CURSO 2020-2021
Convocatoria de julio de 2021

Trabajo Fin de Máster

COVID 19 Y CIBERCRIMEN

Máster Universitario en Análisis y Prevención del Crimen

Autor: Omar Abdul-Bar Méndez

Tutor: Steven Kemp

CRIMINA

UNIVERSITAS
Miguel Hernández

RESÚMEN

El aumento del uso de Internet y todas las nuevas tecnologías asociadas a éste han aumentado de manera exponencial anualmente, como se verá en éste trabajo. Tras la llegada de la pandemia propiciada por la Covid 19 cambió el mundo, obligándonos a quedarnos en nuestros hogares con el fin de controlar los contagios. Esto hizo que aumentara el consumo de Internet, y que con la histeria colectiva y el miedo, las estafas con la venta de material de protección fueran un gran campo de actuación de los cibercriminales. Durante el presente trabajo se analizan las denuncias recogidas en el ámbito de la Guardia Civil durante los años 2017 a 2020, con el fin de esclarecer si ha habido un aumento de los ciberdelitos a raíz de la pandemia. Para ello con los datos anonimizados, se realiza un estudio comparativo con el fin de verificar si es cierto.

ABSTRACT

The increase in the use of the Internet and all the new technologies associated with it has increased exponentially on an annual basis, as will be seen in this paper. After the arrival of the pandemic caused by Covid 19, the world changed, forcing us to stay in our homes in order to control contagion. This led to an increase in Internet consumption, and with the collective hysteria and fear, scams involving the sale of protection material became a major field of action for cybercriminals. This paper analyses the reports collected by the Guardia Civil from 2017 to 2020, in order to clarify whether there has been an increase in cybercrime as a result of the pandemic. To do this, a comparative study is carried out with anonymised data in order to verify whether this is true.

PALABRAS CLAVE

Cibercrimen, ciberseguridad, actividades rutinarias, oportunidad delictiva, Covid19.

KEYWORDS

Cybercrime, cybersecurity, routine activities, criminal opportunity, Covid19.

ÍNDICE

1.- INTRODUCCIÓN

Pocas personas del mundo iban a pensar que a partir del primer trimestre del año 2020, el mundo tal y como lo conocíamos iba a cambiar de una manera tan sustancial que crearía un nuevo panorama tanto social como económico[1]. Todo ello provocado por el virus conocido SARS-CoV 19, comúnmente conocido como COVID-19.

La rápida propagación del virus a nivel mundial gracias a la globalización en la que nos encontramos, hizo que de una manera exponencial, llegara a todos los países del mundo, infectando a millones personas, matando a un número muy elevado de personas, colapsando los sistemas sanitarios mundiales y creando una situación de pandemia con una grave emergencia sanitaria.

Este virus, con una mortalidad superior a la gripe común[2], su alta facilidad de propagación y contagio, está haciendo que en el momento de la confección del trabajo, más de 2,58 millones de personas en todo el mundo han fallecido en el mundo, si bien en el momento de la lectura la cifra haya aumentado.

Esta crisis sanitaria, como es lógico, ha tenido una serie de consecuencias, siendo la principal una grave emergencia económica, ya que las medidas restrictivas que se han implementado para evitar la propagación del virus, han hecho que tuvieran un cierre inmediato de todo negocio a excepción de los servicios esenciales.

En el caso concreto de España, el gobierno planificó una desescalada por provincias con una serie de fases muy diferentes según el nivel de contagios por cada 100.000 habitantes publicadas en el Real Decreto-ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19.

---

[2] Xu, Z., Shi, L., Wang, Y., Zhang, J., Huang, L., Zhang, C., ... & Wang, F. S. (2020). Pathological findings of COVID-19 associated with acute respiratory distress syndrome. *The Lancet respiratory medicine*, *8*(4), 420-422.

Esto ha derivado en una gran crisis económica[3], así como por una serie de hechos como fue el confinamiento extremo que nos vimos inmersos en España, en el que se suprimió la libertad de circulación por la vía pública, de todos los ciudadanos en el territorio nacional. Esto ha afectado en una manera muy clara en nuestras actividades rutinarias y cotidianas, ya que las personas no circulaban por la calle, los negocios estaban cerrados, los vehículos no circulaban por las calles, etc. Esto ha afectado en las cifras de reducciones de los fallecimientos por accidentes de tráfico[4], o los delitos relacionados con el patrimonio[5], cosa que es obvia, debido a que no se podía circular libremente por las calles y vías del territorio.

Todo ello, en palabras de Stickle y Felson, (2020) "nos encontramos ante el mayor experimento de criminología de la historia" ya que nuestras actividades cotidianas como se ha explicado con anterioridad, han cambiado de manera tan sustancial que como no podía ser menos, el crimen ha tenido un desplazamiento ya que la oportunidad del delito cambió. En este caso, probablemente se ha visto readaptado al ciberdelito[6], en el que aprovechando el miedo creado por la pandemia, el aumento del teletrabajo y el consumo de Internet en los hogares, propició que aumentara esa tipología criminal tal y como se reflejan en diferentes informes, tanto a nivel nacional[7] como internacional[8].

---

[3] Felgueroso, F., de la Fuente, A., Boscá, J. E., Doménech, R., Ferri, J., García Pérez, J. I., ... & Viola, A. (2020). Aspectos económicos de la crisis del Covid-19. *Boletín de seguimiento*, *3*.

[4] DGT (2021) Los accidentes de tráfico se cobran la vida de 870 personas durante el año pasado. Recuperado de la Dirección General de Tráfico de España el 22 de mayo de 2021 de https://www.dgt.es/es/prensa/notas-de-prensa/2021/Los_accidentes_de_trafico_se_cobran_la_vida_de_870_personas_durante_el_ano_pasado.shtml

[5] Portal estadístico de la Criminalidad de la Secretaría de Estado de Seguridad del Ministerio del Interior de España. https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/portal/datos.html?type=pcaxis&path=/Datos1/&file=pcaxis

[6] Llinares, F. M. (2021). Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos. *IDP: revista d'Internet, dret i política*, (32).

[7] Las estafas por Internet aumentan un 70% durante la pandemia. Ortega P. (2020) El País. Recuperado el 29 de marzo de 2021 de https://elpais.com/espana/2020-04-19/las-estafas-por-internet-aumentan-un-70-durante-la-cuarentena.html

[8] Interpol (2020) Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19. Recuperado de Interpol el 29 de marzo de 2021 de

Para tratar de aclarar qué es un **ciberdelito** según la RAE, se trata de un "*delito informático"* (Real Academia Española, 2020, definición 1), significando que se trata de una "*infracción penal cometida utilizando un medio o instrumento informático*" (Real Academia Española, 2020, definición 1). Por otro lado Consejo Nacional de Política Económica y Social (CONPES) del Gobierno de Colombia según cita[9] al Ministerio del Gobierno de ese mismo país, el ciberdelito se trata de una "*Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito*."

Hoy en día el uso de la informática está muy extendida y no hay que reducirla a un simple ordenador personal o portátil, ya que nuestros teléfonos móviles inteligente, tabletas o incluso televisiones, son una serie de sistemas o medios informáticos, que generalmente se encuentran conectados a algún tipo de Intranet o Internet, con el fin de tener una serie de prestaciones. Hoy en día imaginar un mundo sin Internet, quizás sería muy difícil, ya que nos ha unido de gran manera y ha agilizado el trabajo y soluciones diarias, de una manera muy exponencial.

1.1 El cibercrimen en Europa

La Unión Europea (UE), dentro de sus políticas preventivas contra el crimen, tiene el organismo denominado Europol, cuya cuartel general se encuentra en La Haya.

https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

[9] Posada Maya, R. (2017). The cybercrime and its efects in the theory of typicity: from a physical reality to a virtual reality. *Nuevo Foro Penal*, *13*(88), 72-112.

Esta Agencia de la Unión Europea para la Cooperación Policial (Europol), entre otras misiones trata de velar por el cumplimiento de la Ley en la UE. Tal y como reza en su página web[10], las labores que realizan son:

- *apoyo sobre el terreno a las operaciones de las fuerzas y cuerpos de seguridad*
- *central de intercambio de información sobre actividades delictivas*
- *centro de conocimientos especializados en materia de aplicación de la ley.*

Esta organización europea cuenta dentro de estas labores con una serie de prioridades respecto al crimen y tipologías delictivas, llamado Organised Crime Threat Assessment (SOCTA)[11].

Entre ellas, se encuentra la prioridad del cibercrimen, organizada dentro del Internet Organised Crime Threat Assessment (IOCTA)[12] comandada por el European Cybercrime Centre (EC3)[13] de Europol.

