir a encuestar a zonas de Donostia-San Sebastián que eran muy transitadas como por ejemplo, Amara, la Parte Vieja, la zona de la Concha, Gros, etc. para así obtener resultados seguros de sujetos residentes en diferentes barrios de Donostia-San Sebastián sin tener la necesidad de ir al lugar en cuestión a encontrar a dichos individuos.

La metodología de mi investigación es cuantitativa ya que lo que estoy utilizando es una técnica de encuesta que tiene como fin operacionalizar o traducir realidades sociales en datos numéricos. Con mi instrumento de medida lo que hago es operacionalizar ciertas realidades sociales relacionadas con los hábitos de cada sujeto en la red y convertirlas en datos numéricos para luego poder medirlas.

El instrumento utilizado en mi investigación es una encuesta semiestructurada que está compuesta por preguntas abiertas, cerradas y semicerradas, aunque en su mayoría está constituida por preguntas cerradas. Más particularmente las preguntas abiertas de la encuesta hacen referencia a los ítems 19 y 23; en el caso de los ítems semicerrados son el 17 y el 20 y por último los ítems 15, 16, 18, 21 y 22 son relativos a las preguntas cerradas.

3.3.2 MUESTRA

En un principio hicimos un estudio basándonos en la población total de Donostia-San Sebastián –que consta de más de 180.000 habitantes- con el objetivo de establecer una muestra que fuera representativa de la ciudad. Esta investigación nos hizo determinar una muestra de aproximadamente 130 personas encuestadas. Tratamos de dividir de forma igualitaria el muestrario entre los diferentes barrios de Donostia-San Sebastián para que de esta forma fuese aún más representativo de la población.

A la hora de llevar a cabo la encuesta en el exterior nos dimos cuenta de que era muy difícil poder obtener ciertas personas de cada barrio, y además nos surgieron muchos imprevistos de tiempo con lo cual no pudimos realizar una muestra tan extensa de personas –todo ello lo explicaré posteriormente en el instrumento-.

Por ello decidimos realizar un estudio piloto o teórico que no fuese representativo de la población total de la ciudad con la intención de simplemente describir una realidad pero sin poder generalizar nuestra investigación al total de los habitantes de Donostia-San Sebastián. De esta forma utilizamos un muestreo no probabilístico circunstancial en el cual éramos nosotras mismas como investigadoras las que establecíamos una muestra, denominada muestra por conveniencia, determinando nuestras propias preferencias tal y como he explicado en el apartado anterior.

Finalmente la muestra estuvo compuesta por un total de 73 personas residentes en los diferentes barrios de Donostia-San Sebastián. Tal y como he comentado anteriormente esta muestra no es representativa de la población total de la ciudad, pero creo que es justo poder plasmar el nivel de confianza del estudio con la muestra establecida.

Nivel de confianza 95%	11,50%
Nivel de confianza 97%	12,70%
Nivel de confianza 99%	15,10%

Gráfico 25: Nivel de confianza para mi estudio con muestra de 73 individuos.

Tal y como se ve plasmado en la tabla en ningún caso se pueden generalizar o extrapolar los resultados a la población total de Donostia-San Sebastián porque el nivel de confianza está muy lejos del utilizado en cualquier investigación científica.

Por ello realizo un estudio teórico-exploratorio en el cual solo trato de comprender el fenómeno de la percepción de inseguridad en la red, analizando lo que opinan los sujetos encuestados sobre el mismo.

Ahora bien, como en nuestro estudio de prácticas analizábamos delitos tales como abusos y agresiones sexuales, decidimos utilizar un porcentaje un poco mayor de mujeres que de hombres, ya que por regla general el miedo a este tipo de delitos es mayor en el género femenino que en el masculino. En mi análisis individual -que es la percepción de inseguridad en la red- no tiene mayor importancia que la muestra esté compuesta por más mujeres que hombres ya que realizaré un análisis meramente descriptivo de los resultados existentes en la encuesta.

Por lo tanto la división de la muestra por género quedaría de la forma que expondré en la siguiente gráfica:

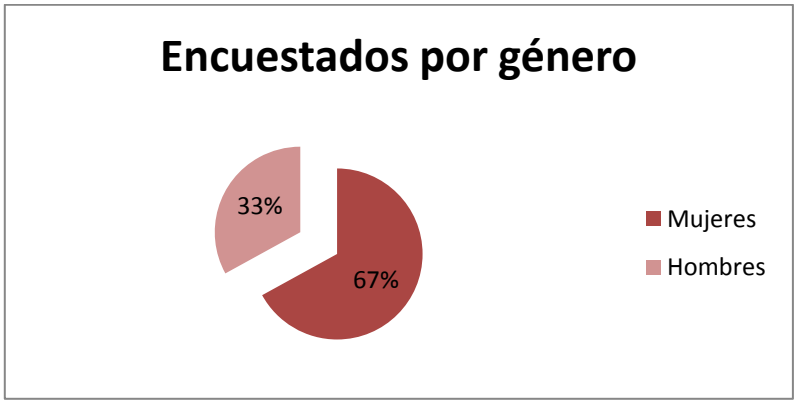


Gráfico 26: División de los encuestados por género.

Pero esta no es la única diferenciación que realizamos de la muestra, en nuestro trabajo de prácticas también realizamos la distinción de los encuestados por edades. Por las circunstancias aleatorias del muestreo mencionadas anteriormente obtuvimos la mayoría de los encuestados comprendidos entre las edades de 18 y 29 años, hecho que es muy positivo para mi investigación ya que cabe pensar que los individuos que se encuentran dentro de estos márgenes de edad son los que más utilizan la red para múltiples acciones.

Asimismo la gráfica expuesta a continuación nos muestra cuáles fueron las diferenciaciones por edades de las personas encuestadas:

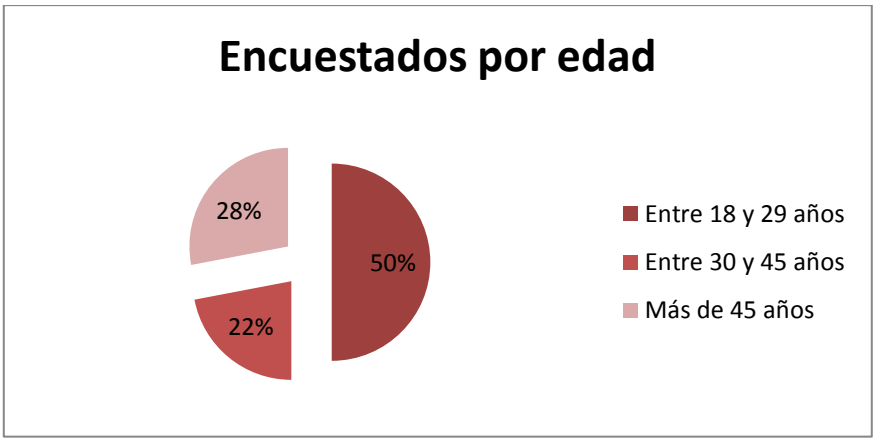


Gráfico 27: División de los encuestados por edad.

Para finalizar el apartado de la muestra hay una última especificación que realizamos de la misma que para mi estudio no es significativa pero creo que es importante plasmarla ya que formó parte de la realización de la encuesta. Esta división es la realizada por barrios. Para mi investigación sobre Internet no tiene ningún tipo de repercusión el hecho de que la persona encuestada viva en Gros o en la Parte Vieja, lo que en realidad sí es significativo para mi estudio es el uso que ese individuo hace de la red.

Asimismo la última diferenciación de las personas encuestadas por barrios queda de la siguiente forma:

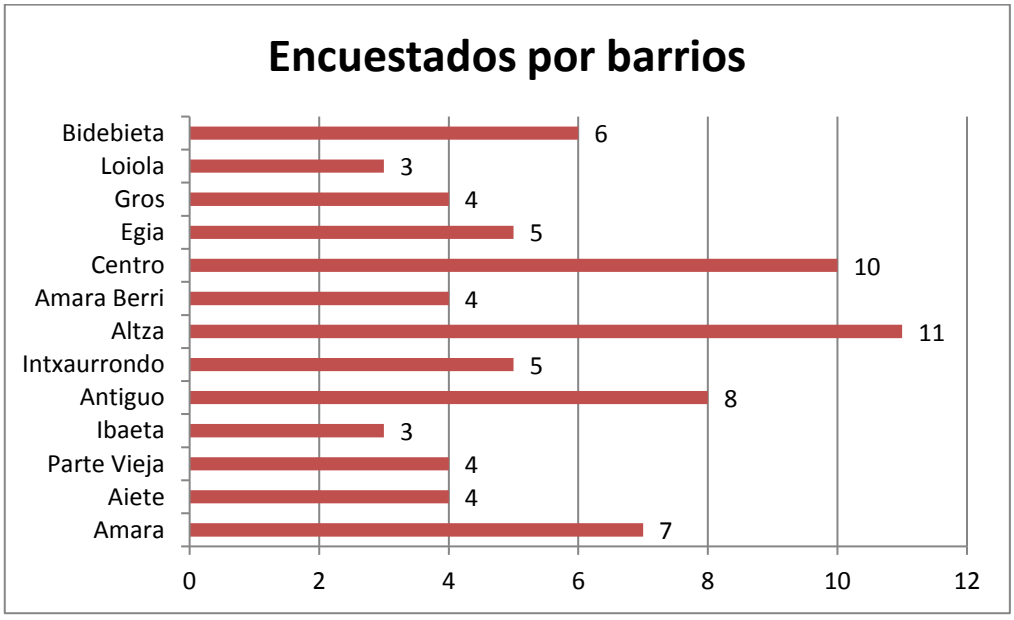


Gráfico 28: División de los encuestados por barrios de residencia.

3.3.3 PROCEDIMIENTO

El cuestionario fue creado por nosotras mismas para nuestra propia investigación y por lo tanto tiene unos propósitos concretos por lo que no es generalizable para otros fines.

En cuanto a la creación de los ítems, muchos de ellos fueron recogidos y adaptados a nuestro estudio de páginas tales como: el Instituto Nacional de Estadística (2016) y el Ministerio del Interior (2014), sobre encuestas tanto de seguridad ciudadana como de seguridad en Internet que se realizaron años anteriores. Algunos ítems fueron creados por nosotras mismas dependiendo de nuestras propias preferencias o de los objetivos que queríamos evaluar en nuestro sondeo –todos ellos valorados por profesionales a los que acudimos de forma voluntaria-.

Centrándome en mi trabajo he de afirmar que, tal y como se puede apreciar en la encuesta y como explicaré posteriormente en el apartado del instrumento, todos los ítems están relacionados con las compras en Internet ya que mi investigación se centra, particularmente, en las estafas producidas a través de la compra de bienes y de la contratación de servicios online, y por ello todas las preguntas están orientadas a dicho ámbito. Cierto es que los últimos tres ítems tienen una tendencia más legal que social ya que se centran más en la protección de datos y en el derecho fundamental a la intimidad que tienen los individuos, pero considero que darle a la encuesta dicho enfoque hace que el estudio sobre la percepción de inseguridad de los habitantes de Donostia-San Sebastián sea más completo.

3.3.4 INSTRUMENTO

Ya para finalizar con la metodología de la encuesta el instrumento utilizado es una encuesta de cifra negra e inseguridad ciudadana (ver anexo).

La encuesta está formada por 23 preguntas y dividida en 4 partes:

- Preguntas 1-4: en ellas se evalúa la cifra negra. Fue la base principal del Trabajo de Fin de Grado de una de mis compañeras, Marina Gomeztegui. Al individuo se le preguntará si ha sufrido alguno de los delitos marcados en el

estudio como principales –hurto, hurto documentación, robo con violencia o intimidación, agresión o abuso sexual y estafa informática- aunque también se le deja un apartado o bien para que mencione otro delito del que ha sido víctima que no es ninguno de los anteriores o bien para que marque la respuesta de NS/NC cuando el sujeto no quiere decir de qué delito ha sido víctima. Realmente el objetivo principal de este apartado no es el conocer qué delito ha sufrido el sujeto, sino el hecho de que si realmente ha sido víctima de algún delito, el acto ha sido denunciado o no y por qué.

- Preguntas 5-12: en ellas se evalúa la seguridad o inseguridad ciudadana. Fueron la base principal del trabajo de prácticas y del Trabajo de Fin de Grado de mi compañera Jennifer Hoyos. Estos ítems recogen información relativa a la seguridad que tienen los sujetos encuestados cuando se encuentran en los barrios escogidos en nuestra investigación –Amara, Gros, Paseo de la Concha, Parte Vieja, Centro, Intxaurrondo y una zona específica como es el Pasadizo de Egia-. También se evalúa el miedo a sufrir los delitos mencionados en las primeras cuatro preguntas, así como ítems relativos a la inseguridad o seguridad que sienten los individuos tanto en su barrio como en contextos específicos como pueden ser caminando solo por el Centro, a ciertas horas, etc.
- Preguntas 13-14: son relativas al uso de las cámaras de videovigilancia en lugares públicos. En ellas se quiere conocer la opinión de los encuestados sobre el uso de este tipo de cámaras en el exterior, así como si están de acuerdo o no con la utilización de las mismas.
- Preguntas 15-23: estos ítems hacen referencia al ciberdelito. Son la base de mi investigación y las preguntas que voy a analizar de ahora en adelante. En ellas se estudia tanto el uso que hacen los encuestados de Internet, como el grado de percepción de inseguridad que tienen los sujetos encuestados a la hora de utilizar la red diariamente. También hay preguntas sobre los métodos de pago de los individuos y sobre la valoración que hacen ellos de la protección de datos en Internet, entre otras. Más particularmente las preguntas relativas a la percepción de inseguridad en Internet son las siguientes:
    - Pregunta 15: en ella se pregunta a los sujetos para qué acciones utiliza Internet diariamente: información sobre actualidad, compras,

entretenimiento, intercambio de archivos, participación en chats y foros, intercambio de comunicación, contratación de servicios y/o uso de datos bancarios.

- Pregunta 16: hace referencia a si los individuos encuestados conocen la diferencia entre una página web legal y una ilegal. Entendiendo como una página web ilegal un portal que, aparentemente parece legal, pero que solamente se utiliza para captar datos bancarios o personales de los usuarios con el fin de utilizarlos sin su consentimiento.
- Pregunta 17: es referente a qué problemas ven los usuarios encuestados al uso diario de Internet: velocidad, seguridad, coste, calidad del acceso, falta de confidencialidad, demasiada publicidad, infección por virus y/u otros.
- Pregunta 18: en ella se quiere determinar si los sujetos encuestados creen que Internet es un entorno seguro o no lo es.
- Pregunta 19: hace referencia a si los ciudadanos de Donostia-San Sebastián encuestados utilizan el método online para hacer una transacción bancaria o prefieren ir al banco a realizarla y por qué.
- Pregunta 20: es referente a qué método de pago utilizan los usuarios encuestados a la hora de adquirir un bien o un servicio a través de la red: tarjeta de crédito o de débito, contrareembolso, domiciliación bancaria, transferencia, a través del teléfono móvil, PayPal y similares y/u otros.
- Pregunta 21: a través de la realización de la pregunta se quiere analizar si los sujetos encuestados confían en la protección de sus datos personales a través de la red.
- Pregunta 22: hace referencia a si los ciudadanos encuestados creen que a través de la red a veces se vulnera su derecho a la intimidad.
- Pregunta 23: es referente al hecho de si los usuarios encuestados creen que se debe hacer una reforma en la ley en el ámbito de protección de los datos personales a través de la red.

La duración aproximada para la realización de la encuesta es de 5 minutos. Las formas de respuestas son varias pero muy sencillas para hacer el sondeo lo más

llevadero posible. En general hay tres métodos de respuesta: de elección rápida (marcar con una X), respuestas dicotómicas (en las cuales los encuestados deben responder si o no) y por último escala Likert de 1 a 5 puntos con una misma puntuación en todas las preguntas (1 = nada o poco seguro y 5 = mucho o muy seguro).

A partir de este punto comenzaré a analizar los resultados teniendo en cuenta tanto el objetivo general como los objetivos específicos.

3.4 ANÁLISIS DE LOS RESULTADOS CON RELACIÓN A LOS OBJETIVOS ESPECÍFICOS

En este apartado analizaré los resultados de la investigación con relación a los objetivos específicos marcados al principio de la segunda parte de mi trabajo.

El estudio se hará tanto de forma global examinando a todos los encuestados en su conjunto, como diferenciando la muestra por género y por edad, para así realizar una investigación más completa de la percepción de inseguridad en Internet.

En el primero de los objetivos específicos se quiere analizar para qué acciones utilizan los sujetos encuestados diariamente la red. Este objetivo es muy interesante de examinar ya que en él se puede determinar si existe percepción de inseguridad en los sujetos encuestados a la hora de utilizar Internet en su día a día, si lo utilizan para realizar acciones relacionadas con compras y datos bancarios, o por el contrario solamente lo utilizan para entretenerse e informarse de lo que ocurre en el mundo o en su ciudad, por ejemplo.

En la siguiente gráfica se van a plasmar los porcentajes de respuesta a este ítem:

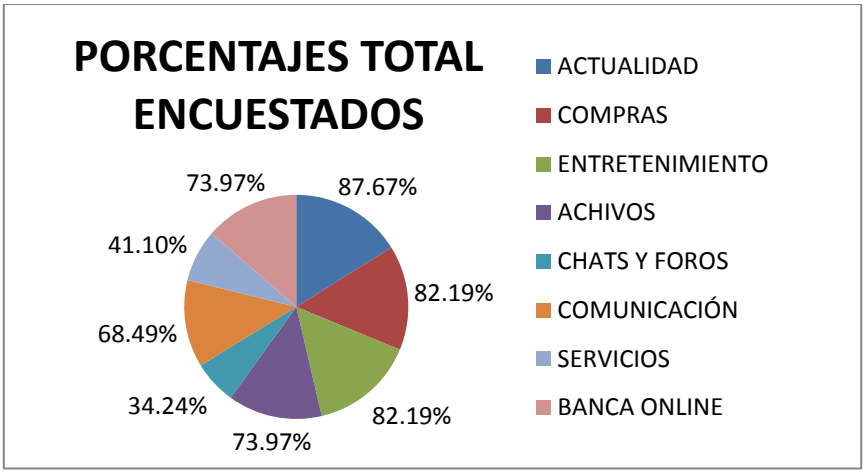


Gráfico 29: Respuestas al ítem 15, ¿utiliza Internet? Si es que si, dígame para cuál de los siguiente ámbitos lo utiliza.

A través del análisis del gráfico se puede llegar a la conclusión de que casi todos los ámbitos han obtenido unas proporciones de respuesta muy elevadas, por lo que la mayoría de los sujetos encuestados utilizan la mayoría de las acciones marcadas *a priori* en la encuesta.

Más particularmente los ámbitos de uso de Internet de los individuos encuestados son: con un 87,67% la información sobre actualidad, con un 82,19% las compras y el entretenimiento, con un 73,97% el uso de la banca online y el intercambio de archivos y con un 68,49% el intercambio de comunicación.

Asimismo solo dos de los porcentajes ocupan menos del 50% de respuesta aunque también se consideran proporciones relevantes para el estudio. Estos ámbitos son: la contratación de servicios –con un 41,10%- y la participación en chats y foros –con un 34,24%-.

Dividiendo los resultados por géneros en ambas categorías los porcentajes son muy elevados, pero hay algunas diferencias con respecto al uso que hacen de Internet tanto las mujeres encuestadas como los hombres encuestados, tal y como vemos representado en la siguiente gráfica:

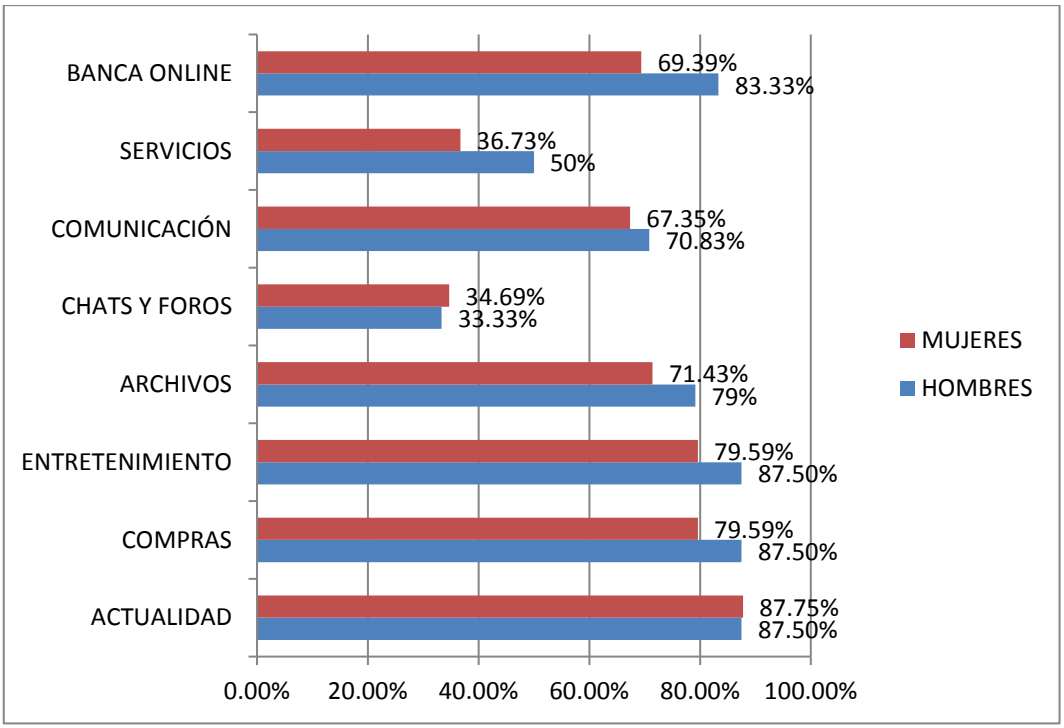


Gráfico 30: Respuestas al ítem 15 por género encuestado, ¿utiliza Internet? Si es que si, dígame para cuál de los siguiente ámbitos lo utiliza.

Como he comentado anteriormente, en ambos géneros los porcentajes de respuesta son muy elevados pero en algunos de ellos hay diferencias apreciables que cabe mencionar. Específicamente, la banca online y la contratación de servicios son los dos ámbitos que comparten distintas proporciones de respuesta en ambas categorías.

En los hombres encuestados el uso de la banca online tiene un porcentaje del 83,33% y la contratación de servicios del 50%.

En las mujeres encuestadas el primer ámbito de uso de Internet ocupa el 69,39% y el segundo el 36,63%.

Este hecho puede llevar consigo una gran conclusión que se verá ratificada o no en los siguientes objetivos específicos, ésta es que los hombres encuestados aparentan ser más impulsivos a la hora de utilizar la red, y por ello se aprecia en estos gráficos que el género masculino encuestado tiene una puntuación mayor que el femenino encuestado en todos los ámbitos de utilización de Internet relativos a adquisición de bienes y servicios online, entre los que se incluye también el uso de la banca online.

Asimismo dividiendo los resultados por edad nos encontramos con que, tal y como he mencionado anteriormente, la mayoría de los usuarios encuestados utilizan casi todos los ámbitos de uso de la red determinados *a priori* en la encuesta, pero hay algunas diferencias de uso que cabe mencionar y que se ven representadas en la siguiente gráfica:

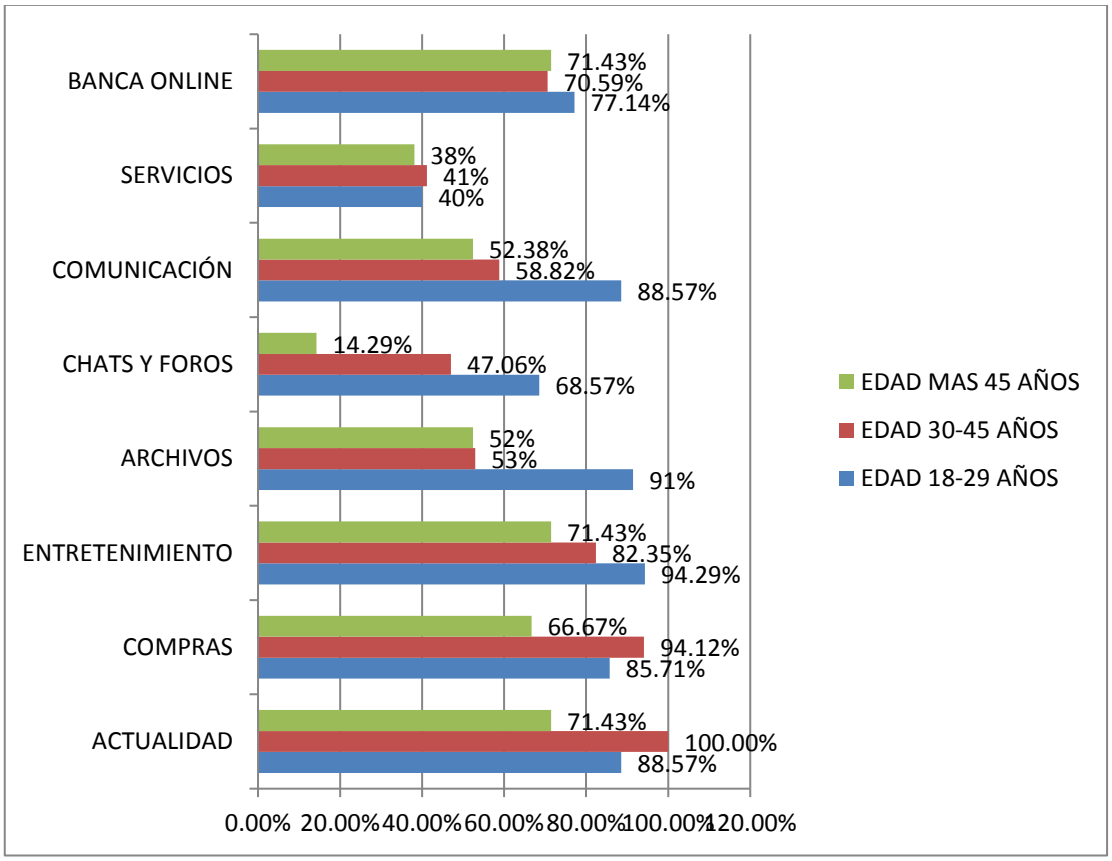


Gráfico 31: Respuestas al ítem 15 por edad encuestada, ¿utiliza Internet? Si es que si, dígame para cuál de los siguiente ámbitos lo utiliza.

Tal y como se ve representado en el gráfico anterior la mayoría de porcentajes son muy elevados. Asimismo las proporciones de respuesta son muy similares en los siguientes ámbitos de uso de la red: uso de la banca online –el 77,14% se encuentran en edades comprendidas entre 18 y 29 años, el 70,59% entre 30 y 45 años y el 71,43% tienen más de 45 años-, contratación de servicios –el 40% se encuentran entre 18 y 29 años, el 41% entre 30 y 45 años y el 38% tienen más de 45 años- y entretenimiento –el 94,24% están en la franja de 18 a 29 años, el 82,35% entre 30 y 45 años y por último el 71,43% tienen más de 45 años-. En éste último ámbito de uso de la red el porcentaje de uso va disminuyendo a medida que aumenta la edad, y lo

mismo ocurre con: el intercambio de archivos –el 91% de los usuarios encuestados se encuentra entre los 18 y los 29 años, el 53% entre los 30 y los 45 años y el 52% tienen más de 45 años-, la participación en chats y foros -68,57%, 47,06% y 14,29% respectivamente- y el intercambio de comunicación –el 88,57% se encuentra entre los 18 y los 29 años, el 58,82% entre 30 y 45 años y el 52,38% tienen más de 45 años-.

En el caso de las compras y de la información sobre actualidad es en la franja de edad comprendida entre los 30 y los 45 años donde los porcentajes de respuesta son mayores. En el caso de las compras el 94,12% se encuentran dentro de estas edades, seguido del 85,71% que tienen entre 18 y 29 años y el 66,67% que tienen más de 45 años. Por último, en el caso de la información sobre actualidad, el 100% de las personas encuestadas con edades comprendidas entre 30 y 45 años utilizan dicho ámbito de uso de Internet en su día a día, seguido de un 88,57% de usuarios encuestados que tienen entre 18 y 29 años y un 71,43% que tienen más de 45 años.

El segundo de los objetivos específicos hace referencia al hecho de si los individuos encuestados saben diferenciar entre una página web legal y una página web ilegal. Esto es muy importante ya que hay individuos que se aprovechan de este desconocimiento para apoderarse del dinero de terceras personas. Más particularmente, tal y como he explicado en el apartado del marco teórico, hay dos formas de fraude o estafa informática como son el Phising o el Pharming –webs ilegales- en las cuales los potenciales infractores crean páginas aparentemente legales con el objetivo de que los usuarios plasmen ahí sus datos bancarios o sus datos personales, y de esta forma se puedan apoderar de ellos para así conseguir tener acceso al dinero de los individuos.

Los resultados de este segundo objetivo en la encuesta son los siguientes:

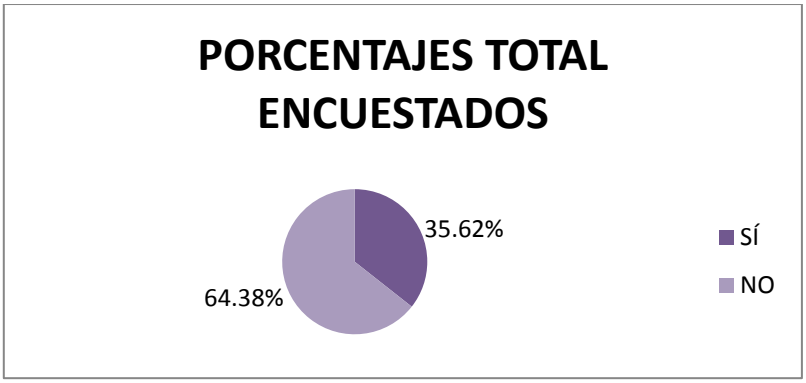


Gráfico 32: Respuestas al ítem 16, ¿sabría distinguir entre una página web legal y una página web ilegal?

Tal y como se ve representado en la gráfica la mayoría de los encuestados –un 64,38%- no saben diferenciar entre una página web legal y una página web ilegal, frente a un 35,62% que afirman que sí sabrían diferenciar entre estas dos páginas si se las encontrasen navegando por Internet o en la bandeja de entrada de su correo electrónico. Los resultados determinan que muchas de las personas que acceden a Internet en su día a día no saben diferenciar una página de otra, lo que es beneficioso para esos individuos que se quieren apoderar del dinero de terceros creando estos portales para captar datos bancarios o datos personales de los usuarios.

Dividiendo las respuestas por géneros no encontramos mayores diferencias ya que los porcentajes son muy similares al total de los encuestados, en los hombres encuestados un 62,50% y en las mujeres encuestadas un 65,31% no saben diferenciar entre un portal y otro a simple vista.

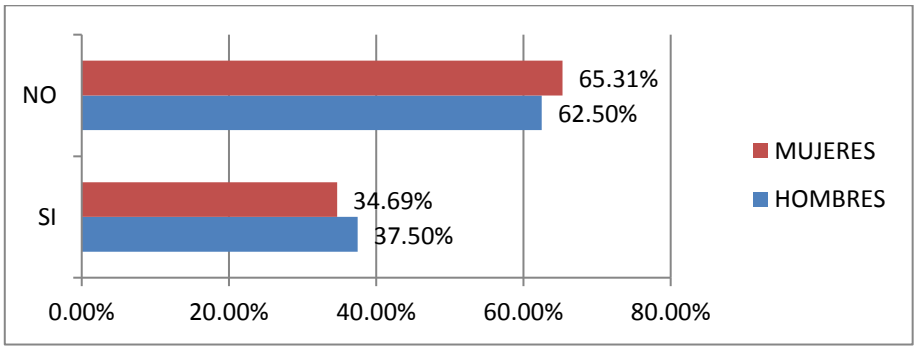


Gráfico 33: Respuestas al ítem 16 por género encuestado, ¿sabría distinguir entre una página web legal y una página web ilegal?

Asimismo dividiendo los resultados por edad nos encontramos con esta gráfica:

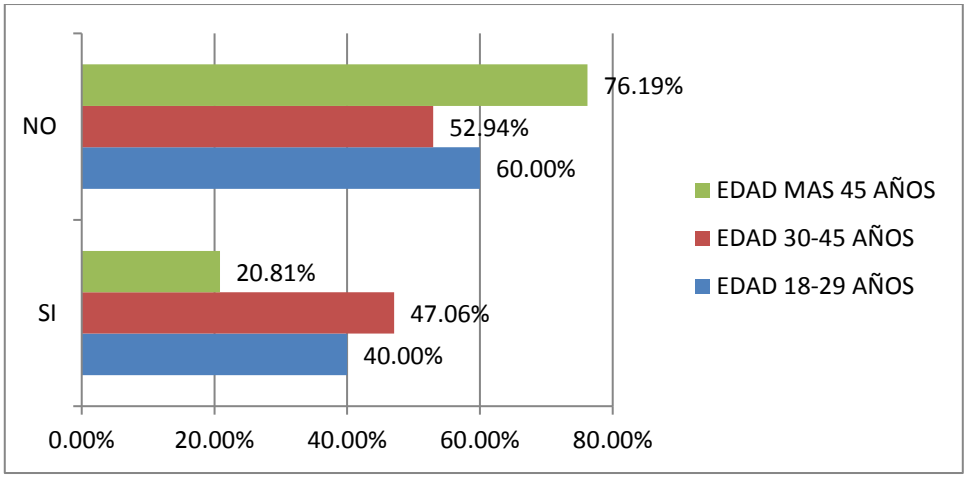


Gráfico 34: Respuestas al ítem 16 por edad encuestada, ¿sabría distinguir entre una página web legal y una página web ilegal?

A través del gráfico podemos apreciar que la franja de edad con el porcentaje más elevado que afirma que sí sabe diferenciar entre una página web legal y una ilegal es la de 30 a 45 años de edad –con un 47,06%-. Cabe pensar que el porcentaje de respuesta mayor que afirma que no sabe diferenciar entre ambas páginas sea el más avanzado en edad y exactamente eso es lo que ocurre con los sujetos encuestados, más particularmente el 76,19% se encuentra en edades superiores a 45 años.

El tercero de los objetivos específicos señalado es relativo a qué problemas ven los encuestados al uso diario de Internet. Con este objetivo lo que se quiere determinar es si los usuarios le dan más importancia a la seguridad, a la falta de confidencialidad o a la calidad del acceso, o por el contrario para ellos es más importante otro tipo de inconvenientes que nada tienen que ver con los mencionados anteriormente como pueden ser: el coste, la velocidad, la publicidad o la infección por virus.

Incluso los usuarios tienen la oportunidad de mencionar cualquier otro problema, que no es ninguno de los anteriores, pero que para ellos presenta una gran importancia.

Tal y como se muestra en la posterior gráfica los resultados son los siguientes:

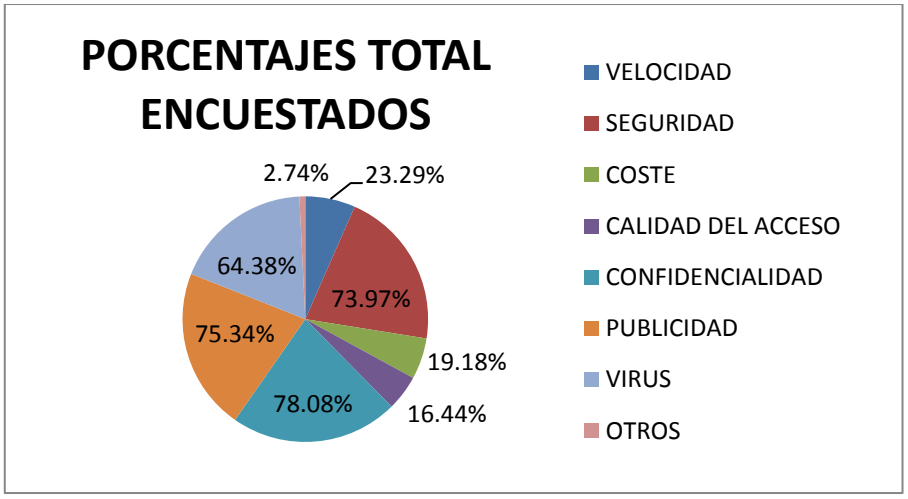


Gráfico 35: Respuestas al ítem 17, ¿qué problemas ve al uso diario de Internet?