Dentro de este IOCTA se encuentran una serie de prioridades de ciclo político llamadas Empact, comprendiendo el ciclo político actual entre los años 2017 a 2021. Se tratan de periodos de cuatro años, donde se analizan y se establecen una serie de prioridades en cuanto a qué tipos de delitos a investigar son los principales. El cibercrimen sin duda se trata de una de ellas, tal y como se plasma en la web[14] de la UE:

[10] Agencia de la Unión Europea para la Cooperación Policial (Europol). Recuperado de la UE el 3 de junio de 2021 de https://europa.eu/european-union/about-eu/agencies/europol_es

[11] Serious and Organised Crime Threat Assessment (SOCTA). Recuperado de la UE el día 3 de junio de 2021 de https://www.europol.europa.eu/socta-report#fndtn-tabs-0-bottom-1

[12] Internet Organised Crime Threat Assessment (IOCTA) Recuperado de la UE el día 3 de junio de 2021 de https://www.europol.europa.eu/iocta-report

[13] European Cybercrime Centre (EC3) Recuperado de la UE el día 3 de junio de 2021 de https://www.europol.europa.eu/iocta-report

[14] EU Policy Cycle - EMPACT. Recuperado de la UE el día 3 de junio de 2021 de https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact

"To fight cybercrime, by disrupting the criminal activities related to attacks against information systems, particularly those following a Crime-as-a-Service business model and working as enablers for online crime, by combating child sexual abuse and child sexual exploitation, including the production and dissemination of child abuse material, and by targeting criminals involved in fraud and counterfeiting of non-cash means of payment, including large-scale payment card fraud (especially card-not-present fraud), emerging threats to other non-cash means of payment and enabling criminal activities."

Para comprender mejor las prioridades dentro del IOCTA, en cuanto a las tipologías establecidas en el EMPACT de los años 2017 a 2021 son las siguientes:

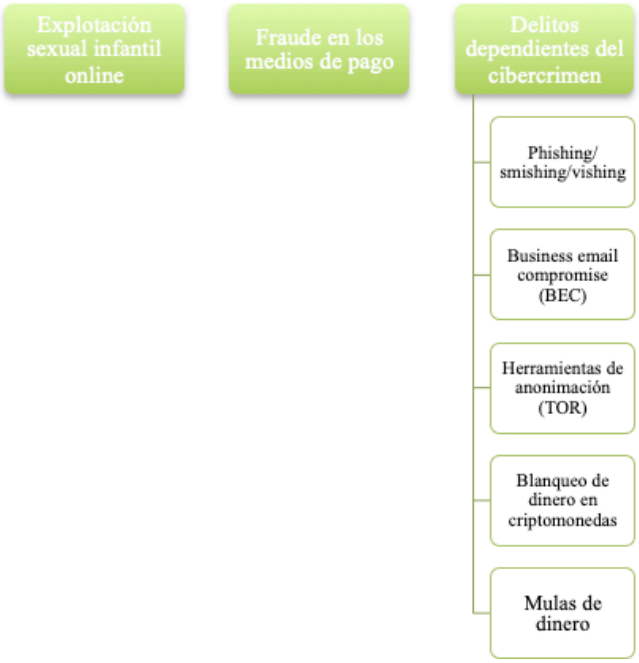


Imagen 2. Prioridades EMPACT 2017-2021. Diseño propio.

Queda patente que para la UE, el cibercrimen se trata de una realidad y una de las principales prioridades tal y como se ha podido demostrar.

1.2 El cibercrimen internacionalmente y sus definiciones.

En lo que respecta a la Organización Internacional de Policía (INTERPOL) de la que España forma parte, desde los inicios de la pandemia, se ha tomado muy en

serio los riesgos relacionados con el cibercrimen y la Covid19, notando ese riesgo real de aumento de ataques. Para ello han creado un sitio web[15] relacionado con los ciber-riesgos relacionados con la Covid19. Dentro de esto clasifican los ciberataques de la siguiente manera en su página web:

Dominios maliciosos

En Internet se ha registrado un número nada desdeñable de dominios que contienen los términos "coronavirus", "corona-virus", "covid19" y "covid-19". Aunque en algunos casos esos sitios web son legales, los ciberdelincuentes crean miles de sitios web nuevos cada día para llevar a cabo campañas de correos no deseados (spam) o ataques de phishing, o para propagar malware.

Malware.

Los ciberdelincuentes están aprovechando la gran cantidad de comunicaciones mundiales que ha despertado el coronavirus para esconder en ellas sus actividades. En los sitios web y mapas interactivos sobre el coronavirus se han encontrado integrados malware, spyware y troyanos. Asimismo, los usuarios reciben correos no deseados en los que se les intenta engañar para que pulsen en enlaces que activan la descarga de malware en sus ordenadores o dispositivos móviles.

Ransomware

Los ciberdelincuentes están lanzando ataques de ransomware contra hospitales, centros médicos e instituciones públicas, porque creen que, al estar estos saturados por la crisis sanitaria, no pueden quedarse sin acceso a sus sistemas y, por tanto, es más probable que accedan a pagar el rescate exigido. El ransomware puede penetrar en los sistemas por medio de correos electrónicos con enlaces o archivos adjuntos infectados, pirateando los datos de acceso de los empleados, o aprovechando una vulnerabilidad del sistema."

[15] Cyberthreats are constantly evolving in order to take advantage of online behaviour and trends. The COVID-19 outbreak is no exception. Recuperado de INTERPOL el día 3 de junio de 2021 de https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats

Este organismo internacional de policía, cuenta dentro de su organigrama, con un departamento de cibercrimen, ubicado en Singapur. Dentro de sus prioridades de investigación se encuentra el cibercrimen, por lo que vemos de la realidad importante de esta modalidad delictiva que va en aumento.

Según datos de la Unión Internacional de Telecomunicaciones[16], Internet es usado por el 48,997% de toda la población mundial (datos del año 2017). Cifra elevada si contamos con ciertas regiones en vías de desarrollo donde es complicado tener servicios esenciales y disponen de conexión a Internet.

Es importante constatar que la cifra de usuarios de Internet va en aumento casi exponencial tal y como se muestra en la siguiente gráfica.

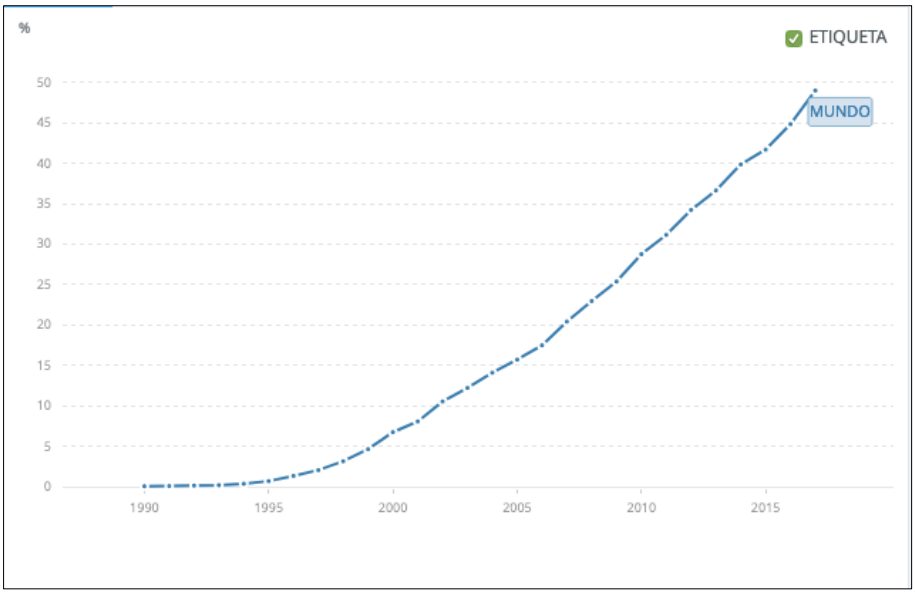


Imagen 1. Gráfico por porcentaje de usuarios de Internet a nivel mundial (Banco Mundial 2021)

[16] Personas que usan Internet (% de la población) Recuperado del Banco Mundial el 3 de junio de 2021 de https://datos.bancomundial.org/indicator/IT.NET.USER.ZS

1.3 Perspectiva del cibercrimen en España

Con el fin de tratar de contrastar los diferentes informes[17] relacionados con el aumento alarmante de esos ciberdelitos comprendidos entre los años 2017 al 2020, se va a tratar de verificar si el mismo ha sido real a través de un análisis exhaustivo de los datos anonimizados facilitados por las denuncias presentadas en el ámbito de Guardia Civil, que son a las que se ha podido tener acceso. Tras realizar una serie de depuración de datos, en los que se han obtenido una serie de datos anónimos, únicamente contando con las variables que posteriormente se van a plasmar, se va a tratar de realizar una serie de análisis estadísticos, así como posibles propuestas de mejora para tratar de prevenir los delitos cometidos a través de las TIC,s.

Es de interés recalcar que el presente estudio tiene por objeto el análisis de los delitos cometidos contra el orden socioeconómico y patrimonio (estafa o daños entre otros) y no los cometidos contra las personas, como son el acoso, amenazas o contra la libertad sexual desde el inicio de la pandemia del Covid 19 (desde marzo de 2020).

Pese a que se usen las TIC,s en ambos casos, las tipologías son muy diferentes, y es por ello que se realiza este apunte.

[17] Informe Europol sobre Covid 19 y Ciberdelitos de 19-06-2020 (Restringido). Informe BKA sobre Covid 19 y Ciberdelincuencia de enero de 2021 (Restringido).

2.- MARCO TEÓRICO

Como se ha propuesto en el anterior apartado, nos encontramos que debido al virus Covid19, el mundo ha cambiado radicalmente. Pero ¿qué cambios son los que han habido para que se consideren de tal magnitud?