Los problemas principales que los usuarios encuestados ven a Internet son: con un 78,08% la falta de confidencialidad, con un 75,34% la publicidad, con un 73,97% la seguridad y por último la infección por virus con un 64,38%.

Los resultados hacen referencia al hecho de que casi la totalidad de los encuestados creen que tanto la seguridad como la falta de confidencialidad son unos inconvenientes muy importantes a la hora de utilizar Internet diariamente. Por el contrario los factores que menos importancia suscita a las personas encuestadas son la calidad del acceso-con un 16,44%- y el coste -con un 19,18%-. En relación con este último era de esperar ya que actualmente el acceder a Internet tanto a través el teléfono móvil como a través del propio domicilio es muy sencillo y además tiene un coste bajo, lo que puede impulsar que muchos de los individuos encuestados no lo consideren como un problema de gran envergadura. Por el contrario, el hecho de que la calidad del acceso no provoque a penas importancia a los encuestados es muy difícil de comprender, ya que este problema hace referencia a si las páginas web crean confianza al individuo tanto por la legalidad de las mismas como por la información que quieren plasmar, desde un punto de vista más general está muy relacionado con la seguridad del acceso. Por ello me parece extraño que la seguridad tenga un porcentaje tan elevado y la calidad sea el problema con menos importancia para los individuos encuestados.

Solamente dos de todos los encuestados propusieron otros problemas como principales con relación al uso diario de Internet –que hacen referencia al 2,74%-. Los inconvenientes que marcaron fueron: la calidad de la información que se plasma en Internet –que es relativo a la calidad del acceso- y el robo de los datos personales -que hace referencia a la seguridad, a la falta de confidencialidad y a la calidad del acceso-.

Dividiendo los resultados por géneros nos damos cuenta de que los porcentajes más elevados son muy similares entre hombres encuestados y mujeres encuestadas, lo que varía es el orden de porcentaje de respuesta. En cuanto a los demás problemas son totalmente diferentes unos de otros tal y como explicaré a continuación:

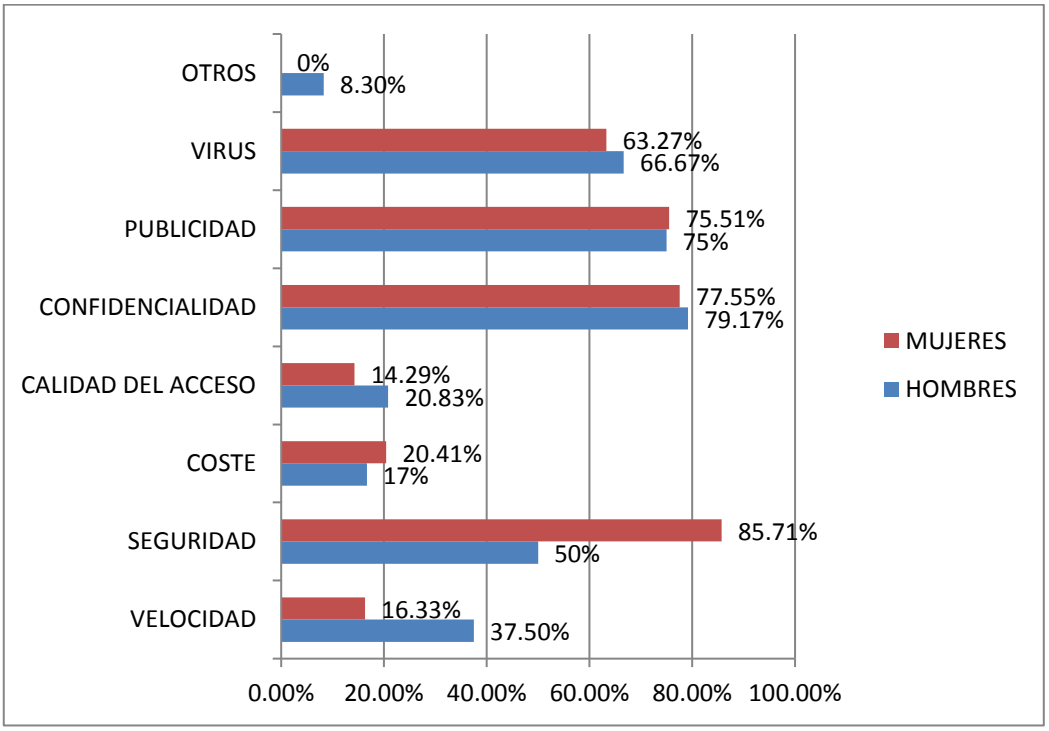


Gráfico 36: Respuestas al ítem 17 por género encuestado, ¿qué problemas principales ve al uso diario de Internet?

Para las mujeres encuestadas la seguridad –con un 85,71%- es el inconveniente que más importancia tiene a la hora de utilizar diariamente Internet, seguido de la falta de confidencialidad –con un 77,55%-, de la publicidad –con un 75,51%- y por último de la infección por virus –con un 63,27%-. Esto no tiene mayor diferenciación con respecto al total de los encuestados. Lo que sí varía son los problemas que menos importancia suscita a las mujeres encuestadas, estos son: la calidad del acceso –con

un 14,29%- y la velocidad –con un 16,33%-. El coste aumentaría de proporción en relación con el total de los encuestados –llegaría a ocupar un 20,41%-. Para los hombres encuestados el problema más significativo es la falta de confidencialidad –con un 79,17%-, seguido de la publicidad –con un 75%- y de la infección por virus –con un 66,67%-. Lo que más llama la atención es que la seguridad solamente ocupa el 50% de respuesta, esto es muy importante ya que ratifica que en los hombres encuestados la fiabilidad con respecto a Internet es un hecho que les suscita mucho menos interés que a las mujeres encuestadas. Por último los factores que menos importancia generan en los hombres encuestados son diferentes a los de las mujeres encuestadas, entre ellos encontraríamos el coste –con un 17%- y la calidad del acceso -con un 20,83%-. La velocidad es un factor que aumentaría de proporción en los hombres encuestados y llegaría hasta el 37,50% de respuesta.

Asimismo, dividiendo los resultados por edad, nos encontramos con el hecho de que la mayoría de los problemas determinados *a priori* en la encuesta tienen los porcentajes muy similares entre las tres franjas de edad, tal y como se puede apreciar en la siguiente gráfica:

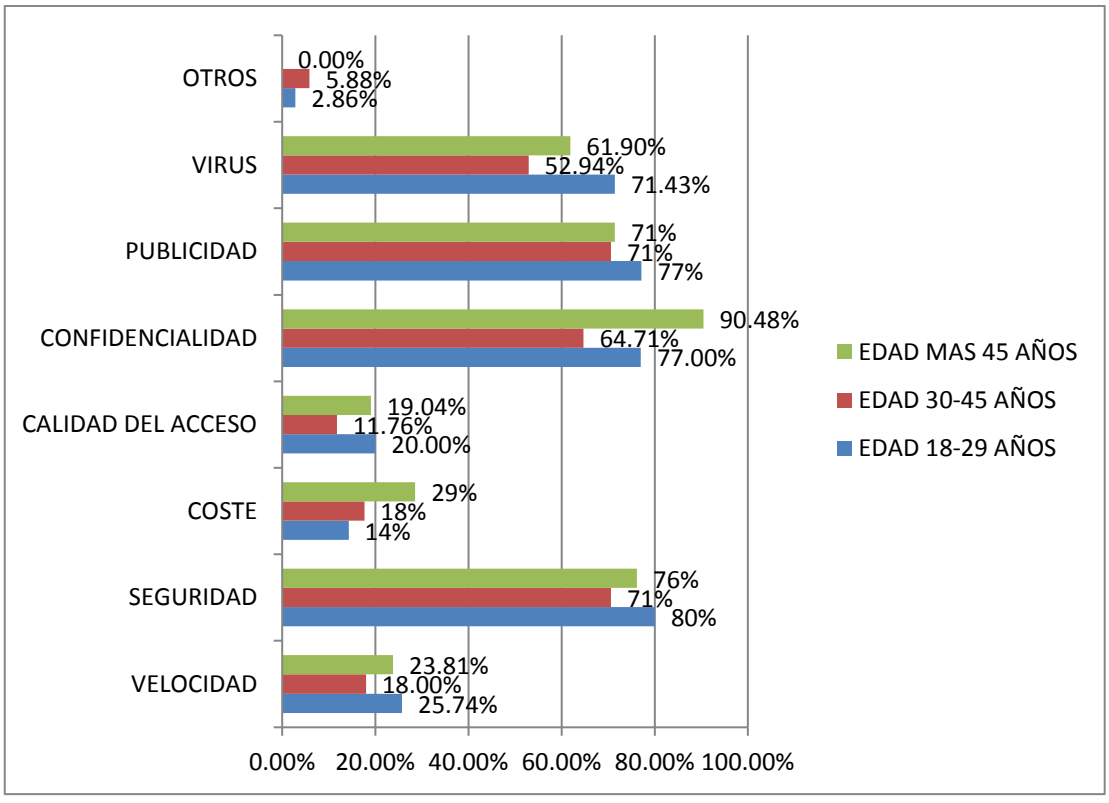


Gráfico 37: Respuestas al ítem 17 por edad encuestada, ¿qué problemas principales ve al uso diario de Internet?

Tal y como he comentado anteriormente y como se ve representado en la gráfica, todos los problemas determinados en la encuesta tienen unos porcentajes muy similares, pero cabe mencionar algún aspecto. Éste está relacionado con el hecho de que ciertos problemas suscitan más importancia a medida que avanza la edad, más particularmente éstos son: la confidencialidad –un 77% de los sujetos encuestados se encuentran entre los 18 y los 29 años, un 64,71% entre los 30 y los 45 años y por último, un 90,48% tienen más de 45 años-; y el coste –un 14% tienen edades comprendidas entre los 18 y los 29 años, seguido de un 18% que se encuentran ente 30 y 45 años y un 29% que tienen más de 45 años-. El resto de los problemas no cabe mencionarlos ya que tienen unos porcentajes de respuesta muy similares entre sí.

El cuarto de los objetivos específicos es en el que se analiza, a través de una escala Likert de 1 a 5 puntos -donde 1 es poco seguro y 5 es muy seguro-, si los sujetos encuestados creen que Internet es un entorno seguro o no lo es para adquirir bienes o servicios. Con este objetivo lo que se quiere examinar es si los sujetos encuestados confían en la red para realizar compras o adquisiciones de servicios.

Los resultados del sondeo para esta pregunta se encuentran expresados en la siguiente gráfica:

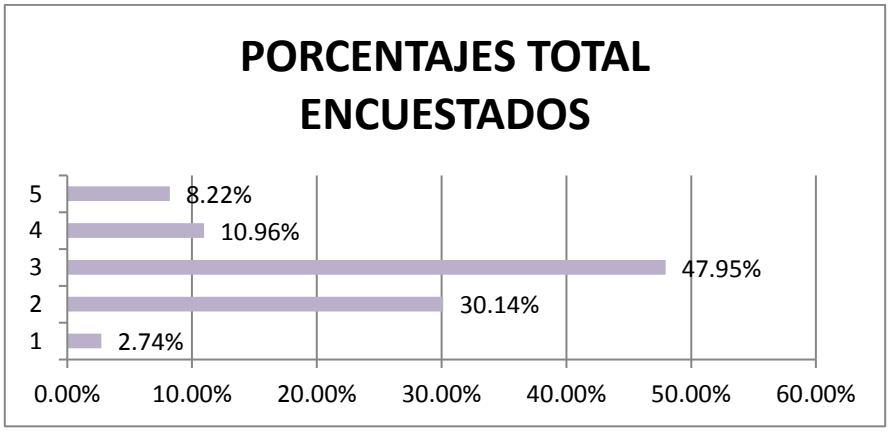


Gráfico 38: Respuestas al ítem 18, ¿cree que Internet es un entorno seguro para realizar compras o contratar servicios?

La mayoría de los sujetos encuestados han respondido con un 3 en la escala -47,95%- con lo que cabe pensar que muchos de los individuos encuestados ni creen que sea 100% seguro pero tampoco creen que sea 100% inseguro. Con esto considero que en los individuos encuestados existe una percepción de inseguridad en la red, pero

tampoco es tan intensa como para no realizar compras de bienes o servicios a través de la misma.

Dividiendo los resultados por géneros no hay mayor diferencia de lo observado con anterioridad. En las mujeres encuestadas el 44,90% marcaron un 3 en la escala. En los hombres encuestados un 54,17% también respondieron al ítem con un 3. Ambos resultados se pueden apreciar en la gráfica siguiente:

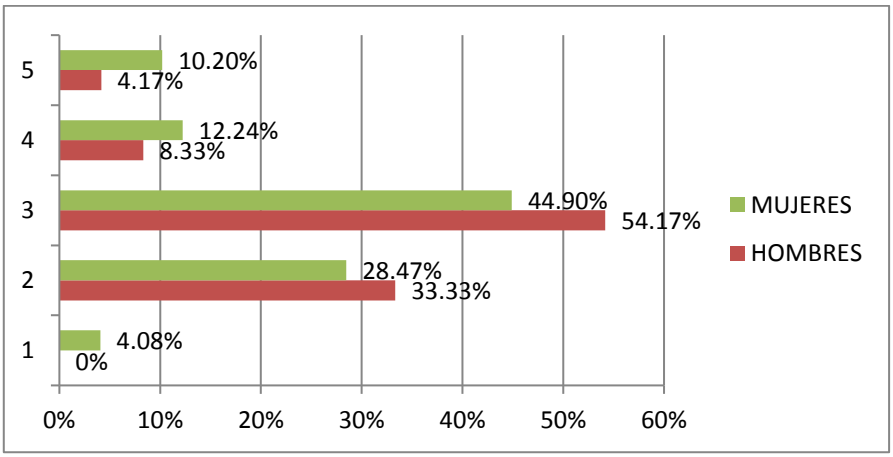


Gráfico 39: Respuestas al ítem 18 por género encuestado, ¿cree que Internet es un entorno seguro para realizar compras o contratar servicios?

Asimismo dividiendo los resultados por edad encontramos algunos aspectos que son importantes de matizar, pero primero es importante plasmar la gráfica que representa los resultados por edades:

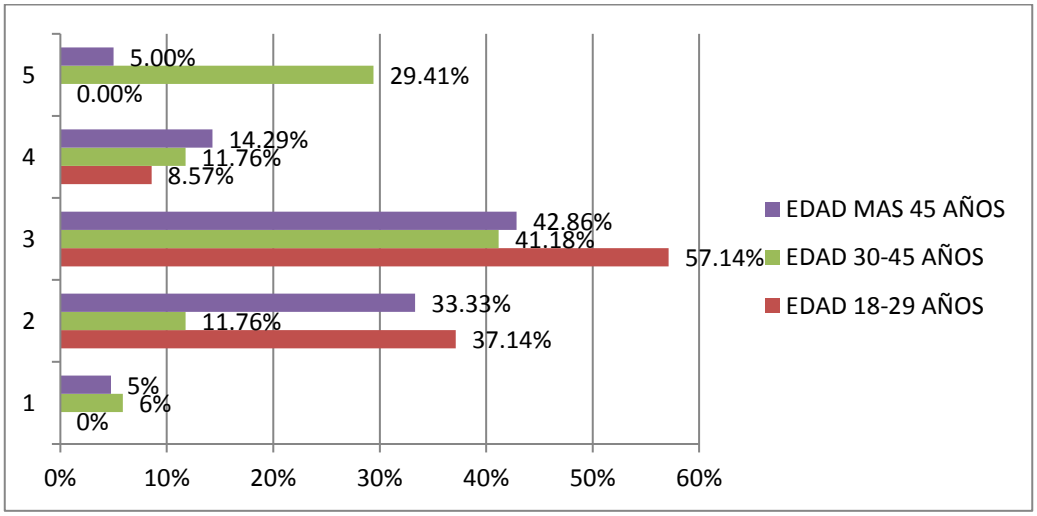


Gráfico 40: Respuestas al ítem 18 por edad encuestada, ¿cree que Internet es un entorno seguro para realizar compras o contratar servicios?

Se puede ver claramente plasmado en la gráfica que la mayoría de los usuarios encuestados de las tres franjas de edad han respondido con un 3 en la escala. Esto no tiene mayor diferencia a lo mencionado hasta el momento.

Lo primero que llama la atención de la gráfica anteriormente expresada es que ninguno de los sujetos que se encuentran entre 18 y 29 años de edad ha respondido en la escala con un 1 o con un 5. Con este hecho cabe pensar que no hay ningún joven que se fie o no se fie 100% de la red para adquirir bienes o contratar servicios.

Otro de los aspectos que llama la atención es la gran diferencia de respuesta entre las franjas de 18 y 29 años y de más de 45 años, con la de edades comprendidas entre 30 y 45 años, con el hecho de marcar un 2 en la escala. Más particularmente el 57,14% de los jóvenes y el 33,33% de la franja de edad más avanzada han marcado un 2 en la escala Likert, frente a un 11,76% que se encuentran entre los 30 y los 45 años. Este hecho puede afirmar que en los sujetos encuestados los usuarios que tienen entre 30 y 45 años de edad se fían más de la red que los de edades restantes.

Esto se puede ver ratificado con el último de los aspectos que más llama la atención de la gráfica, éste es que el 29,41% de los usuarios encuestados que se encuentran en edades comprendidas entre 30 y 45 años han marcado un 5 en la escala Likert.

El quinto de los objetivos específicos a determinar es el relativo a las transferencias bancarias. Con este propósito se quiere analizar qué tipo de preferencia tienen los individuos encuestados a la hora de realizar una transacción bancaria. Más particularmente se quiere conocer si, por un lado prefieren hacer las transferencias online, o por el contrario se inclinan por llevarlas a cabo directamente en el banco.