Uno de los principales cambios habidos, ha sido la libertad de movimiento. Hemos estado sometidos a éste o incluso hay países, que en el momento de la confección del presente trabajo, se encuentran con un confinamiento domiciliario o cierre de fronteras, como es el caso de nuestro país vecino francés[18] o el portugués[19].

Hay que recordar esa fecha del viernes 13 de marzo de 2020, el Gobierno de la Nación Española, dada la gravedad por las fallecidos y contagiados del virus, decretó un confinamiento domiciliario de todos los ciudadanos, así como el cierre de todos los establecimientos y servicios no esenciales. Es decir, que se prohibía la libertad circulatoria a todos los ciudadanos, salvo caso justificado. Esto hizo que pudiéramos tener unas imágenes tan desoladoras como ver el centro de Madrid, sin personas circulando por la calle y las pocas que se veían, con una actitud de miedo.

Este miedo, es otra de las variables de la ecuación, ya que en ese momento, en el que el Gobierno y que ante la falta de previsión ante el virus, hizo que no hubiera mascarillas y gafas de protección para el personal sanitario y mucho menos para los ciudadanos. Así como la falta de un elemento esencial para prevenir la propagación del virus, como eran los geles hidro-alcohólicos. Y para culminar, la

[18] EFE (2021) Emmanuel Macron pone a toda Francia en confinamiento durante un mes y cerrará las escuelas al menos tres semanas. Recuperado del El Periodico el 09 de abril de 2021 de https://www.elperiodicoextremadura.com/internacional/2021/04/08/macron-pone-francia-confinamiento-46170818.html

[19] Chacón F. (2021) Se amplía el cierre de la frontera entre Portugal y España hasta el 19 de abril. Recuperado de ABC el 09 de abril de 2021 de https://www.abc.es/sociedad/abci-amplia-cierre-frontera-entre-portugal-y-espana-hasta-19-abril-202104021818_noticia.html

falta de respiradores para los enfermos críticos hizo que ese miedo fuera superior en la sociedad.

2.1 Clasificación de los ciberataques.

Siguiendo a Miró (2012)[20] es importante realizar una clasificación de los tipos de cibercrimen que podemos encontrarnos para ello realiza las siguientes clasificaciones:

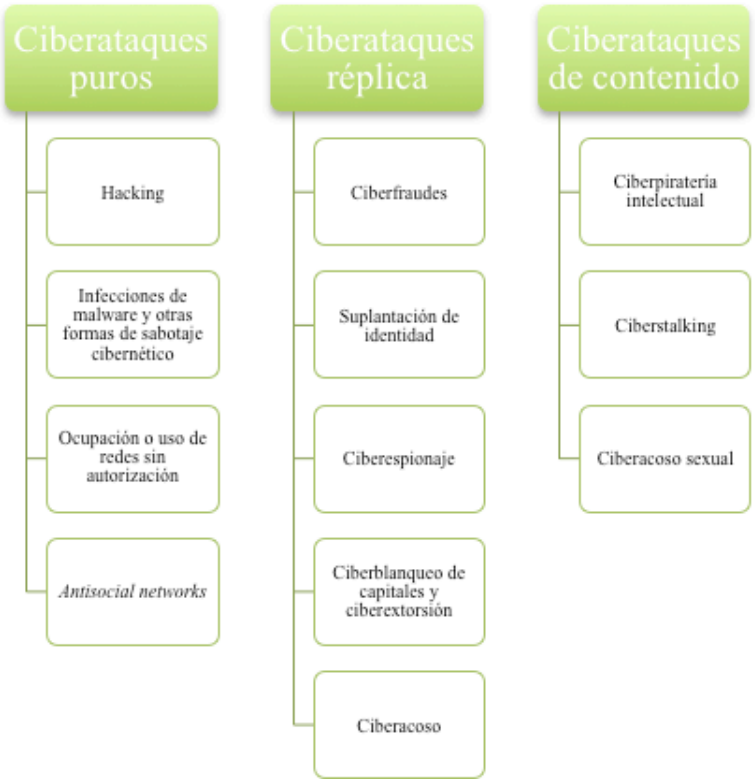


Imagen 2. Clasificación atendiendo a la incidencia de las TIC,s en el comportamiento criminal Miró (2012). Diseño propio.

[20] Miró Llinares, F. (2012). El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio. *El cibercrimen*, 1-332.

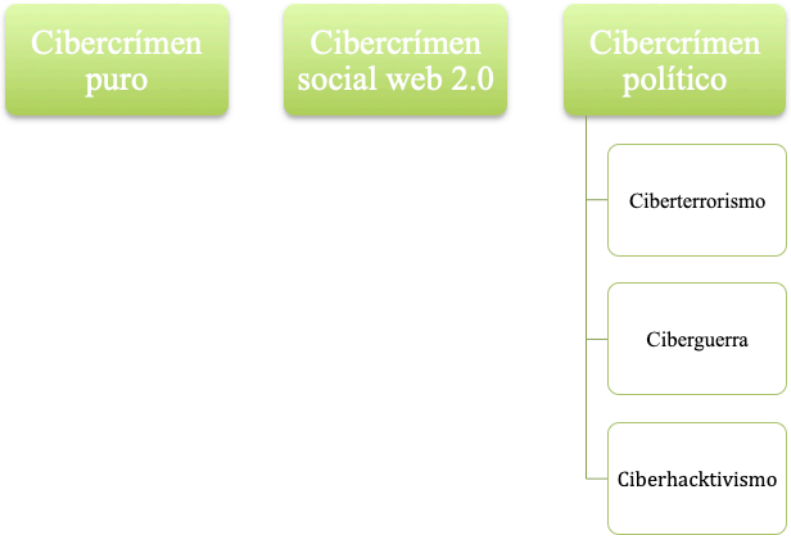


Imagen 3. Clasificación atendiendo al móvil y contexto criminológico. Miró (2012). Diseño propio.

2.2 El Código Penal español y los ciberdelitos.

El aumento en España del uso de Internet, ha ido en aumento. Hoy el día el crecimiento de hogares con acceso a Internet ha crecido de una manera elevada, tal y como se puede observar en el siguiente gráfico:

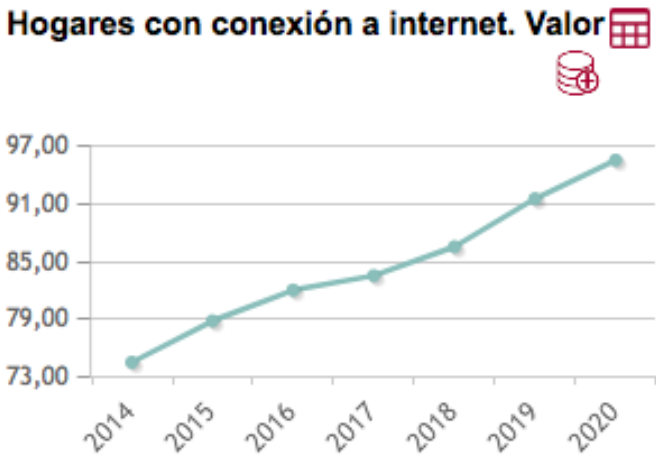


Imagen 4. Hogares españoles con conexión a Internet. Instituto Nacional de Estadística (2021)

Con las actuales modificaciones del Código Penal (CP), se han ido adaptando al marco legislativo aquellos delitos que guardan relación con la cibercriminalidad.

Es importante tener una buena retroalimentación por parte de las Autoridades, en relación a las nuevas tipologías delictivas, para poder realizar un abordaje desde las mismas en relación a la cuestión penal, así como para tratar de resarcir a las víctimas. No menos importante es la materia preventiva sobre ese tipo de hechos, que la base es el desconocimiento de estas nuevas tecnologías.

Desde la perspectiva jurídica los ciberdelitos forman parte de la tipicidad (conductas típicas) así expresadas en nuestro CP y donde la principal característica de estos delitos es que el objetivo o medio de comisión son los medios informáticos o las TIC,s.

Para tratar de profundizar y centrar los hechos penales que se puedan considerar en un sentido estricto, se van a plasmar las conductas tipificadas por el CP en el que haya un uso o afectación de esos dispositivos informáticos o TIC,s o que hayan sido realizados esos medios para realizar hechos delictivos.

Encuadrando dentro del marco legal, las modificaciones del CP sobre los ciberdelitos, debemos trasladarnos al 23 de febrero de 2001 que se creó el Convenio sobre la Ciberdelincuencia en Budapest y que España ratificó el citado convenido el 17 de septiembre de 2010, publicado en el Boletín Oficial del Estado (BOE) número 226, páginas 78847 a 78896. Entre las características más importantes son que los países firmantes, establecen unas herramientas de colaboración entre éstos para la prevención e investigación de estos delitos.

Como precedente en el apoyo de este tratado, la UE creó la Directiva 2000/31/CE aprobando la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico que regula y audita la responsabilidad de las empresas operadoras de las redes, las empresas prestadoras de servicios así como las proveedoras de servicios de Internet.