Además de ello se les pide que justifiquen la elección de una preferencia u otra para así poder determinar cuál es realmente el motivo de la selección.

Los resultados de la encuesta para este objetivo se encuentran plasmados en la siguiente gráfica:

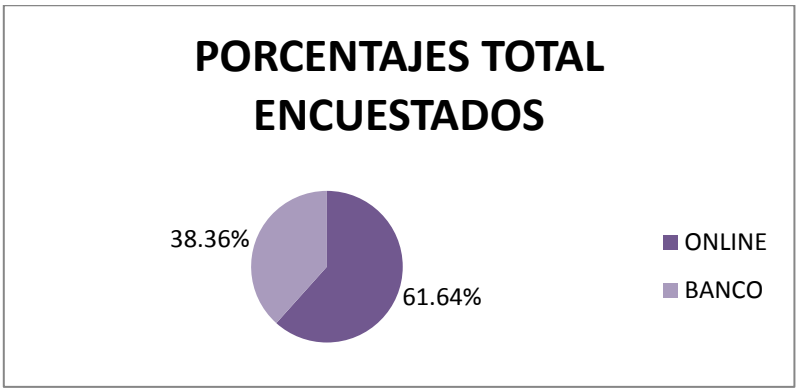


Gráfico 41: Respuestas al ítem 19, ¿qué método de pago utiliza usted, el método online o prefiere acudir directamente al banco?

Según aparece expresado en el gráfico el 61,64% de los individuos encuestados prefieren hacer las transferencias bancarias online, frente a un 38,36% que se inclina por acudir directamente al banco a realizarlas. Con este resultado lo que se quiere transmitir es que más de la mitad de los encuestados confían en Internet para realizar sus transacciones bancarias. Pero una vez analizados los motivos que los individuos encuestados dieron para poder justificar su elección, me doy cuenta de que realmente no es la confianza lo que impulsa a las personas encuestadas a realizar las transferencias bancarias a través del método online, tal y como se expresa en la siguiente tabla:

MOTIVOS BANCO	MARCADOS	MOTIVOS ONLINE	MARCADOS
SEGURIDAD	17	SEGURIDAD	6
FACILIDAD	1	***COMODIDAD***	24
COSTUMBRE	2	***RAPIDEZ***	13
COMODIDAD	1	PRACTICO	3
CONFIANZA	1	FALTA DE TIEMPO	1
TRATO PERSONAL	3	FACILIDAD	2
NO SÉ HACERLO ONLINE	1	NO RECARGOS	1
GENERA EMPLEO	1	EL BANCO LIMITA HORARIO	1
		NO DESPLAZAMIENTO	1
		SOLO TENGO BANCA ONLINE	1

Gráfico 42: Motivos para elección de método online o banco, ítem 19.

Una vez analizada la tabla se puede apreciar que 24 de los individuos encuestados marcaron la comodidad como motivo clave para la elección del método online a la hora realizar una transacción bancaria, seguido de 13 personas que marcaron la rapidez como causa de su selección. En el caso del banco vemos que 17 de los encuestados señalaron la seguridad como razón principal de su preferencia.

Con todo ello cabe pensar que la mayoría de los sujetos encuestados que dieron un motivo para la justificación de la respuesta le dan más importancia a realizar las transferencias de una manera confortable desde casa, desde el trabajo, sin tener la necesidad de desplazarse hasta el banco más cercano, que a lo que realmente debe tener más interés, que es la confianza en que sus datos bancarios o sus datos personales estén en buenas manos y no sean utilizados por posibles infractores para apoderarse de ellos. Da la casualidad que ese es el motivo principal que dieron los individuos encuestados que marcaron el banco como método mediante el cual realizan la mayoría o todas sus transacciones bancarias.

Dividiendo las respuestas por géneros encontramos grandes diferencias de respuesta entre hombres encuestados y mujeres encuestadas. A continuación plasmaré la gráfica en la que aparecen los resultados de ambas categorías y posteriormente la analizaré:

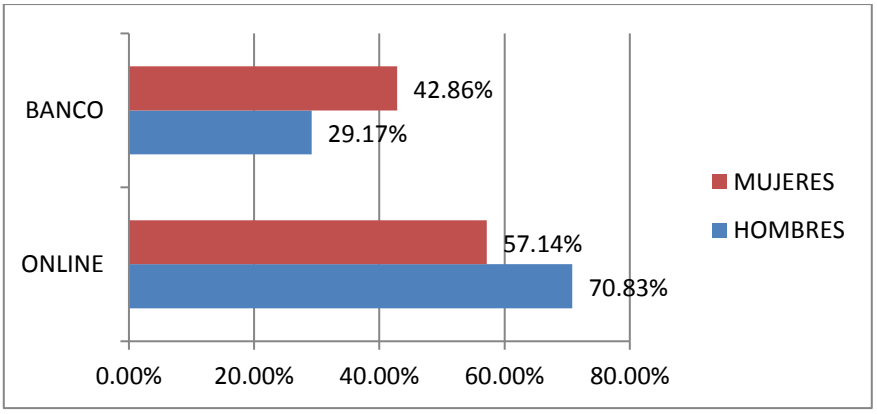


Gráfico 43: Respuestas al ítem 19 por género encuestado, ¿qué método de pago utiliza usted, el método online o prefiere acudir directamente al banco?

A simple vista las diferencias entre ambos géneros son bastante apreciables, el 57,14% de las mujeres encuestadas y el 70,83% de los hombres encuestados prefieren el método online para llevar a cabo sus transacciones, es decir, que al mismo tiempo que un porcentaje muy elevado de hombres encuestados afirman

utilizar dicho procedimiento, en las mujeres encuestadas casi hay un 50% de respuesta entre ambos dos sistemas de pago. En la práctica estas respuestas se pueden configurar de una forma, tal y como he comentado en el objetivo específico número uno, según éste cabe pensar que mientras que los hombres encuestados parecen más impulsivos, que se dejan llevar más por la comodidad y la rapidez de una transferencia online, por el contrario las mujeres encuestadas aparentan ser más reflexivas en cuanto a las consecuencias de la plasmación de sus datos bancarios o personales en Internet, y por ello los porcentajes entre ambos dos métodos son casi similares.

Asimismo, realizando la diferenciación por edad, en la siguiente gráfica se puede apreciar que los porcentajes en las tres franjas de edad marcadas en la encuesta son muy similares tanto para la realización de las transferencias bancarias a través de la red como a través del banco:

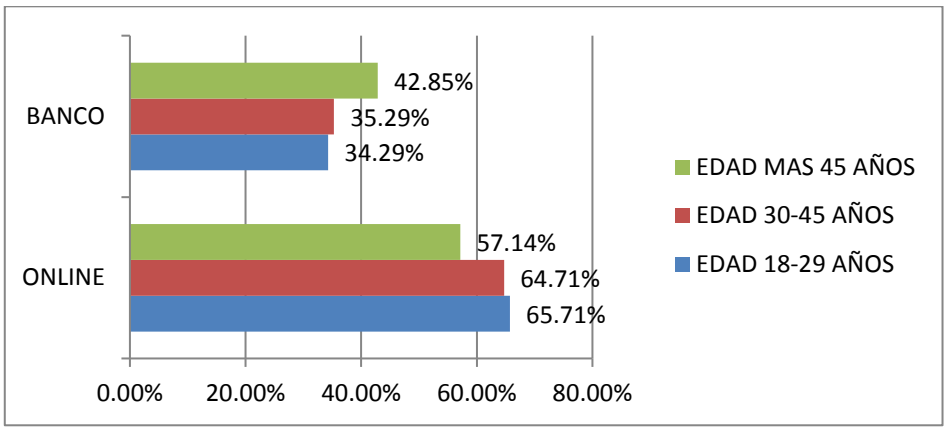


Gráfico 44: Respuestas al ítem 19 por edad encuestada, ¿qué método de pago utiliza usted, el método online o prefiere acudir directamente al banco?

Tal y como acabo de comentar anteriormente y como se ve reflejado en la gráfica los porcentajes de respuesta para ambos dos métodos de pago son más o menos similares. La mayoría de los sujetos encuestados utilizan el método online, pero más particularmente el 65,71% de las personas que se encuentran en la franja de edad de 18 a 29 años utilizan este método, el 64,71% de los sujetos que tienen entre 30 y 45 años también y por último se encuentra el porcentaje menor, aunque más o menos similar a los anteriores -un 57,14%-, que corresponde a los individuos encuestados que tienen más de 45 años.

El sexto objetivo es referente al método de pago utilizado cuando se realiza una compra online. Este propósito tiene como fin averiguar si los sujetos encuestados optan por plasmar sus datos bancarios en las páginas de compra de bienes online, o por utilizar otros métodos de pago como pueden ser: a contrareembolso, domiciliación bancaria, transferencia o utilizan PayPal y similares. También es de interés conocer si los usuarios utilizan otro método, que no está expresamente referido en la encuesta, con el fin de determinar todas las formas posibles de pago que emplean los sujetos encuestados.

Los resultados del sondeo para este objetivo se encuentran expresados en el siguiente gráfico:

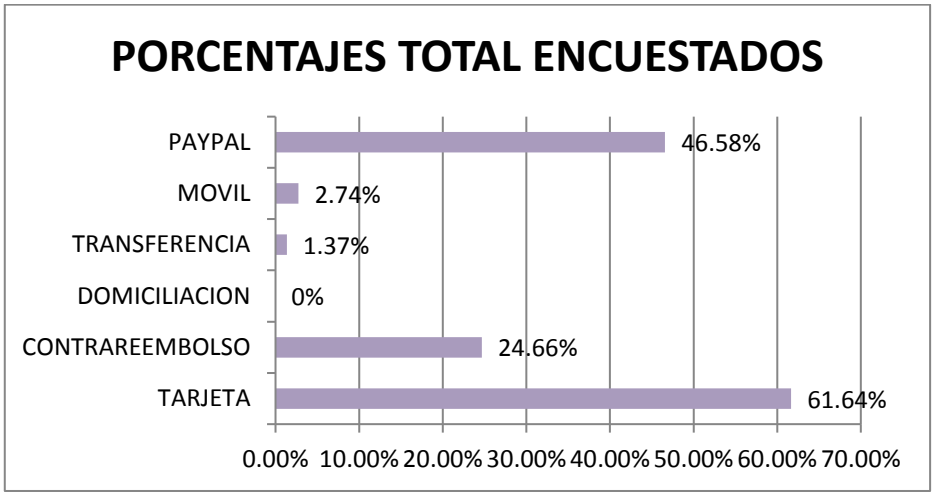


Gráfico 45: Respuestas al ítem 20, ¿qué método de pago utilizaría?

El 61,64% de los encuestados utilizan sus tarjetas personales de crédito o de débito para realizar las compras de bienes online. Seguido del 46,58% que afirman utilizar PayPal y similares. Y por último el 24,66% de los sujetos encuestados manifiestan que se decantan más por el método a contrareembolso.

Hay que tener en cuenta que en esta pregunta de la encuesta la respuesta es múltiple, es decir, que las personas que la están realizando pueden marcar más de una opción al mismo tiempo, y por lo tanto la misma persona que utiliza la tarjeta puede emplear también el método a contrareembolso para algunas de sus compras y viceversa. De todas formas, más de la mitad de los usuarios han manifestado utilizar la tarjeta para ejecutar sus compras online, tal y como se ve representado en la siguiente tabla:

MÉTODOS DE PAGO	MARCADOS
TARJETA+CONTRAREEMBOLSO+PAYPAL	3
TARJETA	**22**
PAYPAL	**16**
TARJETA+PAYPAL	**12**
TARJETA+CONTRAREEMBOLSO	7
CONTRAREEMBOLSO+PAYPAL	2
CONTRAREEMBOLSO	4
TARJETA+CONTRAREEMBOLSO+TRANSFERENCIA+PAYPAL	1
A TRAVÉS DEL TELÉFONO MÓVIL	2
NINGUNO	4

Gráfico 46: Respuestas múltiples al ítem 22, ¿qué método de pago utilizaría?

Según la tabla 22 de los sujetos encuestados han afirmado que utilizan solamente la tarjeta para realizar sus compras online, seguido de 16 que manifestaron que emplean el método de pago denominado PayPal y posteriormente 12 de los sujetos encuestados declararon que utilizan ambos dos métodos para adquirir bienes a través de Internet.

Solamente cuatro individuos de todos los sujetos encuestados han declarado que no utilizan ninguno de los métodos porque no realizan compras de bienes por Internet.

Dividiendo los resultados por géneros, no hay ninguna diferencia apreciable con respecto al total de los encuestados como se puede apreciar en el posterior gráfico:

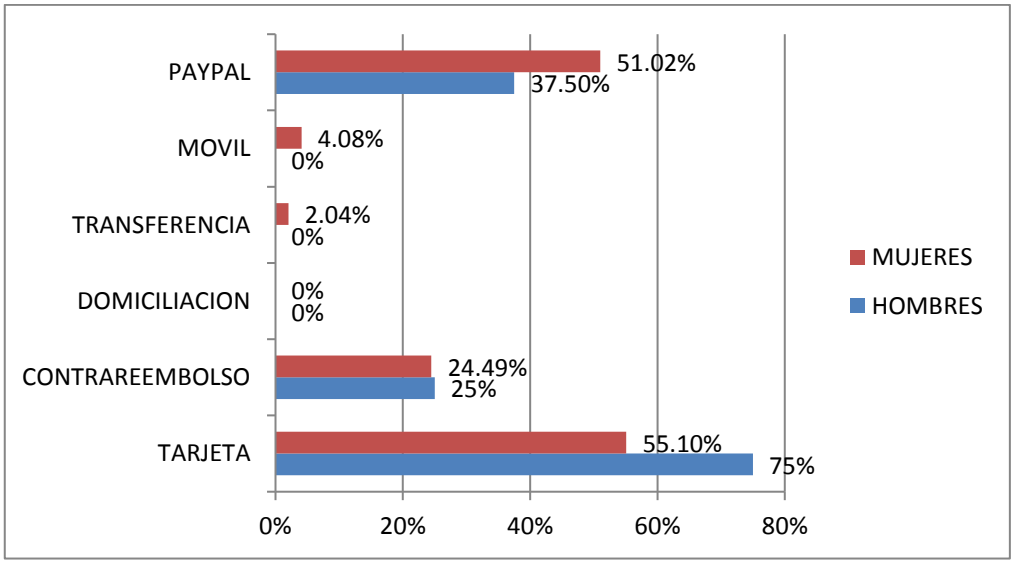


Gráfico 47: Respuestas al ítem 20 por género encuestado, ¿qué método de pago utilizaría?

Tal y como se puede observar en la gráfica ni el orden de preferencia ni los métodos de pago son diferentes a los del total de los encuestados ni en hombres encuestados ni en mujeres encuestadas. Asimismo las proporciones de respuesta en las mujeres encuestadas son: el uso de la tarjeta con un 55,10%; el de PayPal y similares con un 51,02% y la utilización del método a contrareembolso con un 24,49% de respuesta; el resto de porcentajes son mínimos. En el caso de los hombres encuestados se encontraría en cabeza el uso de la tarjeta para realizar compras online con un 75%, seguido del de PayPal y similares con un 37,50% y por último, el sistema a contrareembolso con una proporción del 25% de respuesta. Lo que más llama la atención en los hombres encuestados es que los demás porcentajes son del 0%, y si a esto se le suma el hecho de que, según las respuestas, utilizan mucho más la tarjeta bancaria que cualquier otro método de pago, se puede ver ratificada la conclusión que he comentado objetivos atrás de que los hombres encuestados aparentan ser más impulsivos que las mujeres encuestadas a la hora de realizar acciones en la red.

Ahora bien, dividiendo los resultados por edades hay algún aspecto que es importante poder matizar:

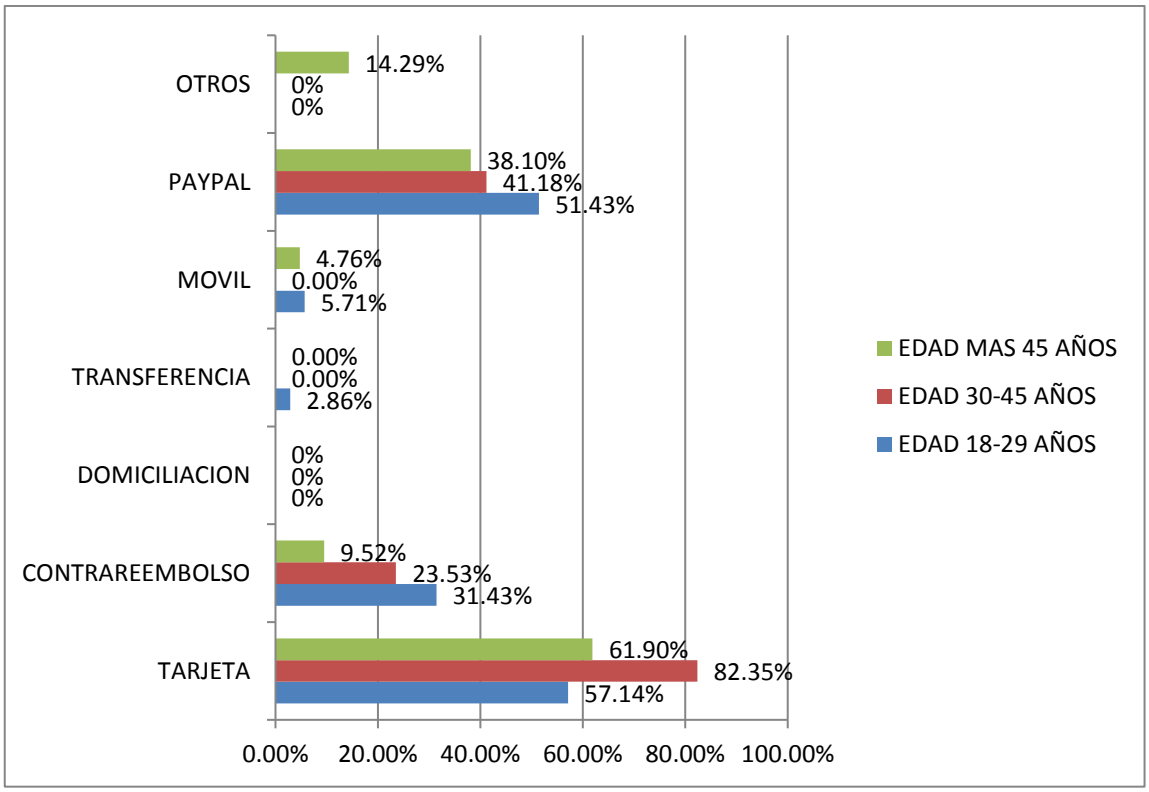


Gráfico 48: Respuestas al ítem 20 por edad encuestada, ¿qué método de pago utilizaría?