Otra de las novedades de interés que ha adoptado España, es la creación de la Fiscalía de Criminalidad Informática (FCI) mediante el RD 1735/2010, cuya misión entre otras es la investigación de los delitos encuadrados como "ciberdelitos". Ésta Fiscalía mediante la Instrucción 2/2011 establece y desarrolla las categorías para investigar siendo las siguientes:

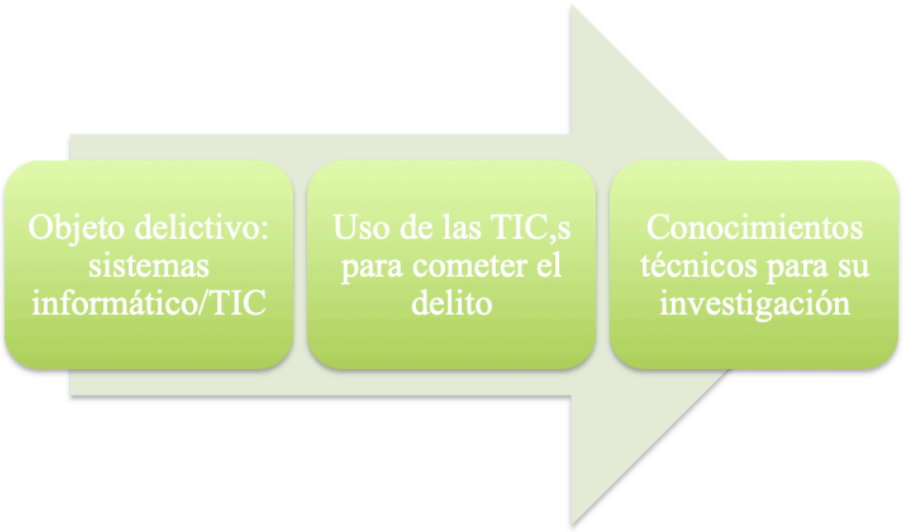


Imagen 5. Clasificación Instrucción FCI. Diseño propio.

Dada la importancia del aumento de los ciberdelitos, tal y como se va a ver en siguientes apartado en el correspondiente análisis descriptivo, la legislación española adaptó ciertos tipos delictivos relacionados con los ciberdelitos a través de la modificación del CP creando la Ley Orgánica 1/2015 de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, publicado en el BOE número 77 de 31 de marzo de 2015.

Es interesante ver cómo en esta modificación y adaptación de ciertos tipos penales, incluyeran los relacionados con los ciberdelitos, ya que se trata de una realidad delictiva.

A continuación se plasman los nuevos artículos o los que han sido modificados o adaptados, con el fin de visualizar los tipos de delitos encuadrados en el cibercrimen. Se reseñan que son descritos los principales delitos investigados en el presente trabajo.

ARTÍCULO	ANTERIOR CP 10/1995	NUEVO CP 1/2015
197	1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con laspenas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. 2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero. 3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años. Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b ag del apartado 7 del artículo 33. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.	1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses 2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero. 3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior. 4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando: a. Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima. Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior. 5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior. 6. Si los hechos se realizan con fines

		lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.
197 bis, ter cuater y quinquies	No existían en el anterior CP y se crean en el nuevo.	ART. 197 BIS 1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años. 2. El que mediante la utilizaciónde artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses. ART. 197 TER Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que serefieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis: a) un programa informático, concebido o adaptado principalmente para cometer dichosdelitos; o b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un

		sistema de información ART. 197 QUATER Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado. ART. 197 QUINQUIES Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.
264	1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisiónde seis meses a dos años. 2. El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años. 3. Se impondrán las penas superiores en grado a las respectivamente señaladas en los dos apartados anteriores y, en todo caso, la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias: 1º Se hubiese cometido en el marco de una organización criminal. 2º Haya ocasionado daños de especial gravedad o afectado a los intereses generales. 4. Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrán las siguientes penas: a) Multa del doble al cuádruple del perjuicio causado, si el delito cometido por la persona física tiene prevista una pena de prisión de más de dos años. b) Multa del doble al triple del perjuicio causado, en el resto de los casos. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las	1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años. 2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias: 1º Se hubiese cometido en el marco de una organización criminal. 2º Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos. 3º El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad. 4º Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones. 5º El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter. Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado. 3. Las penas previstas en los apartados

	letras b) a g) del apartado 7 del artículo 33.	anteriores se impondrán, en sus respectivos casos, en sumitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero
264 bis, ter y cuater.	No existían en el anterior CP y se crean en el nuevo.	ART. 264 BIS 1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno: a. realizando alguna de las conductas a que se refiere el artículo anterior; b. introduciendo o transmitiendo datos; o destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica. Si los hechos hubieran perjudicado de forma relevante laactividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado. 2. Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior. 3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en sumitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero. ART. 264 TER Será castigado con una pena deprisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores: a) un programa informático, concebido o adaptadoprincipalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores;o b) una contraseña de ordenador, un código de acceso o datossimilares que permitan acceder a la totalidad o a una parte de un sistema de información. ART. 264 QUATER Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los tresartículos anteriores, se le impondrán

		las siguientes penas: a) Multa de dos a cinco años o del quíntuplo a doce veces el valor del perjuicio causado, si resulta una cantidad superior, cuando se trate de delitos castigados con una pena de prisión de más de tres años. b) Multa de uno a tres años o del triple a ocho veces el valor del perjuicio causado, si resulta una cantidad superior, en el resto de los casos. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.
400	La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.	La fabricación, recepción, obtención o tenencia de útiles, materiales, instrumentos, sustancias, datos y programas informáticos, aparatos, elementos de seguridad, u otros medios específicamente destinados a la comisión de los delitos descritos en los Capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

2.3 Teorías criminológicas relativas al fenómeno de la ciberdelincuencia.

El ámbito criminal en el espacio de la ciberdelincuencia, como no podría ser menos, se trata de un fenómeno delictivo, que pese a ser relativamente reciente, ya que el descubrimiento y uso de las TIC,s lleva pocos años con nosotros, no deja de ser una modalidad delictiva. Siguiendo a Serrano Maíllo (2009), éste propone que los desarrollos teóricos creados sobre los cibercrímenes, se sustentan en las teorías criminológicas tradicionales.

Es por ello que hay autores criminólogos que han tratado de dar una explicación de la etiología del ciberdelito apoyados en estas teorías criminológicas tradicionales[21][22]

[21] GONZÁLEZ GARCÍA, Abel (2016). "Cibercriminología, el futuro está aquí", en BRIGGS, D., RÁMILA, J., & PÉREZ SUÁREZ, J.R. (Dirs.). La Criminología de hoy y del mañana. Dykinson, Madrid.

[22] CHOI, K.S. & TORO- ÁLVAREZ, M.M. (2017). Cibercriminología. Guía para la investigación del cibercrimen y mejores prácticas en seguridad digital (Cybercriminology Guide for the investigation of cybercrime and best practices in digital security). Universidad Antonio Nariño, Bogotá.

Esas teorías criminológicas relacionadas con el ciberdelito que se proponen son las siguientes:

- **Teoría de las Actividades Rutinarias y de la Oportunidad.**

Dentro de la teoría de las Actividades Rutinarias de Cohen y Felson (1979) proponían que habían tres factores que favorecen la victimización criminal: una víctima propicia + ofensor motivado + ausencia de fuerza para el control de la violación de la norma. Si sumamos los factores, tal y como se han expuesto en los tipos de ciberdelitos, propongo el siguiente ejemplo:

Imagen 6. Ejemplo de las teorías Rutinarias de Cohen y Felson aplicadas al cibercrimen. Diseño propio.

Es una clara muestra de la aplicación de ésta teoría al cibercrimen. No obstante la Covid 19 ha generado un gran cambio en las personas. Como anteriormente he reflejado Stickle y Felson, (2020) exponen que "nos encontramos ante el mayor experimento de criminología de la historia" ya que nuestras actividades cotidianas como se ha explicado con anterioridad, han cambiado de manera tan sustancial que como no podía ser menos, han repercutido en el crimen. Todo ello ha quedado reflejado en la nueva teoría que han propuesto y revisado estos autores, en relación con la Covid 19 en "Crime Rates in a Pandemic: the Largest Criminological Experiment in History." En lo que respecta a la teoría de la

oportunidad de Cloward y Ohlin (1960), nos encontramos con que los ciberdelincuentes, utilizan las brechas de seguridad en los dispositivos para realizar esos ataques o fraudes, aprovechando esa oportunidad delictiva en la que el control social es mínimo.

- **Teoría la elección racional.**

Desarrollada por Cornish y Clarke (1986), trata de una manera clara la acción del ser humano en base a la racionalidad sobre el coste de la acción y el beneficio de la misma. Explicado de otra manera lo que trata el comportamiento humano es la detener una maximización de un interés propio en base a nuestras elecciones. Para ello se basa en tres condiciones ideales:

1. Que la acción sea el mejor medio para conseguir lo que ansía el individuo.
2. Las creencias sobre el objetivo deben ser racionales.
3. Una inversión óptima de los recursos a invertir para que le salga rentable.

¿Cómo podríamos traducirlo en el cibercrimen? Con el caso anteriormente propuesto del delito de estafa en inversiones en criptomonedas. Los beneficios económicos pueden llegar a ser muy altos y donde, sin entrar en detalles del hecho, el tipo penal genérico correspondería al Art, 248.5 de nuestro Código Penal, donde la pena de prisión está entre los 6 meses y 3 años de prisión, siempre y cuando se pudiera localizar al autor, o aplicando el Artículo 250 donde a pena de prisión comprende entre 1 y 6 años de prisión. Un claro ejemplo de cómo el coste-beneficio puede llegar a ser rentable en ciertos casos, ya que hay estafas como las inversiones en criptomonedas, donde hay causas millonarias como se ha expuesto.