Más particularmente hay dos aspectos que, a través del análisis de la anterior gráfica, cabe mencionar. El primero de ellos está relacionado con el uso de la tarjeta de crédito o de débito para realizar pagos en Internet, tal y como se ve en el anterior gráfico son los sujetos encuestados comprendidos entre los 30 y los 45 años los que más utilizan este método de pago para realizar sus compras online –el 82,35%-. Es sorprendente que la segunda franja de edad que se encuentra con el porcentaje seguido a éste son los individuos encuestados mayores de 45 años con un 61,90% de respuesta. Asimismo los jóvenes de entre 18 y 29 años tienen una cifra muy similar a la anterior, un 57,14%.

El segundo aspecto que es importante mencionar es el relacionado con los métodos de pago a contrareembolso y PayPal y similares que disminuyen su uso para realizar compras online a medida que aumenta la edad. En el caso del pago a contrareembolso, en los jóvenes encuestados, el porcentaje de respuesta es del 31,43%, en los sujetos encuestados comprendidos entre 30 y 45 años del 23,53% y por último en los individuos encuestados mayores de 45 años la cifra desciende hasta el 9,52%. Para finalizar con este objetivo queda por analizar el método de pago denominado PayPal y similares, entre los individuos encuestados de 18 a 29 años el porcentaje es del 51,43%, en la siguiente franja de edad, que son los sujetos encuestados de 30 a 45 años, la cifra es del 41,18% y en los individuos encuestados mayores de 45 años del 38,10%.

El séptimo de los objetivos específicos marcados al principio es referente al grado de confianza que tienen los encuestados sobre la protección de sus datos en Internet. Este propósito es clave ya que cabe pensar que el hecho de que los sujetos encuestados utilicen métodos de pago en los que se necesiten datos personales, como por ejemplo la tarjeta de crédito o de débito –tal y como se ha determinado en el objetivo anterior-, puede tener como consecuencia que confíen en la protección de dichos datos en la red.

En la encuesta la medición del grado de seguridad que tienen los usuarios en la protección de sus datos personales en Internet se va a llevar a cabo a través de una escala Likert de 1 a 5 puntos –donde 1 es poco seguro y 5 es muy seguro- y los resultados obtenidos se ven plasmados en la siguiente gráfica:

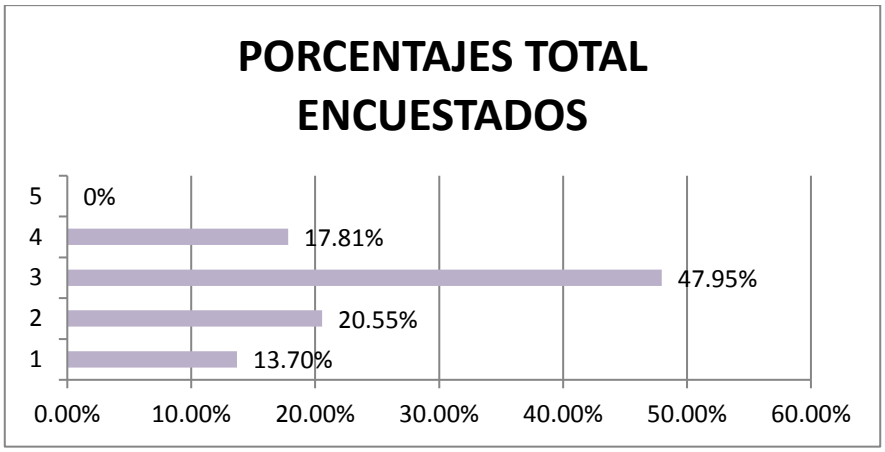


Gráfico 49: Respuestas al ítem 21, ¿confía usted en la protección de sus datos en Internet?

Según el gráfico la mayoría de los encuestados se encuentra en una situación de incertidumbre en la cual ni confían ni desconfían del todo en la protección de sus datos personales a través de la red, por ello hay un 47,95% de sujetos que han marcado un 3 en la escala Likert.

Dividiendo los resultados por géneros nos encontramos que la mayoría tanto de hombres encuestados como de mujeres encuestadas respondieron con un 3 en la escala como podemos observar en el siguiente gráfico:

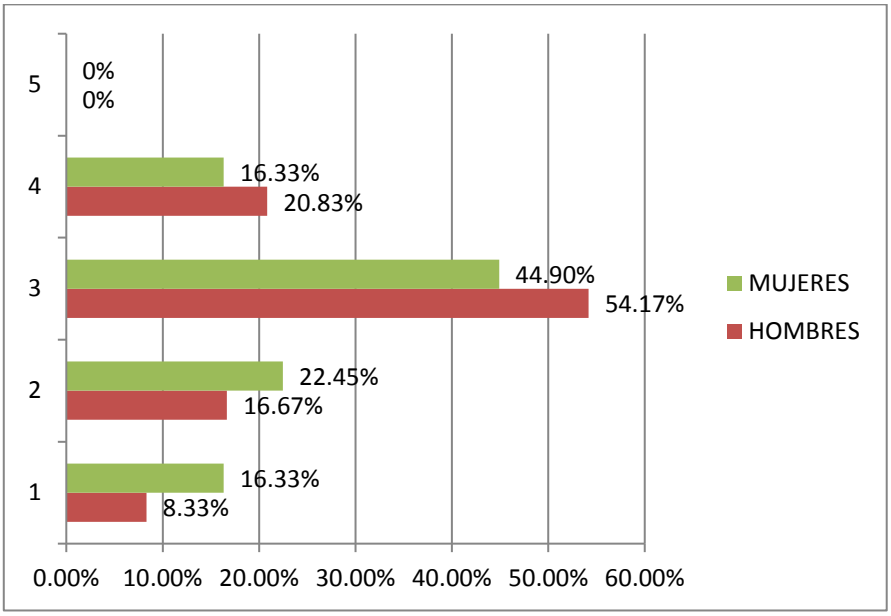


Gráfico 50: Respuestas al ítem 21 por género encuestado, ¿confía usted en la protección de sus datos en Internet?

Tal y como he mencionado anteriormente la mayoría tanto de mujeres encuestadas como de hombres encuestados ni confían ni desconfían totalmente de Internet como protector de sus datos personales, más particularmente el 44,90% de las mujeres encuestadas y el 54,17% de los hombres encuestados respondieron con un 3 al ítem. Con esto cabe pensar que en los sujetos encuestados sí existe una percepción de inseguridad –ya que nadie ha contestado que confíe 100% en Internet- pero esta percepción no es demasiado importante como para que no utilicen la red para realizar todo tipo de acciones en las que datos personales o bancarios son necesarios, tal y como se ha visto confirmado en los objetivos anteriores.

Dividiendo los resultados por edad nos encontramos con la siguiente gráfica:

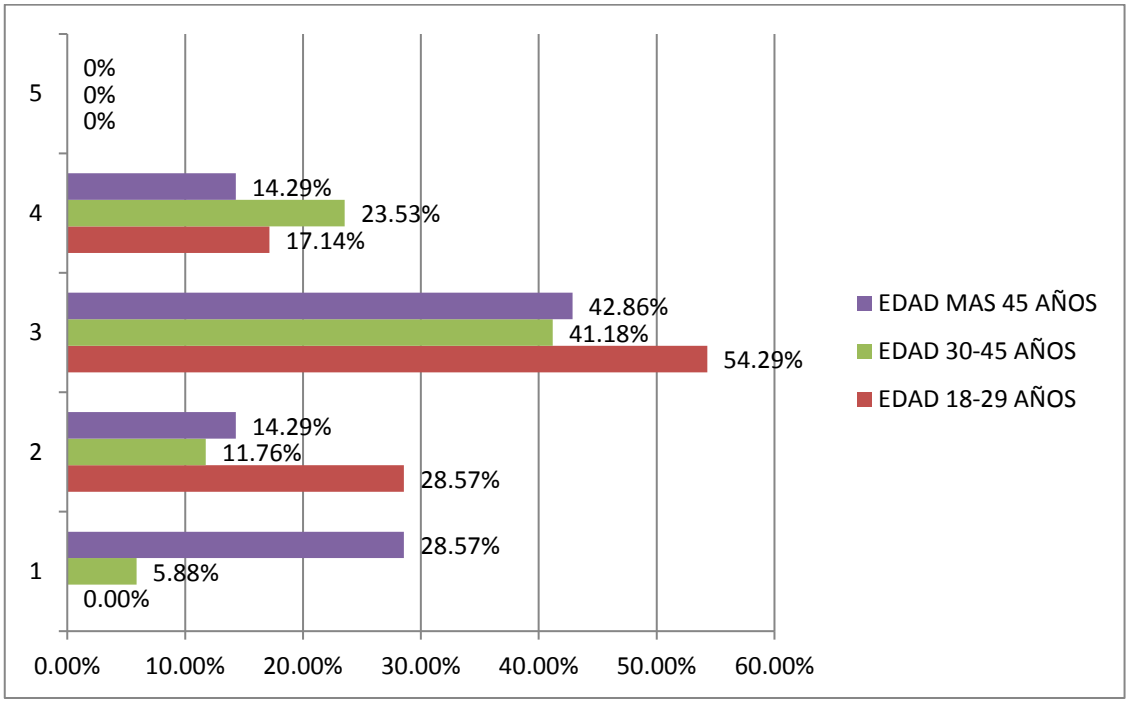


Gráfico 51: Respuestas al ítem 21 por edad encuestada, ¿confía usted en la protección de sus datos en Internet?

Lo primero que es importante mencionar es que casi la mitad de las tres franjas de edad divididas en la encuesta ha respondido con un 3 a la escala Likert -54,29%, 41,18% y 42,86% respectivamente-.

Ahora bien, hay algunos aspectos que son importantes para destacar. El primero de ellos guarda relación con el objetivo número seis, que por recordar era el uso de ciertos métodos de pago a la hora de realizar compras a través de la red, y tal y como

se aprecia en la gráfica anterior el 23,53% de los sujetos encuestados comprendidos entre los 30 y los 45 años de edad han respondido con un 4 en la escala, esto concuerda con que sean estos sujetos los que más utilicen la tarjeta a la hora de realizar compras a través de Internet.

El segundo aspecto que cabe mencionar es que el 28,57% de los jóvenes encuestados, que tienen una edad entre los 18 y los 29 años, contestaron a este ítem con un 2 con lo cual su percepción de inseguridad en la red es mayor que los de la franja de entre 30 y 45 años. Lo mismo ocurre con los sujetos encuestados que tienen una edad superior a los 45 años, pero en este caso estos individuos han respondido con un 28,57% al ítem con un , con lo que cabe pensar que su percepción de inseguridad es aún mayor que la de los jóvenes encuestados.

El penúltimo de los objetivos específicos a analizar hace referencia a la opinión que tienen los encuestados con respecto al hecho de si a través de la red a veces se viola su derecho a la intimidad. Este fin guarda mucha relación con el anterior ya que cabe pensar que las personas que hayan contestado con una puntuación baja en la escala Likert del objetivo que le precede a éste van a responder que la red viola su derecho a la intimidad, ya que no confían en ella para proteger sus datos personales y por ende cabe pensar que estos sujetos encuestados podrían creer que en cualquier momento se puede llevar a cabo un traspaso o un robo de sus datos.

Los resultados del sondeo a este objetivo los encontramos expresados en la siguiente gráfica:

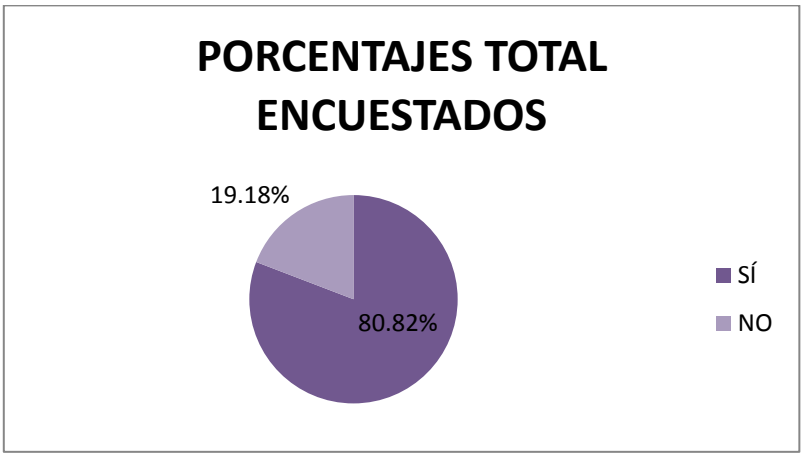


Gráfico 52: Respuestas al ítem 22, ¿cree que su derecho a la intimidad a veces se ve violado a través de la red?

A simple vista se aprecia claramente que la mayoría de los encuestados cree que su derecho a la intimidad se ve violado a través de la red en algunas ocasiones, más particularmente el 80,82% así lo piensan.

De la misma forma, dividiendo los resultados por géneros, podemos observar que son prácticamente similares unos de otros pero hay un hecho que llama mucho la atención como evaluaré a continuación después de presentar la gráfica de ambas categorías:

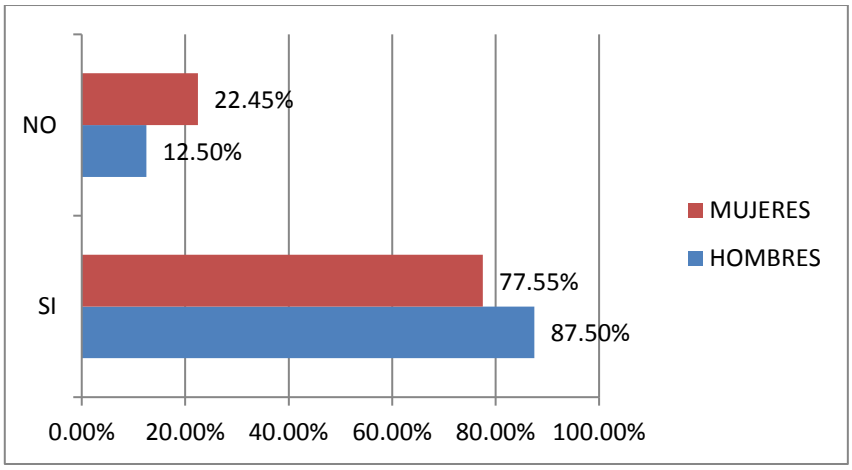


Gráfico 53: Respuestas al ítem 22 por género encuestado, ¿cree que su derecho a la intimidad a veces se ve violado a través de la red?

Ambos dos géneros tienen una puntuación muy elevada de respuesta al hecho de creer que sí que Internet afecta a su derecho a la intimidad –un 77,55% en las mujeres encuestadas y un 87,50% en los hombres encuestados-. Pero que el porcentaje sea mayor en los hombres encuestados que en las mujeres encuestadas tiene mucho interés a la hora de analizar las respuestas al ítem. En todas las respuestas analizadas hasta el momento he examinado a hombres que confían en Internet para plasmar sus datos personales, para realizar compras online, para llevar a cabo transferencias bancarias a través de la red, etc. y es muy importante ver que, a la hora de realizarles la pregunta más específica sobre la posible vulneración de su derecho a la intimidad, la mayoría de ellos crea que sí que Internet afecta a ese derecho en determinadas ocasiones. Esto ratifica que en los hombres encuestados, aunque utilicen los datos bancarios o personales diariamente para muchas de sus actividades en Internet, en ellos existe una percepción de inseguridad que les hace mantenerse alerta en el hecho de que en la red existe la comisión de múltiples tipos

de actos delictivos realizados a través de compras. En mi opinión creo que la percepción de inseguridad es una emoción que va unida al hecho de utilizar el ciberespacio para realizar cualquier tipo de actividad, ya que todo el mundo conoce que Internet es un espacio en el que la comisión de un ciberdelito se encuentra a la orden del día.

Pero en el caso de las mujeres encuestadas no resulta llamativa su respuesta ya que en toda la encuesta se muestran más pensativas a la hora de realizar actos online, y era de esperar que la mayoría de ellas respondiesen que sí al hecho de que la red a veces vulnere su derecho a la intimidad.

Asimismo dividiendo los resultados por edad nos encontramos con el siguiente gráfico:

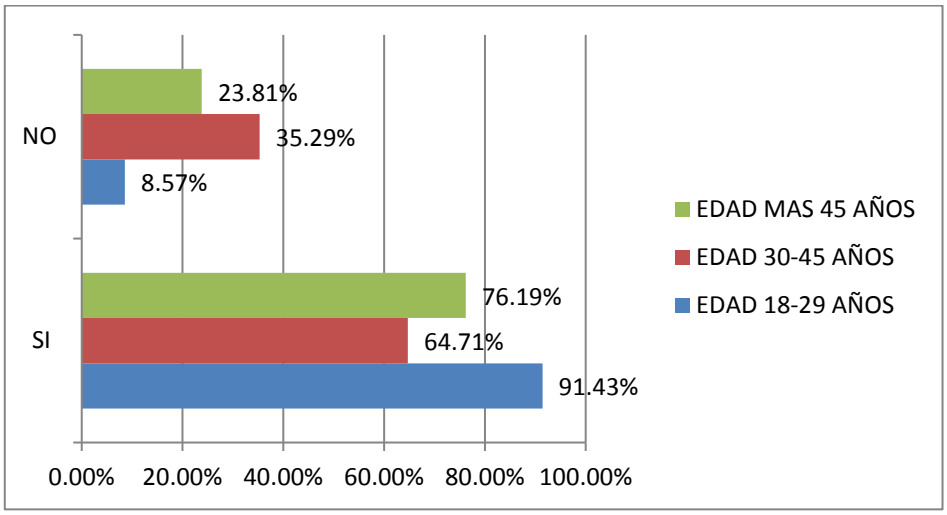


Gráfico 54: Respuestas al ítem 22 por edad encuestada, ¿cree que su derecho a la intimidad a veces se ve violado a través de la red?