- **Teoría de aprendizaje social y la asociación diferencial.**

Este conjunto de teorías basadas en Akers (1979) y Sutherland (1929), tienen como punto de partida que las personas, al establecer relaciones comunicativas con otras mismas personas, es de por sí una herramienta de aprendizaje. El delito podría aprenderse mediante una asociación diferencial creada por un proceso de aprendizaje. Si trasladamos esto al cibercrimen, los delincuentes se relacionan con sus víctimas a través del ciberespacio. Siguiendo a Skinner y Fream (1997) citado por Cámara S. (2020) definen esta relación como un proceso de contaminación criminógena.

- **Teoría de las ventanas rotas.**

Esta conocida teoría de Wilson y Kelling (1982) en la que se propone que los medios de control social mediante su inacción, traslada la idea de que hay un desorden y una decadencia en la sociedad. Si lo extrapolamos al cibercrimen, tal y como se explica en este trabajo, ciertas tipologías delictivas en el ámbito del cibercrimen, al no haber métodos eficaces para su detección por parte de las Autoridades, ya que algunos delitos son de muy difícil resolución, así como las penas de prisión como se exponen en este trabajo, son mínimas frente al coste-beneficio, creando esa sensación de ventanas rotas en los criminales.

- **Teoría del control social, autocontrol y vínculos sociales.**

Siguiendo a Gottfredson y Hirschi (1990) citado por cámara S. (2020), el factor etológico dentro de la teoría del autocontrol, es la capacidad que tiene el individuo para poder tener un control sobre los impulsos y deseos. Hoy en día con la implementación de las TIC, han conseguido que los vínculos sociales tradicionales, se han ido impersonalizando y deshumanizando, debido a este tipo de comunicaciones más irreales, debido a la falta del factor físico y humano. Como ejemplo las diferentes redes sociales conocidas como son Facebook o Instagram. Este uso de redes con un bajo control social, especialmente por parte

de los padres ya que ofrecen una privacidad a los usuarios, difícilmente de controlar y que podría darse el caso de tener una impunidad tras las redes.

- **Teoría general de la tensión de Robert Agnew.**

Dentro de los postulados de esta teoría, en los que se presume que el crimen es fuente de la frustración que recibe el individuo por ciertos estados emocionales que son negativos. Si trasladamos esta teoría al cibercrimen, el ciberespacio podría ser un lugar en el que el delincuente se encuentre con una libertad, donde pueda liberar esas tensiones y con ello encontrar esa tranquilidad. Recordemos la falta de control que hay en el ciberespacio, y que ello puede hacer que sea un motivo de "relajación" de esa tensión por parte del delincuente. Siguiendo a Hinduja y Pachín (2015) citado por Cámara S. (2020) hay una vinculación de desviación criminógena en víctimas de cyberbullying, donde encuentran en el ciberespacio esa liberación de la tensión.

- **Otras teorías relacionadas.**

El cibercrimen se trata de una nueva metodología delictiva que es de muy reciente creación y es por ello que hay que realizar una readaptación de las teorías criminológicas más clásicas y readaptarlas. Como ejemplo se propone la Teoría de la Acción situacional revisada para Internet (SAT-RI) la cual tiene su raíz en la Teoría de la Acción situacional propuesta por Wikström (2010) y que Pérez (2015)[23] la apoya en el contexto digital.

[23] González, AG. (2016). Cibercriminología, el futuro está aquí. In *La Criminología de hoy y del mañana* (pp. 113-128). Dykinson.

3.- OBJETIVOS E HIPÓTESIS, DATOS Y METODOLOGÍA

3.1.- Objetivos e hipótesis

Las hipótesis que se plantean en el presente trabajo, en relación a la relación del Covid 19 y los ciberdelitos, son las siguientes:

- H1 Los ciberdelitos denunciados en España han aumentado durante la pandemia de COVID-19.
- H2 No todos los tipos de ciberdelito han aumentado durante la pandemia de COVID-19.
- H3 Los ciberdelitos relacionados con la venta online han aumentado durante la pandemia de COVID-19.

Los objetivos que se proponen con el presente trabajo, es conocer si realmente ha habido esa incidencia respecto al aumento del cibercrimen respecto a la pandemia por la Covid 19 para ello se enumeran a continuación:

- Verificar si realmente ha habido ese aumento de ciberdelitos correlacionados por la pandemia.
- Analizar qué delitos han aumentado y en qué medida.
- Qué autonomías han tenido mayor variación de los ciberdelitos (aumento descenso).
- En caso de que sea cierto ese aumento, proponer una serie de medidas respecto a la política criminal y medidas preventivas desde el aspecto victimológico.

3.2.- Datos y metodología

El presente análisis de este estudio se realiza con todos los datos relativos a los delitos ocurridos en el ámbito de competencia territorial de la Guardia Civil. Dichos datos, han sido cedidos sin datos personales de las víctimas o perjudicados

pero con una calidad de los mismo que se puedan desarrollar de una manera efectiva, el estudio del ellos y obtener una información de interés.

Los datos recibidos se han confeccionado a través de un archivo Excel, donde debido a la forma en que se encuentra integrada la información en los sistemas de la Guardia Civil, ha habido que realizar una depuración de los datos, realizando una verificación de la información, acarreando una compleja labor, dado que había gran cantidad de información contenida.

La estructura que se encuentran los datos de las bases se encuentran de la siguiente forma:

Medio empleado:

Se trata de la herramienta utilizada para realizar el ataque.

Modus operandi:

Es la forma en que se ha utilizado el ataque para cometer el hecho delictivo con la que sin ella, no hubiera podido realizarse.

Las variables que se han decidido que son de interés son las siguientes:

- Hecho tipo. (Tipo de delito)
- Fecha de ocurrencia.
- Tipo de medio empleado/modus operandi. (Se establece como en la descripción anterior de medio o modus, tal y como establece la GC)

Las hipótesis que se han planteado, se desarrollarán realizando un análisis estadístico, aplicando tanto valores cualitativos como cuantitativos, de los datos que se han obtenido, mediante el apoyo del programa estadístico SPSS, de los diferentes tipos de delitos anteriormente expuestos relacionados con el cibercrimen que se encuentran en la demarcación de Guardia Civil entre los años 2017 al 2020.

Se va a emplear una metodología de estadística descriptiva con el fin de una manera científica y sencilla, tratar de exponer los resultados obtenidos mediante el estudio de los datos y resultados obtenidos. Se va a hacer un análisis detallado por años, así como por trimestres con el fin de tratar de verificar de una manera más aproximada los datos concretos.

En el siguiente epígrafe, se establecen los datos obtenidos comparativos a través de las variables obtenidas y según la clasificación dada por la Guardia Civil tanto en medio empleado como en modus operandi en los delitos relacionados con el presente estudio. No se establece de otra manera la clasificación ya que con ello se trata de preservar la calidad de los datos evitando hacer transformaciones con el fin de descartar la mayor pérdida de datos posibles.

4.- RESULTADOS

En el presente apartado se va a tratar de analizar los datos obtenidos totales, en los que se comparan entre los años 2017 al 2020 los diferentes tipos de delitos ocurridos, según el Modus Operandi o Medio Empleado, como se ha descrito anteriormente.

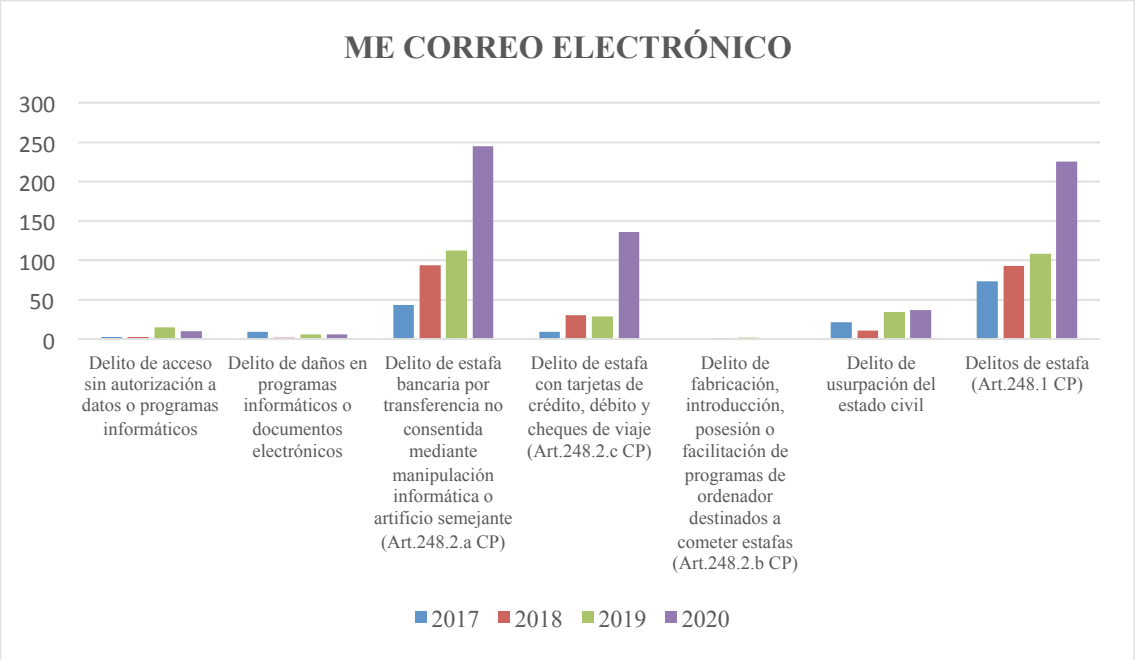
Los datos que se han considerado que ha habido un aumento durante el año 2020, se han subdivido por trimestres con el fin de tratar de tener una mayor precisión en los datos.