Los resultados de la diferenciación por edad de los sujetos encuestados son parecidos a lo examinado hasta el momento. En el caso de los jóvenes encuestados, que se encuentran entre los 18 y los 29 años, el 91,43% han respondido que sí que la red a veces vulnera su derecho a la intimidad. El porcentaje que está inmediatamente debajo a éste es el de los individuos encuestados mayores de 45 años con un 76,19% de respuesta. Por último y según lo analizado hasta el momento era de esperar que el porcentaje menor fuera el los encuestados con edades comprendidas entre los 30 y los 45 años, y tal y como se ve representado en la gráfica eso es lo que ha ocurrido ya que el 64,71% de los individuos encuestados que se encuentran dentro de esa franja

de edad han respondido que sí que la red vulnera su derecho a la intimidad en determinadas ocasiones.

Para finalizar el análisis de los objetivos específicos acabaré por examinar el último de los propósitos que fijé al principio de mi estudio, éste es referente a la protección de datos personales, pero en él quiero ir más allá de simplemente saber si confían o no en Internet y paso a conocer si los encuestados creen necesaria una regulación del mismo en el ámbito de protección de dichos datos personales. En la encuesta también propongo que los sujetos libremente puedan expresar en qué ámbito regularían ellos el amparo de sus datos personales en la red.

Comenzaré por analizar a través de una gráfica qué porcentaje de encuestados creen necesaria una regulación y posteriormente mediante una tabla plasmaré los resultados de los sujetos que establecieron un ámbito para la realización de la misma:

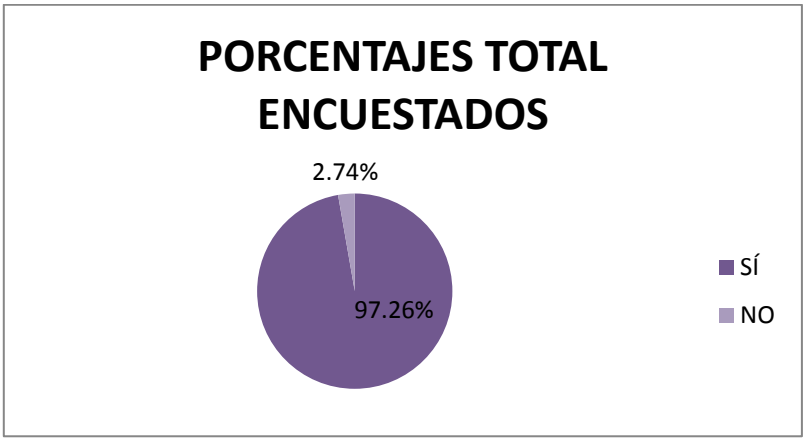


Gráfico 55: Respuestas al ítem 23, ¿cree necesaria una regulación de Internet en el ámbito de protección de datos personales?

Claramente se puede apreciar que casi la totalidad de los encuestados cree necesaria dicha regulación –el 97,26% de los sujetos encuestados-.

De la misma forma, haciendo la diferenciación por géneros, obtenemos un porcentaje altísimo tanto para las mujeres encuestadas como para los hombres encuestados -97,96% y 95,83% respectivamente-.

Todo ello se presenta en la siguiente gráfica:

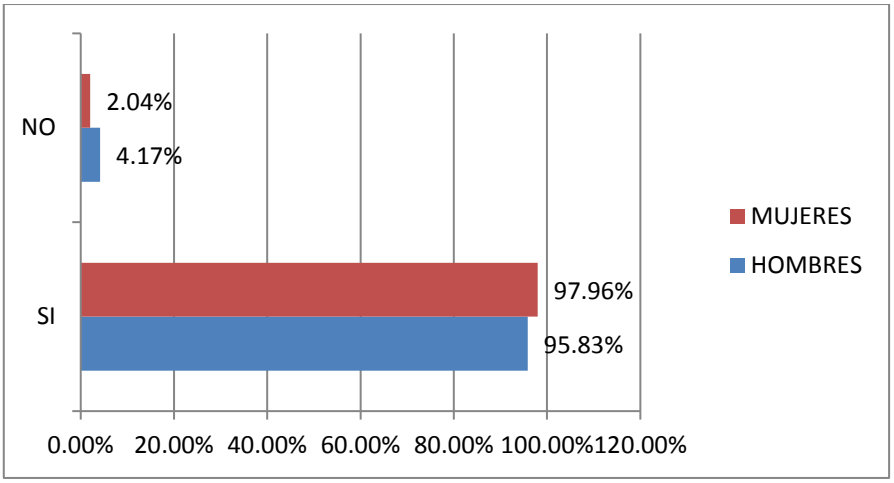


Gráfico 56: Respuestas al ítem 23 por género encuestado, ¿cree necesaria una regulación de Internet en el ámbito de protección de datos personales?

Asimismo haciendo la diferenciación por edad de los sujetos encuestados nos encontramos con que los porcentajes son muy altos al hecho de hacer una reforma con respecto a la protección de los datos personales a través en Internet, tal y como se ve reflejado en la siguiente gráfica:

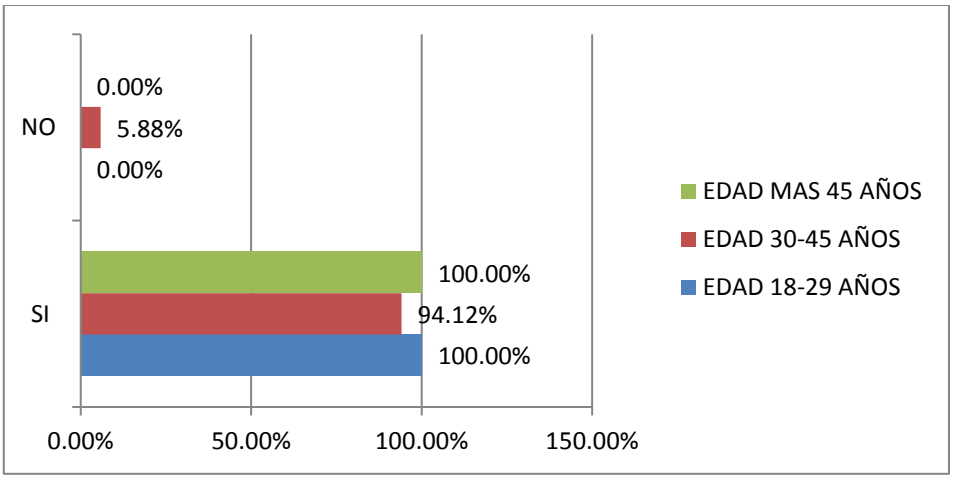


Gráfico 57: Respuestas al ítem 23 por edad encuestada, ¿cree necesaria una regulación de Internet en el ámbito de protección de datos personales?

El 100% tanto de los sujetos encuestados mayores de 45 años como de los jóvenes que tienen edades comprendidas entre 18 y 29 años han respondido con un sí al ítem. Solamente el 5,88% de los individuos encuestados que tienen edades que se incluyen dentro de la franja de edad de 30 a 45 años han contestado con un no al hecho de

realizar una reforma con el fin de modificar la protección de los datos personales en Internet, el resto -un 94,12%- marcaron un si como respuesta.

Por último, para finalizar este apartado y pasar al siguiente –que es el análisis del objetivo general del estudio-, quedan por analizar los ámbitos de regulación que los sujetos encuestados plasmaron como importantes para ellos, en los que se debería establecer un cambio en el ámbito de Internet.

Los resultados se encuentran plasmados en la siguiente tabla:

EN QUÉ AMBITO	MARCADOS
SECTOR SANITARIO	1
LLAMADAS PUBLICITARIAS NO SOLICITADAS	2
CORREOS COMERCIALES	2
A LA HORA DE CONTRATAR UN SERVICIO ONLINE	2
MAYOR PENALIZACION DE FRAUDES Y ESTAFAS	3
ELIMINAR PAGINAS WEBS ILEGALES	1
EN LAS REDES SOCIALES	**6**
TRANSFERENCIA DE DATOS PERSONALES	**9**
EVITAR EL USO DE MUCHOS DATOS PERSONALES	**4**
MÁS PRIVACIDAD EN LOS MENORES	**5**
FINES DEL USO DE LOS DATOS PERSONALES	**4**
CLAVES DE ACCESO PERSONALIZADAS	1
A LA HORA DE COMPRAR UN BIEN ONLINE	2
MAYOR IDENTIFICACION PARA OPERAR	1
CONTROL DE ACCESO A LOS DATOS	1
MÁS PROTECCION DE LA INTIMIDAD	3
SECTOR EMPRESARIAL	2
HACKERS	1
BUSQUEDA DE GOOGLE	1
DDFF Y DERECHO AL OLVIDO	1

Gráfico 58: Ámbitos de regulación de Internet en el sector de protección de datos personales.

Una vez analizada la misma vemos que la respuesta con más número de sujetos -9 encuestados- fue la de la regulación en el ámbito de limitación de datos personales, en los cuales los sujetos encuestados piden que las páginas web donde se necesiten datos personales tengan más seguridad para que se pueda restringir o limitar la transmisión de esos datos.

Seguido a esto encontramos que 6 encuestados piden la regulación en el ámbito de la redes sociales, más particularmente lo que los sujetos encuestados exigen es que se pueda mejorar la privacidad para el traspaso de datos de una red social a otra y se pueda restringir el uso de los mismos para realizar conductas ilícitas con ellos.

En tercer lugar 5 sujetos demandan que en el caso de los menores, se mejore su privatización en la red para proteger su derecho a la intimidad, es decir, lo que los encuestados revindican es que en el caso de los menores de edad, cuando utilizan la red, tengan más protección ya que por regla general no poseen la capacidad de obrar que tiene una persona adulta y por ende se exige que sea más dificultosa la vulneración de su derecho a la intimidad y de su derecho a la vida privada.

Por último dos ámbitos de regulación coinciden en el número de encuestados que los marcaron como importantes -4 sujetos-. Por un lado nos encontramos con la evitación del uso de muchos datos personales, en este espacio los individuos reclaman que para adquirir bienes online o para hacer cualquier transacción a través de la red no sea necesario plasmar muchos datos personales en la página concreta. Y por otro lado solicitan otro ámbito de regulación que tiene que ver también con los datos personales, en él se demanda que cuando una página concreta dentro de la red obliga a colocar los datos bancarios o personales en ella, se explique perfectamente cuáles son los fines principales en los que van a participar los mismos para de esta forma conocer su finalidad exacta.

Una vez finalizado este punto, en el apartado siguiente analizaré la resolución del objetivo general de mi estudio que era determinar el grado de percepción de inseguridad que los sujetos encuestados tienen en la red.

3.5 ANÁLISIS DEL OBJETIVO GENERAL DEL ESTUDIO

Tal y como acabo de mencionar mi objetivo general es conocer el grado de percepción de inseguridad que tienen los ciudadanos de Donostia-San Sebastián con respecto a Internet, pero como he determinado en la metodología del estudio los resultados no se pueden generalizar a toda la población de dicha ciudad, y por lo tanto, el producto de la investigación solo se puede globalizar a los sujetos

encuestados. Asimismo el propósito pasaría a ser delimitar el grado de percepción de inseguridad que tienen los sujetos encuestados –cuyo requisito fundamental es vivir en dicha ciudad- con respecto a la red. Y según todo lo analizado hasta el momento se puede determinar cuál es el grado de inseguridad que suscita Internet a los individuos.

Conforme a lo examinado en el estudio existe una percepción de inseguridad en los sujetos encuestados a la hora de utilizar la red para realizar compras de bienes o adquisiciones de servicios. Pero el grado de percepción de dicha inseguridad no es suficiente como para que los individuos encuestados no realicen la adquisición de dichos bienes o servicios a través de la red. En mi opinión creo que la existencia de una percepción de inseguridad en Internet es una emoción que va unida al hecho de utilizar la misma para múltiples acciones en nuestro día a día. Todo el mundo o casi todo el mundo conoce que a través del ciberespacio se cometen múltiples acciones ilegales y se mueven millones de datos bancarios y personales que pueden caer en manos de delincuentes que los utilicen para fines ilícitos, pero creo que ninguno o muy pocos de los sujetos que he encuestado en mi trabajo utilizan sus datos personales o sus datos bancarios sin ningún tipo de juicio en la red, sino que todos conocen las situaciones en las que esos datos personales pueden ser utilizados de manera ilegal y toman ciertas medidas de seguridad inconscientemente a la hora de adquirir bienes o servicios a través del ciberespacio –con esto me refiero al hecho de plasmar dichos datos en la red de una forma juiciosa, no en cualquier página o en cualquier enlace que se encuentren navegando por la red-.

3.6 CONCLUSIONES PRINCIPALES DEL TRABAJO DE CAMPO

Una vez realizados tanto el análisis de los objetivos específicos como del objetivo general de mi investigación puedo llegar a una serie de conclusiones complementarias con respecto a las diferenciaciones de la muestra por género y por edad:

La primera de ellas hace referencia a la diferenciación por género encuestado, primero desarrollaré la conclusión a la que he llegado y posteriormente matizaré un hecho que creo que es de gran importancia ya que de haberlo especificado desde el

principio de la investigación se podría haber modificado la conclusión que analizaré a continuación.

Esta conclusión es referente al hecho de que los hombres encuestados a lo largo de toda la encuesta han aparentado ser más irreflexivos cuando hablamos de utilizar la red para plasmar sus datos personales o bancarios que las mujeres encuestadas, ya que se han mostrado más abiertos a la hora de utilizar métodos de pago en los que es necesario plasmar datos bancarios o datos personales. Las mujeres encuestadas, en cambio, han aparentado ser más juiciosas y por ello piensan más a la hora de colocar sus datos en Internet y procuran no utilizar métodos de pago que exijan el reflejo de los mismos.

He podido sacar esta conclusión ya que en la realización de la encuesta no he incurrido en ningún tipo de factor que podría influir en los resultados. Entre estos factores se podrían encontrar, por ejemplo, en el hecho de que los hombres encuestados hayan aparentado ser más irreflexivos puede influir que la mayoría de ellos trabajen en un banco, o su familia, pareja o amigos lo hagan o tengan estudios relacionados con economía o empresas, etc. Por el contrario, en el caso de las mujeres encuestadas, el hecho de que hayan aparentado ser más juiciosas puede ser porque, aunque ellas no hayan sufrido ningún tipo de delito en relación con el robo de sus datos personales, pueden conocer a mucha gente que sí que lo haya sufrido y por ello son más reticentes a utilizar métodos de pago que les requieran el reflejo de sus datos personales.

La segunda y la última de las conclusiones hace referencia a la diferenciación de la muestra por edad, en este caso he de afirmar lo mismo que en la conclusión anterior y es que el hecho de haber evaluado algunos factores externos podría haber modificado los resultados del sondeo. Pero al no haber incurrido en ellos plasmaré la conclusión a la que he llegado con el análisis de los resultados existentes.

Antes de comenzar el análisis de los objetivos específicos de mi investigación pensaba que la franja de edad con menor percepción de inseguridad en la red correspondía a la franja más joven, pero a través del examen de los objetivos he podido llegar a la conclusión de que estaba equivocada. La franja de edad encuestada con menor percepción de inseguridad en Internet es la que va de 30 a 45 años,

seguida de los jóvenes encuestados de entre 18 y 29 años y por último se encuentran los sujetos encuestados mayores de 45 años.

A continuación determinaré unos planes de mejora que si tanto los individuos y las empresas como las plataformas del Gobierno los llevasen a cabo, cabe pensar que se podrían reducir las oportunidades de comisión de ciertos ciberdelitos relacionados con las estafas a través de compras online.

4. PLANES DE MEJORA

Los planes de mejora que voy a plasmar a continuación son una serie de acciones que, tal y como acabo de comentar anteriormente, si los usuarios que utilizan Internet, las empresas que ponen a disposición bienes o servicios a los individuos y la plataformas del Gobierno los llevasen a cabo, cabe pensar que las posibilidades de comisión de ciertos actos ilícitos en Internet se podrían ver reducidas. También es importante matizar que estos no son los únicos planes de mejora que existen para poder incrementar la seguridad de los usuarios en la red, pero son los que en mi opinión considero más significativos después de haber realizado un estudio muy exhaustivo del ciberespacio y más particularmente de las estafas que en él se pueden cometer.

En la sociedad en la que vivimos la mayoría de las personas compran por Internet y lo seguirán haciendo, siempre teniendo en cuenta el hecho de que se debe realizar con mucha precaución. Por ello creo que se deberían de recoger planes de mejora en los cuales se dé por hecho que las personas utilizan la tarjeta bancaria para adquirir bienes online y se ayude a utilizar dicha tarjeta de una forma correcta, sin poner en riesgo sus bienes o su dinero. En general lo que se debe fomentar en la sociedad es una educación basada en enseñar a navegar por Internet de una forma segura (Rayón y Gómez, 2014).

1. El primero de los planes de mejora es la educación a la ciudadanía en tres aspectos muy significativos que deberían ser el asentamiento para una posterior reducción de las posibilidades de comisión de ciertos ciberdelitos. Tal y como afirma Álvarez (2009): “la mejor inversión a largo plazo que puede hacerse en seguridad es concienciar, educar y formar a las personas en

esa materia. Solo así las soluciones tecnológicas como antivirus, cortafuegos, cifrado de archivos, etc., serán plenamente eficaces" (p.16).

1.1 Debe instruirse a los ciudadanos para poder diferenciar entre una página web legal y una página web ilegal. Actualmente el Phising y el Pharming son dos de las estafas informáticas que más se producen en nuestra sociedad (Fernández, 2006) y el hecho de ayudar a los sujetos a distinguir cuando se están plasmando los datos personales o los datos bancarios en una página real, o cuando lo están haciendo en una página creada para captar dichos datos, es clave para que no se confundan y su uso de la tarjeta sea más juicioso.