4.1 Medio empleado.

4.1.1 Correo electrónico

DELITOS	2017	2018	2019	2020
Delito de acceso sin autorización a datos o programas informáticos	3	3	15	10
Delito de daños en programas informáticos o documentos electrónicos	9	2	6	6
Delito de estafa bancaria por transferencia no consentida mediante manipulación informática o artificio semejante (Art.248.2.a CP)	43	94	112	245
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	9	30	29	136
Delito de fabricación, introducción, posesión o facilitación de programas de ordenador destinados a cometer estafas (Art.248.2.b CP)	0	1	2	0
Delito de usurpación del estado civil	21	11	34	37

Delitos de estafa (Art.248.1 CP)	73	93	108	225
TOTAL	**158**	**234**	**306**	**659**



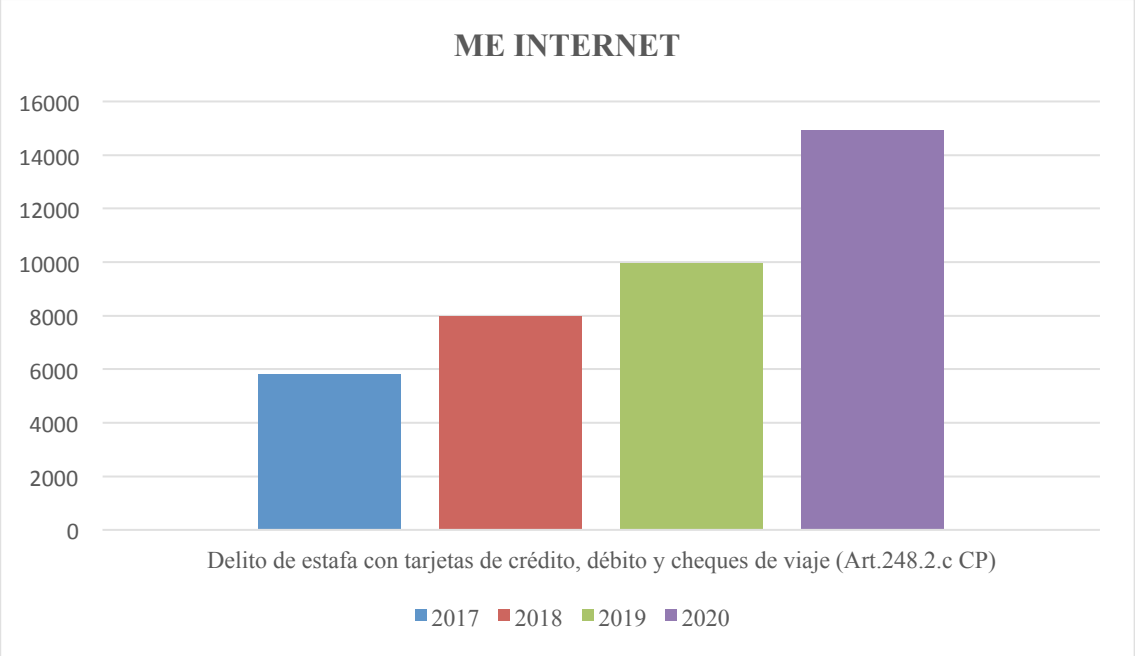
DELITOS 2020	**TRIM 1**	**TRIM 2**	**TRIM 3**	**TRIM 4**
Delito de acceso sin autorización a datos o programas informáticos	1	1	5	3
Delito de daños en programas informáticos o documentos electrónicos	2	1	2	1
Delito de estafa bancaria por transferencia no consentida mediante manipulación informática o artificio semejante (Art.248.2.a CP)	36	53	80	76
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	18	28	41	49
Delito de usurpación del estado civil	9	5	10	13
Delitos de estafa (Art.248.1 CP)	41	68	66	50
TOTAL	**107**	**156**	**204**	**192**

Dentro del Medio Empleado para cometer el delito, mediante el uso del correo electrónico, como se puede observar, el incremento del año 2020 respecto del año 2019, en la suma total de los delitos, ha sido de más de un 100%. Por lo que se

puede comprobar de una manera significativa, que el aumento de ciberdelitos durante el año 2020, año de la Covid19, puede tener una relación directa.

4.1.2 Internet

DELITOS	2017	2018	2019	2020
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	5820	7997	9946	14924
Total general	**5820**	**7997**	**9946**	**14924**

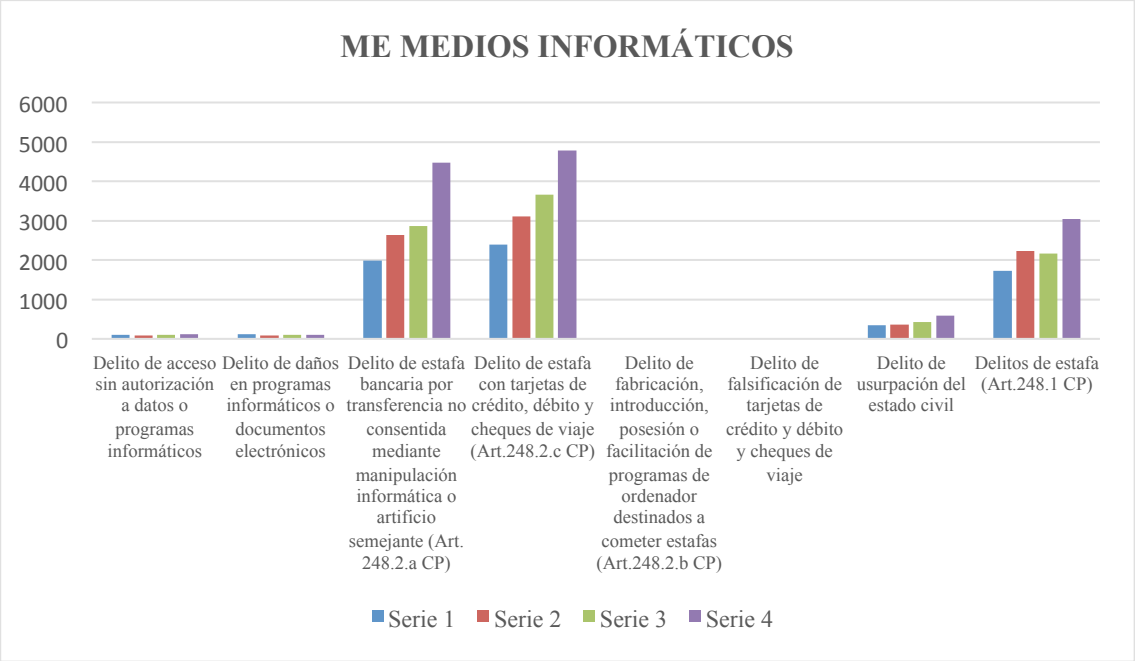


DELITOS 2020	TRIM 1	TRIM 2	TRIM 3	TRIM 4
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	2656	3421	3839	5008
TOTAL	**2656**	**3421**	**3839**	**5008**

Como se aprecia en el Medio Empleado Internet, únicamente se cataloga el delito que se reseña, ya que el sistema interno de la Guardia Civil, únicamente contempla eso. Como se puede observar, nuevamente hay un incremento reseñable de los delitos, respecto a los anteriores años, superando en un 50% el año 2020 frente al año 2019. Los indicios respecto a que el Covid19 haya podido influir en ese aumento, queda patente.