1.2 El segundo aspecto, con respecto a la ciudadanía, sería impulsar una forma de uso de la tarjeta sin que las consecuencias de su captación le hicieran al sujeto perder todo su dinero. Me estoy refiriendo al hecho de fomentar que las personas adquieran una segunda tarjeta bancaria –a poder ser de débito- solamente para adquirir bienes online. Esta es una forma clave y segura de utilizar dicho método de pago sin consecuencias extremadamente negativas –como puede ser el hecho de perder o todo su dinero o grandes cantidades del mismo-. Cuando el individuo quiera comprar cualquier bien online, solamente deberá ingresar el dinero justo para obtener dicho bien a la segunda tarjeta y de esta forma no se tendrá que preocupar de los posibles efectos negativos de la captación de la misma.

En lo referente al hecho de fomentar la seguridad en las tarjetas personales de crédito o de débito se ha propuesto un protocolo denominado SET (Secure Electronix Transaction), en el que las principales compañías bancarias de tarjetas de pago (Visa y Mastercard), están trabajando conjuntamente para poder aumentar la seguridad en Internet cuando se utiliza este método de pago para adquirir bienes o contratar servicios online (López, Mata y Bernal, 2010). Este protocolo ha sido creado para evitar las compras no autorizadas por los titulares de las tarjetas de crédito o de débito y para impedir el robo de los datos personales de los usuarios en las páginas de compra. La seguridad de los datos bancarios de los titulares de la tarjeta se fomenta a través de

contraseñas encriptadas y firmas electrónicas, para así poder otorgar a dicho usuario las seguridad necesaria para poder realizar sus compras sin ningún tipo de duda con respecto a la confianza a la hora de plasmar sus datos.

1.3 La tercera y última de las ideas con respecto a la educación de los usuarios en Internet hace referencia a las compras online. Me refiero al hecho de que a la hora de adquirir un bien online sería muy aconsejable que los usuarios buscaran opiniones de personas que, o bien ya han obtenido el mismo objeto o bien otro diferente, pero lo han hecho en la misma página donde el individuo quiere realizar la compra. Todo ello es recomendable para así tener más certeza de que la página donde se está llevando a cabo la adquisición es real y fiable. Este hecho se puede ver plasmado perfectamente en una noticia de elcorreo.com (2016) en la que *Trusted Shops* realiza una encuesta a sus consumidores que tiene como objetivo lo comentado anteriormente. Los resultados son sorprendentes ya que el 96,50% de los encuestados afirma que a la hora de realizar una compra online buscan comentarios de otros consumidores. Y de hecho les dan tanta importancia que el 58,70% realiza la compra si los comentarios son positivos y el 16% de los usuarios rechazan la adquisición cuando son negativos. Otro trabajo en el que se afirma que es muy importante revisar una segunda opinión antes de comprar un bien online es el de San José, Camarero y Rodríguez (2012) en el que se determina que: "aproximadamente tres de cada cuatro consumidores consultan las opiniones de otros individuos en distintos espacios online (sitios web, foros, blogs, redes sociales, etc.) antes de tomar decisiones de compra" (p.15).

2. Otro de los planes va dirigido a las empresas que ponen bienes a disposición de los usuarios, en ellas creo que se debería fomentar otro método de pago como método estrella como puede ser el sistema PayPal. Para efectuar pagos mediante dicho método el usuario se debe registrar previamente y en la página de adquisición de los bienes basta con colocar un correo electrónico y una contraseña que estará asociado a un número de cuenta. Una de las ventajas es que no hace falta plasmar los datos bancarios de los individuos en la misma página de compra por lo que cabe pensar que para los potenciales infractores será más dificultosa la labor de adquirir dichos datos. Según

Santomá (2004): “el éxito de este servicio se debe a que es totalmente gratuito para sus usuarios, fácil y cómodo, permite el anonimato en las transacciones y es el sistema de pago por Internet más seguro” (p.108). Este autor en su artículo también afirma que una de las acciones que más seguridad suscita a los individuos es que “PayPal se hace responsable de los costes ocasionados por el fraude con las tarjetas” (Santomá, 2004, p.108).

3. Las siguientes ideas de mejora son más difusas y difíciles de conseguir pero considero que es importante poder mencionarlas. Es primordial, respetando los principios fundamentales del Derecho penal, que todos los hechos delictivos cometidos en Internet tengan su castigo plasmado en el Código Penal. Como he comentado anteriormente la globalización de las TIC hace que la ley tenga que cambiar constantemente y que lo que hoy se sanciona, mañana se puede quedar anticuado y necesite un cambio en la legislación.

   Por lo tanto una de las formas de poder reducir las oportunidades de comisión de ciertos delitos online podría ser fomentar la informática para que ésta pueda fortalecer a las páginas legales y consecuentemente a ello, dificultar que sean hackeadas para extraer los datos de los usuarios. Esto tiene tal importancia en la actualidad que, como se extrae de diariosur.es (2016), Yahoo! sufrió un ciberataque masivo en el cual fueron atacados más de mil millones de usuarios. La noticia plasma que “entre la información robada habría nombres, direcciones de correo electrónico, números de teléfono, fechas de cumpleaños y, en algunos casos, preguntas de seguridad, encriptadas o sin encriptar; pero no se incluían datos de tarjetas de pago o contraseñas recompuestas”. Por lo tanto se expresa la idea de que es muy importante que se fortalezcan las páginas legales cada vez más para evitar que se produzcan este tipo de ataques que pueden afectar a millones de usuarios.

   Asimismo es primordial fomentar la idea de que a la vez que la legislación debe cambiar a medida que avanza la sociedad, la informática debería de hacerlo también al mismo tiempo para evitar que ese refuerzo de las páginas se quede obsoleto. De hecho es tan elevada la significación de esto que, tal y como afirma la principal responsable del antivirus Panda, “un antivirus es insuficiente ante la ciberdelincuencia”. Rosa Díaz, a través del periódico

diariosur.es (2016) afirma que la ciberdelincuencia está cada vez más perfeccionada y que debemos de avanzar con ella para poder erradicarla. A su vez también determina que "al igual que los criminales se unen para atacarnos, nos toca a nosotros unirnos y colaborar para hacer frente a la ciberdelincuencia, innovando y trabajando juntos". Según la principal responsable de dicho antivirus ésta sería la clave primordial para el futuro de la ciberseguridad en Internet.

Siguiendo esta misma línea también creo que sería importante poder eliminar todas las páginas web que tengan la posibilidad de ser ilegales para evitar así que cualquier persona pueda llegar a ellas y caer en el error de reflejar sus datos personales. Esta última idea es mucho más dificultosa que la anterior ya que en Internet hay millones de portales web y cada día se crean millones más, y por lo tanto poder llegar a cumplir este plan de mejora en su totalidad es una labor muy costosa y muy laboriosa.

4. El último de los planes de mejora que voy a exponer en mi trabajo no depende de los usuarios sino del Gobierno y ha sido expuesto por Soraya Sáenz de Santamaría en la Conferencia Anual de la Asociación de Editores de Diarios Españoles (AEDE). Tal y como aparece plasmado en diariovasco.com (2016), la vicepresidenta del Gobierno cree que "se debe crear una ley que proteja los derechos de los ciudadanos en Internet y con la que se puedan combatir amenazas". Además de esto Soraya advierte que es importante crear un Ministerio específico en el que se gestionen los datos masivos manejados en la red y con el que "los ciudadanos recuperen el control de su privacidad y de la seguridad de sus comunicaciones".

Finalmente quiero dejar claro que llevando a cabo la realización de todas estas ideas no se puede acabar con los ciberdelitos, ni mucho menos, pero creo que muchas de las oportunidades de que los infractores delincan se las damos nosotros mismos con nuestras acciones, y también entiendo que si tomáramos algunas precauciones previas se podrían reducir muchas de las posibilidades de comisión de ciertos ciberdelitos económicos. Pero los usuarios no son los únicos que deben tener todo el peso para combatir la ciberdelincuencia, sino que si los individuos tomaran dichas prevenciones, si todos los órganos, plataformas y cuerpos legislativos del Estado se

unieran para dar protección a dichos usuarios (Peñaloza y Morillo, 2010) y si los proveedores de los Servicios de Internet realizaran una vigilancia y un control más exhausto de los posibles riesgos que puede tener su servicio prestado y de las posibles acciones ilícitas que se están llevado a cabo en el mismo (Solano, 2012), se conseguiría crear una base ideal para reducir las posibilidades de comisión de ciertos ciberdelitos.

5. CONCLUSIONES FINALES DEL TRABAJO

El primer aspecto a mencionar a la hora de determinar las conclusiones principales de todo el trabajo es que Internet es el motor principal de nuestra sociedad (Castells, 2014) ya que ha modificado muchos de los aspectos de nuestra vida, entre los que se pueden encontrar las comunicaciones, la educación, la cultura, las empresas, los hábitos de consumo e incluso las relaciones afectivas.

A lo largo de todo este trabajo he podido determinar que el ciberespacio tiene una serie de características extrínsecas propias -tales como: deslocalización, transnacionalidad, no centralización, neutralidad, universalidad y popularización- que pueden fomentar que se cometan delitos a través de este nuevo medio, que es Internet (Miró, 2011). Si a todos estos caracteres se le suma el hecho de que en la red no se aprecia el espacio ni el tiempo de la misma manera que en el espacio físico, los ciberdelitos tienen más oportunidades de cometerse ya que es mucho más difícil detener al culpable de un delito online.

El papel que juega la víctima en los delitos cometidos a través de Internet es muy importante a la hora de facilitar ciertas oportunidades de comisión de los mismos, ya que es ella misma la que tiene que llevar a cabo ciertas conductas previas de autoprotección o ciertas medidas de seguridad –como pueden ser: presencia de antivirus, cambio de contraseñas temporalmente, uso juicioso de datos personales en Internet, tener cuidado con quién se comunica a través de la red, etc.-. Pero con todo esto no se quiere afirmar que la víctima es la única culpable de que se lleve a cabo un ciberdelito sobre ella, ni mucho menos, ya que gracias a todas las características de la red que he podido analizar a lo largo de todo mi trabajo, el infractor puede jugar con

la manipulación y con el engaño para poder conseguir información diversa de la víctima, y aunque ésta lleve a cabo conductas de autoprotección constantemente es susceptible de ser utilizada por un potencial infractor que vea en ella un objetivo adecuado del que quiere abusar. También es importante matizar que mucha de la responsabilidad de que los usuarios sufran las consecuencias de ser víctimas de un ciberdelito es de las empresas especializadas y de los bancos, que no tienen en consideración los cuidados que deberían tener para proteger la seguridad de sus usuarios. De esta forma la responsabilidad de los sujetos acaba donde empieza la de las empresas especializadas.

Los ciberdelitos económicos han aumentado en número en la sociedad en la que vivimos ya que la adquisición de bienes online, pagados con la tarjeta de crédito o de débito, se ha convertido en uno de los comportamientos más masivamente realizados por los usuarios de Internet. Por ello hay muchos individuos que ven la posibilidad de conseguir dinero de una forma rápida captando los datos personales de los sujetos que utilizan dicho método de pago para realizar sus compras a través de la red (San Juan, Vozmediano y Vergara, 2009).

Asimismo a lo largo de la realización de la encuesta llevada a cabo en Donostia-San Sebastián he llegado a varias conclusiones sobre los sujetos encuestados.

La primera de ellas hace referencia al objetivo general de la misma, éste era determinar el grado de inseguridad en la red que tienen los usuarios que han sido encuestados. Ahora bien, después del análisis de los resultados del sondeo, se puede afirmar que existe cierto grado de inseguridad en Internet en los ciudadanos de Donostia-San Sebastián encuestados, pero dicha inseguridad no es tan elevada como para que los sujetos encuestados no realicen actividades en las que se requiera el reflejo de los datos bancarios o de los datos personales. Creo que el grado de inseguridad que tienen estos sujetos encuestados va unido al uso que hacen de Internet, es decir, cuando un individuo utiliza la red tiene el conocimiento de que es un espacio donde existen muchos tipos de oportunidades de comisión de muchos tipos penales, por lo que inconscientemente cada sujeto lleva a cabo ciertas conductas de forma juiciosa.

A través de la división de la muestra por edad y por género, y sin valorar ningún tipo de factor más allá de esta diferenciación, he podido llegar a una serie de conclusiones.

Con respecto al género, los hombres encuestados tienen una percepción de inseguridad en la red menor que las mujeres encuestadas, ya que a lo largo de toda la encuesta han aparentado confiar más en Internet porque utilizan métodos de pago donde se requieren datos bancarios o personales para múltiples acciones. Sin embargo, las mujeres encuestadas han aparentado ser más reflexivas y se muestran más reticentes a utilizar la tarjeta de crédito o de débito para adquirir bienes o servicios a través de la red.

Con respecto a la edad, son los sujetos encuestados que se encuentran en la franja de 30 a 45 años quienes tienen una percepción de inseguridad en la red menor, seguidos de los jóvenes encuestados que se encuentran entre los 18 y los 29 años y por último la franja de edad con mayor percepción de inseguridad en Internet son los individuos encuestados mayores de 45 años.

Para finalizar el trabajo he de hacer hincapié en que el ciberdelito va avanzando a medida que avanza la sociedad y que es necesario que la ley y la informática evolucionen a la vez que las TIC para que ningún tipo de acción se quede anticuada con el paso de los años. Por todo ello también es necesaria una educación constante a la ciudadanía basada en ciberdelincuencia ya que según Álvarez (2009): “la mejor inversión a largo plazo que puede hacerse en seguridad es concienciar, educar y formar a las personas en esa materia. Solo así las soluciones tecnológicas como antivirus, cortafuegos, cifrado de archivos, etc., serán plenamente eficaces” (p.16).

6. RESUMEN EJECUTIVO

El presente trabajo está basado en un estudio sobre el ciberdelito, más particularmente, sobre las estafas producidas a través de la compra de bienes y de la contratación de servicios online. Actualmente a través del progreso que han sufrido las adquisiciones tanto de servicios como de bienes a través de la red, el delito económico online es una de las formas más comunes para poder adquirir dinero de usuarios, y de hecho cada vez hay más sujetos que llevan a cabo conductas ilícitas en Internet –como pueden ser: fraudes y estafas- para poder hacerse con el dinero de terceros (San Juan, Vozmediano y Vergara, 2009).

En este estudio se analiza el ciberespacio como medio que puede fomentar la realización de actos ilícitos, los ciberdelitos en general y los ciberdelitos económicos en particular. Asimismo también se examina una encuesta semiestructurada de percepción de inseguridad en Internet realizada en Donostia-San Sebastián durante la ejecución de las prácticas obligatorias de la Universidad en la Guardia Municipal, entre el 25 de enero y el 18 de marzo de 2016, y por lo tanto se entiende que la investigación se encuentra vinculada a dichas prácticas. Esta encuesta tiene como objetivo principal conocer el grado de inseguridad que tienen los sujetos encuestados a la hora de utilizar la red. En el sondeo también existen ciertos objetivos específicos que son:

- Conocer para qué tipo de acciones utilizan más los usuarios encuestados Internet.
- Si los sujetos encuestados saben diferenciar entre una página web legal y una ilegal –entendiendo como una página web ilegal cualquier portal creado única y exclusivamente para captar los datos bancarios de los usuarios y poder utilizarlos sin su consentimiento-.
- Qué problemas ven los usuarios encuestados al uso diario de la red.
- Si los sujetos encuestados creen que Internet es un entorno seguro para adquirir bienes y/o contratar servicios.
- Si los usuarios encuestados realizan las transferencias bancarias a través de la red o prefieren ir directamente al banco.
- Determinar qué métodos de pago son los más utilizados por los sujetos encuestados.

- Si estos usuarios encuestados confían en la protección de sus datos personales a través del ciberespacio.
- Si creen que por medio de la red a veces se ve vulnerado su derecho a la intimidad.
- Y por último si los sujetos encuestados creen necesaria una regulación de Internet en el ámbito de protección de sus datos personales.

Por lo tanto el trabajo se compone de dos partes fundamentales. La primera de ellas es un análisis bibliográfico en el cual se estudia el ciberespacio, los ciberdelitos en general y los ciberdelitos económicos en particular. Se comienza con el análisis del ciberespacio como un nuevo medio de comisión de actos ilícitos cuyas características, tanto extrínsecas como intrínsecas, pueden fomentar la comisión de ciertos ciberdelitos. También se estudia el papel de la víctima dentro de los ciberdelitos y algunos perfiles de posibles víctimas y victimarios en la red. Más tarde el trabajo se centra en el ciberdelito: por un lado se hace un breve examen sobre las posibles teorías explicativas del mismo y por otro lado se menciona la regulación, en el actual Código Penal, de los ciberdelitos después de la reforma producida en el año 2015[27]. Por último, como fuentes secundarias, en lo referente a las estafas online, se realiza el análisis de la estafa informática a través de varias encuestas realizadas por diversas entidades relativas a fraudes y delitos económicos a nivel mundial. La primera se efectuó en 72 países por Aranda y López (2011). La segunda de las encuestas analizadas en el marco teórico se llevó a cabo en 99 países por López, Muñoz y Aranda (2014). La última se efectuó en 115 países por López, Muñoz y Aranda (2016). En el marco teórico, todo ello se completa con la referencia a un estudio sobre ciberseguridad que se llevó a cabo en 3074 hogares españoles por Gómez y Urueña (2014). Debe destacarse la necesidad y oportunidad de incorporar en este tipo de encuestas el trabajo de los criminólogos, profesionales que pueden trabajar tanto en el ámbito público como privado, dada la versatilidad de sus funciones dirigidas finalmente a campañas y medidas de prevención segmentadas por grupos de vulnerabilidad.

[27] España. Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (Ley Orgánica 1/2015, 30 de marzo). Boletín oficial del Estado, nº 77, 2015, 31 marzo.