4.1.3 Medios informáticos

DELITOS	**2017**	**2018**	**2019**	**2020**
Delito de acceso sin autorización a datos o programas informáticos	99	93	110	113
Delito de daños en programas informáticos o documentos electrónicos	120	83	101	99
Delito de estafa bancaria por transferencia no consentida mediante manipulación informática o artificio semejante (Art.248.2.a CP)	1987	2640	2872	4474
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	2387	3112	3665	4780
Delito de fabricación, introducción, posesión o facilitación de programas de ordenador destinados a cometer estafas (Art.248.2.b CP)	13	23	9	16
Delito de falsificación de tarjetas de crédito y débito y cheques de viaje	13	14	10	12
Delito de usurpación del estado civil	339	359	419	594
Delitos de estafa (Art.248.1 CP)	1724	2235	2160	3039
Total general	**6343**	**8200**	**8927**	**12533**

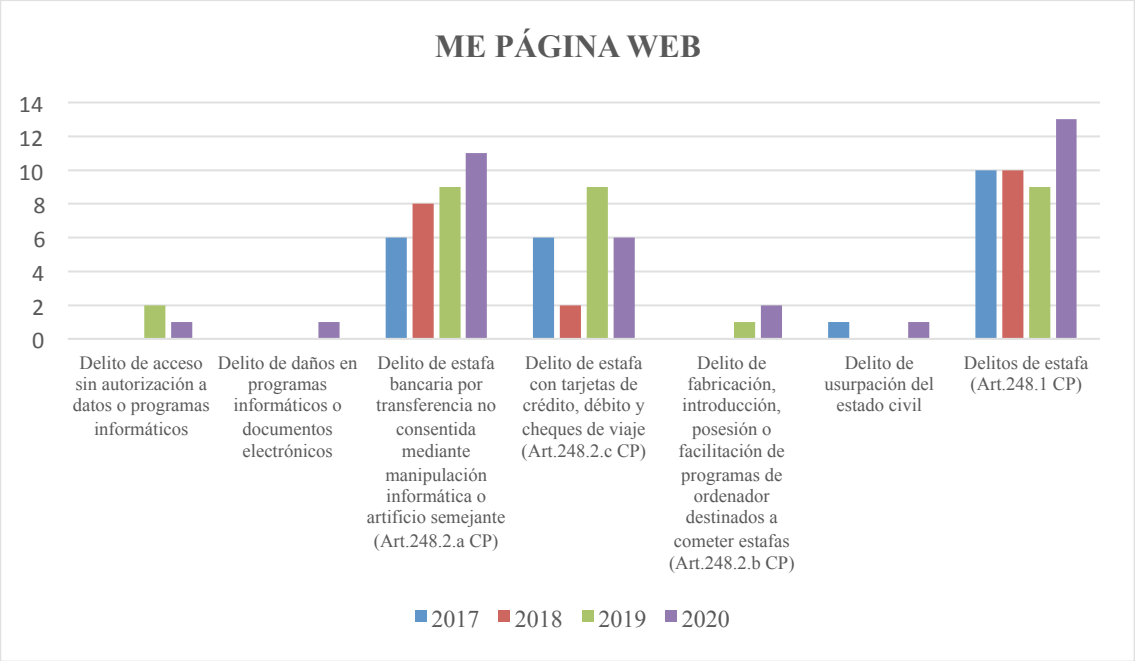


DELITOS 2020	**TRIM 1**	**TRIM 2**	**TRIM 3**	**TRIM 4**
Delito de acceso sin autorización a datos o programas informáticos	20	30	35	28
Delito de daños en programas informáticos o documentos electrónicos	24	21	26	28
Delito de estafa bancaria por transferencia no consentida mediante manipulación informática o artificio semejante (Art.248.2.a CP)	753	1035	1319	1367
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	860	1094	1282	1544
Delito de fabricación, introducción, posesión o facilitación de programas de ordenador destinados a cometer estafas (Art.248.2.b CP)	4	6	4	2
Delito de falsificación de tarjetas de crédito y débito y cheques de viaje	3	2	4	3
Delito de usurpación del estado civil	130	136	148	180
Delitos de estafa (Art.248.1 CP)	517	819	887	816
TOTAL	**2291**	**3113**	**3670**	**3940**

El Medio Empleado por Medios Informáticos, el incremento del año 2020 frente al año 2019, es muy reseñable, ya que el porcentaje nuevamente alcanza algo menos del 50%. Datos muy interesantes, debido a que se trata de una muestra más sobre que el cibercrimen, puede que haya crecido debido a la Covid 19 y todo lo que le rodea.

4.1.4 Páginas de Internet

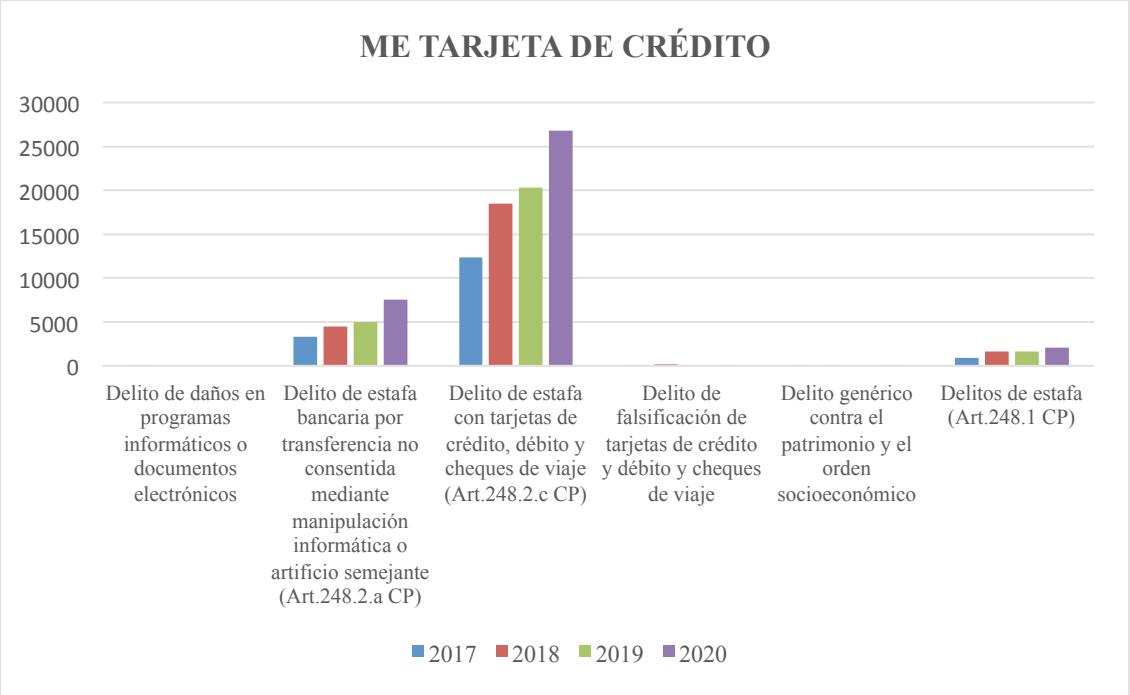
DELITOS	**2017**	**2018**	**2019**	**2020**
Delito de acceso sin autorización a datos o programas informáticos	0	0	2	1
Delito de daños en programas informáticos o documentos electrónicos	0	0	0	1
Delito de estafa bancaria por transferencia no consentida mediante manipulación informática o artificio semejante (Art.248.2.a CP)	6	8	9	11
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	6	2	9	6
Delito de fabricación, introducción, posesión o facilitación de programas de ordenador destinados a cometer estafas (Art.248.2.b CP)	0	0	1	2
Delito de usurpación del estado civil	1	0	0	1
Delitos de estafa (Art.248.1 CP)	10	10	9	13
TOTAL	**23**	**20**	**30**	**35**



El Medio Empleado por Página Web, no hay datos que sean reseñables, si bien, mantiene la tendencia de crecimiento normal, respecto a los años anteriores.

4.1.5 Tarjeta de crédito

DELITOS	**2017**	**2018**	**2019**	**2020**
Delito de daños en programas informáticos o documentos electrónicos	1	0	0	0
Delito de estafa bancaria por transferencia no consentida mediante manipulación informática o artificio semejante (Art.248.2.a CP)	3336	4453	5010	7549
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	12367	18500	20329	26787
Delito de falsificación de tarjetas de crédito y débito y cheques de viaje	90	172	66	54
Delito genérico contra el patrimonio y el orden socioeconómico	46	69	71	14
Delitos de estafa (Art.248.1 CP)	868	1635	1632	2049
Total general	**16708**	**24829**	**27108**	**36453**



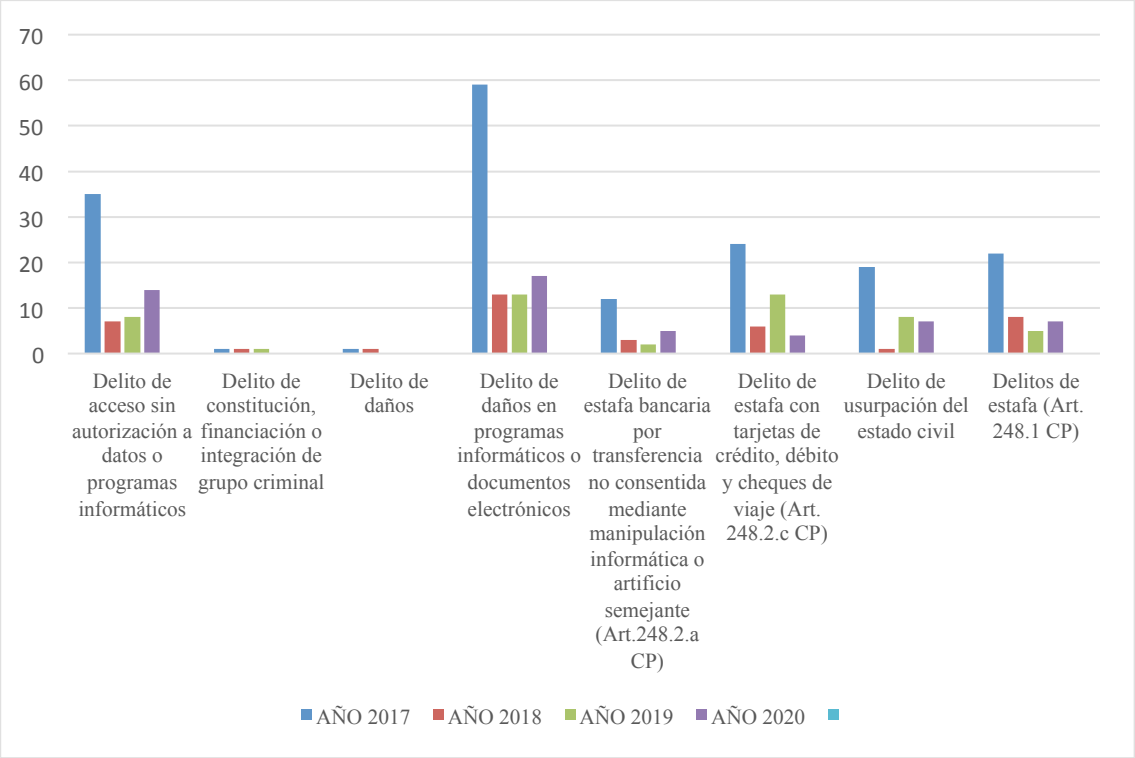
DELITOS 2020	**TRIM 1**	**TRIM 2**	**TRIM 3**	**TRIM 4**
Delito de estafa bancaria por transferencia no consentida mediante manipulación informática o artificio semejante (Art.248.2.a CP)	1524	1810	2031	2184
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	5229	6117	7182	8259
Delito de falsificación de tarjetas de crédito y débito y cheques de viaje	11	12	13	18
Delito genérico contra el patrimonio y el orden socioeconómico	5	4	2	3
Delitos de estafa (Art.248.1 CP)	397	500	530	622
TOTAL	**5642**	**6633**	**7727**	**8902**