La segunda parte del presente trabajo se refiere al propio trabajo de campo mediante una encuesta semiestructurada de inseguridad en Internet. Se realizó a 73 ciudadanos de Donostia-San Sebastián. Al tener una muestra pequeña y un objetivo meramente exploratorio el estudio no es representativo de la población total de dicha ciudad, sino que los resultados solamente se pueden globalizar a los sujetos encuestados. La metodología de la encuesta es cuantitativa ya que se utiliza una técnica que busca operacionalizar o traducir realidades sociales en datos numéricos. Asimismo está formada por preguntas mayoritariamente cerradas, si bien no excluye algunas abiertas y semicerradas.

En cuanto a los resultados principales del trabajo, el primero se refiere a que las características propias que tiene Internet pueden fomentar la comisión de actos ilícitos. Asimismo la víctima juega un papel muy importante en el ciberdelito ya que es ella misma la que tiene que llevar a cabo ciertas conductas de autoprotección o medidas de seguridad para reducir las oportunidades de convertirse en el sujeto pasivo de un acto ilícito en Internet, más particularmente puede producirse el hecho de que ésta pierda grandes cantidades de dinero si no plasma de una forma juiciosa sus datos bancarios en el ciberespacio. En todo caso no se trata de culpabilizar a la víctima o hacer recaer en ella todas las medidas de prevención y protección. Debe considerarse la propia responsabilidad de las empresas que venden los productos y de las que diseñan y gestionan sus páginas web. En este sentido deben considerarse las características propias que tiene Internet, entre las que se encuentra el anonimato. Además el potencial infractor puede utilizar conductas de engaño y manipular a la víctima para conseguir de ella lo que desee, particularmente cuando ésta reúne condiciones de vulnerabilidad. También es importante mencionar que la responsabilidad de una posible víctima acaba donde empieza la de las empresas especializadas y por ello mucha responsabilidad de la comisión de un ciberdelito es o de las empresas que ponen a disposición bienes para que adquieran los usuarios o de los mismos bancos.

Otras de las conclusiones claves de la investigación hacen referencia al objetivo general de la encuesta. Los sujetos encuestados tienen cierto grado de percepción de inseguridad en la red, pero éste no es tan elevado como para que éstos no realicen acciones en Internet que requieran el reflejo de datos bancarios o datos personales. De hecho este grado de inseguridad puede estar relacionado con el uso de la red, ya

que cualquier sujeto conoce que en Internet se llevan a cabo actos ilícitos de múltiple índole, por ello cabe pensar que muchos de los usuarios encuestados realizan ciertas conductas de autoprotección de forma inconsciente y automática, para así fomentar la seguridad de sus datos personales en el ciberespacio. Por ejemplo, a la hora de realizar una compra de un bien a través de la red, los sujetos conocen la existencia de estafas cometidas dentro de este ámbito e inconscientemente procuran colocar sus datos bancarios en páginas que les dan cierta seguridad.

Por último, para finalizar el resumen ejecutivo de mi trabajo, es importante mencionar los agentes que pueden estar interesados en leerlo y los plasmaré en la siguiente tabla:

Asociaciones de usuarios de banca online	- ADICAE - FACUA
Asociaciones dedicadas a la protección de los usuarios de Internet	- AUI - ADDUC
Departamentos de consumo de las empresas	
Fuerzas y Cuerpos de Seguridad del Estado	
Asociaciones de internautas	- AI

Gráfico 59: Asociaciones interesadas en leer mi trabajo sobre percepción de inseguridad en Internet.

Concluiré mi trabajo con una frase que afirma Agustina (2014) en uno de sus artículos que resume de una forma clara y concisa la información que estoy intentando transmitir con mi trabajo, ésta es: “no hacer en el mundo virtual lo que no haría en el mundo real” (p.178).

7. BIBLIOGRAFÍA

Aboso, G.E. & Zapata, M.F. (2006). *Cibercriminalidad y Derecho Penal: la información y los sistemas informáticos como nuevo paradigma del Derecho Penal. Análisis doctrinario, jurisprudencial y derecho comparado sobre los denominados "delitos informáticos"*. Buenos Aires: B de F.

Agustina, J.R. (2014). Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización. *Cuadernos de política criminal, 3(114)*, 143-178.

Álvarez, G. (2009). *Cómo protegernos de los peligros de Internet.* Madrid: Los Libros de la Catarata.

Aranda, S. & López, J. (2011). *Encuesta mundial sobre fraude y delito económico 2011*. Madrid: pwc.

Arias, A.R. (2011). *Sociedad del conocimiento* (Máster de investigación). Universidad de León, León.

Catálogo de Publicaciones de la Administración General del Estado (2015). *Anuario estadístico del Ministerio del Interior*. Descargado de: http://www.interior.gob.es/

Castells, M. (2001). *La galaxia Internet.* Barcelona: Plaza & Janes.

Castells, M. (2014). El impacto de Internet en la sociedad: una perspectiva global. En *19 ensayos fundamentales sobre cómo Internet está cambiando nuestras vidas* (pp. 127-149). España: C@mbio.

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

De la Cuesta, J.L. & De la Mata, N.J. (2010). *Derecho Penal informático*. Cizur Menor: Cívitas.

De la Cuesta, J.L. & Pérez, A.I. (2010). *Ciberdelincuentes y cibervíctimas*. Pamplona: Cívitas.

De la Cuesta, J.L. & San Juan, C. (2010). La Cibercriminalidad: interés y necesidad de estudio. Percepción de seguridad e inseguridad. En *Derecho penal informático* (pp. 57-78). España: Cívitas.

Dentzel, Z. (2014). El impacto de Internet en la vida diaria. En *19 ensayos fundamentales sobre cómo Internet está cambiando nuestras vidas* (pp. 235-254). España: C@mbio.

Di Piero, C. (2013). El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. *Revista para el análisis del derecho, (3)*, 1-6.

Dubois, A. & Cortés, J.J. (2005). *Nuevas Tecnologías de Comunicación para el Desarrollo Humano.* País Vasco: Bantaba.

Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares (2016, 10 de febrero). En *Instituto Nacional de Estadística*. Descargado de: http://www.ine.es/welcome.shtml

Encuesta sobre hábitos de uso y seguridad de Internet de menores y jóvenes en España (2014, 15 de febrero). En *Ministerio del Interior*. Descargado de: http://www.interior.gob.es/es/web/interior/portada

Evans, D. (2011). *Internet de las cosas. Como la próxima evolución de Internet lo cambia todo.* Madrid: Cisco.

El delito económico continúa fuerte en 2016 (2016, 26 de febrero). *INESE*. Descargado de: https://www.inese.es/

Fernández, J. G. (2007). Respuesta penal frente a fraudes cometidos en Internet: estafa, estafa informática y los nudos de la Red. *Revista de Derecho Penal y Criminología, 2(19)*, 217-243.

Fernández, J. G. (2007). *Cibercrimen: los delitos cometidos a través de Internet –estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red*. España: Constitutio Criminalis Carolina.

Fernández, R. (2006). Jornada sobre riesgos penales de la Banca On-line. *Revista de Internet, derecho y política, (2),* 1-3.

Flores, I. (2015). Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia. *Revista Electrónica de Ciencia Penal y Criminología, 17(21),* 1-42.

Gómez, M. & Urueña, A. (2014). *Estudio sobre la ciberseguridad y confianza en los hogares españoles.* Madrid: ONTSI/INTECO.

González, J.J. (2007). Precisiones conceptuales y político-criminales sobre la intervención penal en Internet. En *Delito e informática: algunos aspectos* (pp. 13-41). Bilbao: Publicaciones Universidad de Deusto.

González, M. (2014). *Fraudes en Internet y estafa informática* (Máster universitario). Universidad de Oviedo: Oviedo.

Javato, A.M. (2008). Sobre: Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjetas y otros instrumentos de pago. *Revista electrónica de Ciencia Penal y Criminología, 10(5),* 1-9.

Los consumidores españoles buscan otras opiniones en red antes de comprar (2016, 13 diciembre). *El Correo.* Descargado de: http://www.elcorreo.com/

López, J.; Muñoz, A.L.; Aranda, S. (2014). *Encuesta sobre fraude y delito económico 2014: resultados en España.* Madrid: pwc.

López, J.; Muñoz, A.L.; Aranda, S. (2016). *Encuesta sobre fraude y delito económico 2016: resultados en España*. Madrid: pwc.

López, L.; Mata, F.; Bernal, E. (2010). *Medios de pago electrónico. Piedra angular en el desarrollo del comercio electrónico.* Jaén: Publicaciones Universidad de Jaén.

Mata y Martín, R. (2007). Delitos cometidos mediante sistemas informáticos (estafas, difusión de materiales pornográficos y ciberterrorismo). En *Delito e informática: algunos aspectos* (pp. 129-172). Bilbao: Publicaciones Universidad de Deusto.

Mateos, I. (2013). *Ciberdelincuencia. Desarrollo y persecución tecnológica* (Trabajo fin de Grado). Universidad Politécnica de Madrid, Madrid.

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, 13(7),* 1-55.

Miró, F. (2013a). La victimización por Cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio. *Revista Española de Investigación Criminológica, 5(11),* 1-35.

Miró, F. (2013b). Derecho penal, cyberbullying y otras formas de acoso (no sexual) en el ciberespacio. *Revista de Internet, derecho y política, (16),* 61-75.

Morón, E. (2007). Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos. En *Delito e informática: algunos aspectos* (pp. 85-128). Bilbao: Publicaciones Universidad de Deusto.

Montiel, I. (2016). Cibercriminalidad social juvenil: la cifra negra. *Revista de Internet, derecho y política, (22),* 119-131.

Para la directora general de Panda, "un antivirus es insuficiente ante la ciberdelincuencia" (2016, 13 diciembre). *Diario Sur.* Descargado de: http://www.diariosur.es/

Peñaloza, M.C. & Morillo, M.C. (2010). El sector servicios y los delitos informáticos. *Visión Gerencial, (2),* 308-390.

Rayón, M.C. & Gómez, J.A. (2014). Cibercrimen: particularidad en su investigación y enjuiciamiento. *Anuario Jurídico y Económico Escurialense, (47),* 209-244.

Sánchez, J. (2009). *El bien jurídico protegido en el delito de estafa informática*. Salamanca: Cuadernos del Tomás.

San José, R.; Camarero, C.; Rodríguez, J. (2012). En busca de los evangelizadores digitales: por qué las empresas deben identificar y cuidar a los usuarios más activos de los espacios de opiniones online. *Universia Business Review, (8),* 14-31.

San Juan, C.; Vozmediano, L.; Vergara, A. (2009). Miedo al delito en contextos digitales: un estudio con población urbana. *Eguzkilore, (23),* 175-190.

Santomá, J. (2004). Nuevos medios de pago electrónicos: hacia la desintermediación bancaria. *Informacion comercial española, ICE: Revista de economía, 8(13),* 101-114.

Serrano, A. & Vázquez, C. (2007). *Tendencias de la criminalidad y percepción social de la inseguridad ciudadana en España y en la Unión Europea.* Madrid: Edisofer.

Solano, M.S. (2012). El crimen on-line. Una mirada a la responsabilidad del proveedor de servicio de Internet. *Justicia juris, 8(1),* 75-83.

Soraya Sáenz de Santamaría aboga por regular "en frio" la seguridad de los cibernautas (2016, 13 diciembre). *Diario Vasco.* Descargado de: http://www.diariovasco.com/

Summers, L. (2009). Las técnicas de prevención situacional del delito aplicadas a la delincuencia juvenil. *Revista de Derecho penal y Criminología, 3(1),* 395-409.

Tamarit, J.M. (2016). Ciberdelincuencia y cibervictimización. *Revista de Internet, derecho y política, (22),* 30-31.

Vozmediano, L. & San Juan, C. (2010). *Criminología Ambiental: ecología del delito y de la seguridad.* Barcelona: UOC.

Vozmediano, L.; San Juan, C.; Vergara, A.L. (2008). Problemas de medición del miedo al delito: algunas respuestas teóricas y técnicas. *Revista electrónica de Ciencia penal y Criminología, 10(7),* 1-17.

Wall, D. (2007). *Cybercrime: the transformation of crime in the information age*. Cambridge: Polity Press.

Yahoo! descubre un ciberataque contra mil millones de usuarios más (2016, 15 diciembre). *Diario Sur.* Descargado de: http://www.diariosur.es/

eman ta zabal zazu

Universidad del País Vasco
Euskal Herriko Unibertsitatea

ENCUESTA DE VICTIMIZACIÓN OCULTA E INSEGURIDAD CIUDADANA

Edad:
Género:
Barrio o zona residencial:
Tiempo de residencia en el barrio:

1. ¿Ha sido usted víctima de algún tipo de delito a lo largo de su vida?

Si		¿El autor del delito era una persona conocida o desconocida? --> **Pasar a pregunta 2**	**Conocida:**	**Desconocida:**
No		Y, ¿alguien de su entorno? En caso de NO --> **Pasar a pregunta 5**	**Si:**	**No:**

2. En caso de haber sufrido algún delito, ¿de qué tipo se trata? (pueden ser uno o varios)

Hurto	
Hurto documentación-cartera-bolso	
Robo con violencia o intimidación	
Agresión sexual	
Abuso sexual	
Estafa informática	
Otros (mencionar):	
NS/NC	

3. ¿Ha sido denunciado el delito?

Si	
No	

¿Dónde?

Guardia Municipal	
Ertzaina	
Otros	

--- En caso de haberlo denunciado en la Guardia Municipal, ¿que opinión le merece la atención recibida?

Muy mala	Mala	Regular	Buena	Muy buena

--- En caso de NO haberlo denunciado, ¿por qué no lo ha denunciado?

Por miedo al agresor/autor	
Por vergüenza	
Delito de poca importancia	
La policía no hubiese hecho nada para solucionarlo	
El agresor/autor era un familiar o amigo	
No sé cómo denunciar	
El problema se solucionó	
Otros (mencionar):	

4. En caso de no haberlo denunciado, ¿qué le hubiese ayudado o empujado a hacerlo?

Apoyo familiar	
Apoyo social	
Apoyo de instituciones públicas: policía, sistema judicial u otras entidades públicas	
Otros (mencionar):	

5. En una escala de 1 al 5 (donde 1 significa poco seguro y 5 muy seguro) ¿Qué nota le pondría a la seguridad en los siguientes lugares?

Lugares	1	2	3	4	5
Amara					
Gros					
Paseo de la Concha					
Pasadizo de Egia					
Parte Vieja					
Centro					
Zona de Intxaurrondo					

6. ¿En que medida le generan preocupación social los siguientes delitos en una escala del 1 al 5 (donde 1 significa nada y 5 mucho)?

Delitos	1	2	3	4	5
Hurto					
Robo					
Agresión sexual					
Abuso sexual					
Corrupción					
Otros (mencionar):					

7. ¿Evita usted alguna zona o calle para no ser víctima de un delito?

Si	
No	

¿Podría mencionar la zona o calle indicando el horario que le sugiere mayor preocupación?

Mencionar zona o calle:.....

De 0-4 h	
De 4-8 h	
De 8-12 h	
De 12-16 h	
De 16-20 h	
De 20-24 h	

9. Pensando en su barrio: en una escala del 1 al 5 (donde 1 significa poco seguro y 5 muy seguro) ¿Qué nota le pondría a la seguridad?

1	**2**	**3**	**4**	**5**

10. ¿Qué nivel de seguridad en una escala del 1 al 5 (donde 1 significa poco seguro y 5 muy seguro) sentiría en los siguientes lugares cuando ya está oscuro?

Caminando solo/a por su barrio	
Caminando acompañado/a por su barrio	
Caminando solo/a por el centro	
Caminando acompañado/a por el centro	
Esperando el transporte público	

11. ¿Tomó algún tipo de medida para evitar las zonas referidas anteriormente?

Si	
No	

¿Podría indicarlas?.....

12. ¿Con todas las reformas que se han realizado, considera usted que la zona del pasadizo de Egia es segura?

Si	
No	

¿Qué nivel de seguridad le daría en una escala del 1 al 5 (donde 1 significa poco seguro y 5 muy seguro)?

1	2	3	4	5

13. ¿Se siente usted más seguro en las zonas donde hay instaladas cámaras de seguridad?

Si	
No	

14. ¿Está de acuerdo con el uso de cámaras de vídeo vigilancia en espacios públicos?

Si	
No	

15. ¿Utiliza Internet? Si es que si, dígame para cuál de estos ámbitos lo utiliza (pueden ser uno o varios):

Información sobre actualidad	
Compras	
Entretenimiento	
Intercambio de archivos	
Participación en chats y foros	
Intercambio de comunicación	
Contratación de servicios	
Uso de datos bancarios	

16. ¿Sabría distinguir entre una página web legal y una página web ilegal? (Entendiendo como página web ilegal una página que, aparentemente, parece real pero que solamente se utiliza para captar datos bancarios de los usuarios para luego poder utilizarlos sin el consentimiento del dueño):

Si	
No	

17. ¿Qué problemas principales ve al uso diario de Internet? (pueden ser uno o varios):

Velocidad	
Seguridad	
Coste	
Calidad del acceso	
Falta de confidencialidad	
Demasiada publicidad	
Infección por virus	
Otros (mencionar):	

18. En una escala del 1 al 5, donde 1 es poco seguro y 5 es muy seguro, ¿cree que Internet es un entorno seguro para realizar compras o contratar servicios?:

1	2	3	4	5

19. Centrándonos en las transferencias bancarias, a la hora de llevar a cabo una transacción, ¿qué método utiliza usted, el método online o prefiere acudir directamente al banco?

Método online	
Banco	

¿Por qué?

.....

20. Imagínese que está realizando una compra online en este momento, ¿qué método de pago utilizaría?:

Tarjeta de crédito o débito	
Contra reembolso	
Domiciliación bancaria	
Transferencia	
A través del teléfono móvil	
Paypal y similares	
Otros (mencionar):	

21. En una escala del 1 al 5, ¿confía usted en la protección de datos en Internet?

1	2	3	4	5

22. ¿Cree que su derecho a la intimidad a veces se ve violado a través de la Red?

Si	
No	

23. Por último, ¿cree necesaria una regulación de Internet en el ámbito de protección de datos personales?

Si	
No	

Si la respuesta es afirmativa, ¿de qué tipo?.....

¡GRACIAS POR SU COLABORACIÓN!