El Medio Empleado por Tarjeta de Crédito, arroja datos muy reseñables, ya que el año 2020 tiene un aumento sustancial respecto al año 2019, alcanzando casi un aumento del 50% nuevamente. Algo que mantiene un crecimiento constante respecto con la mayoría de las variables del Medio Empleado. Se puede inferir que ese aumento de ciberdelitos durante el 2020, guarda una relación directa por esa crisis sanitaria, ya que ese incremento habido, no es lineal respecto al periodo del 2017 al 2019.

4.2 Modus operandi

4.2.1 Ataque contra sitio web

DELITOS	2017	2018	2019	2020
Delito de acceso sin autorización a datos o programas informáticos	35	7	8	14
Delito de constitución, financiación o integración de grupo criminal	1	1	1	0
Delito de daños	1	1	0	0
Delito de daños en programas informáticos o documentos electrónicos	59	13	13	17
Delito de estafa bancaria por transferencia no consentida mediante manipulación informática o artificio semejante (Art.248.2.a CP)	12	3	2	5
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	24	6	13	4
Delito de usurpación del estado civil	19	1	8	7
Delitos de estafa (Art.248.1 CP)	22	8	5	7
Total general	**173**	**39**	**50**	**54**

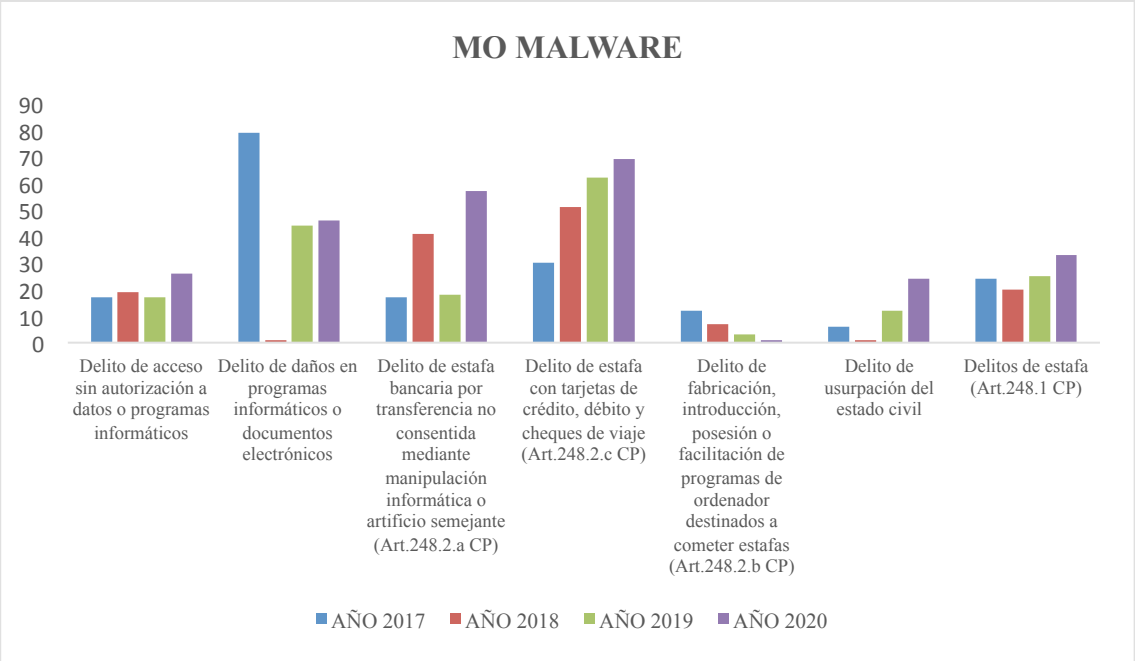


El Modus Operandi por Ataque Contra Sitio web, ha sufrido un descenso sustancial, respecto al año 2017 y que ha mantenido su constante de descenso. No habiendo datos que sean de interés.

4.2.2. Malware

DELITOS	2017	2018	2019	2020
Delito de acceso sin autorización a datos o programas informáticos	17	19	17	26
Delito de daños en programas informáticos o documentos electrónicos	79	1	44	46
Delito de estafa bancaria por transferencia no consentida mediante manipulación informática o artificio semejante (Art.248.2.a CP)	17	41	18	57
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	30	51	62	69
Delito de fabricación, introducción, posesión o facilitación de programas de ordenador destinados a cometer estafas (Art.248.2.b CP)	12	7	3	1
Delito de usurpación del estado civil	6	1	12	24

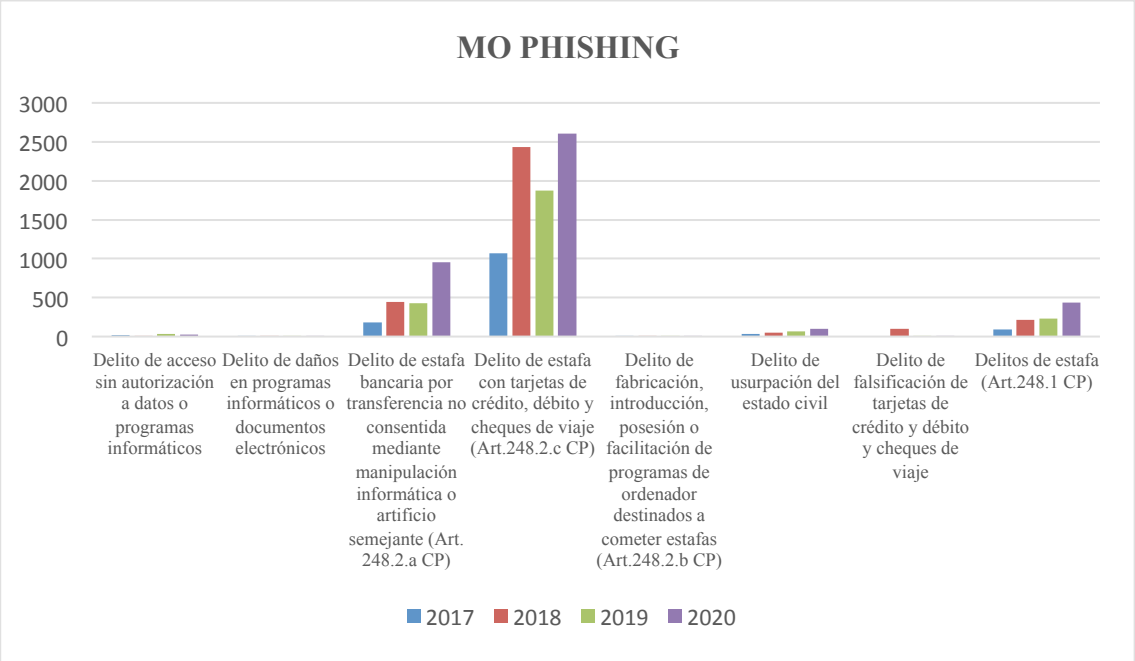
Delitos de estafa (Art.248.1 CP)	24	20	25	33
Total general	**186**	**140**	**181**	**256**



El Modus Operando por Malware ha sufrido un aumento respecto a la línea del periodo objeto de estudio. No hay datos de especial relevancia en el crecimiento de esta tipología, aunque considerando esa cifra el aumento es ligeramente significativo.

4.2.3 Phishing

DELITOS	2017	2018	2019	2020
Delito de acceso sin autorización a datos o programas informáticos	17	12	30	26
Delito de daños en programas informáticos o documentos electrónicos	6	3	8	6
Delito de estafa bancaria por transferencia no consentida mediante manipulación informática o artificio semejante (Art.248.2.a CP)	183	442	429	954
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	1065	2433	1875	2602
Delito de fabricación, introducción, posesión o facilitación de programas de ordenador destinados a cometer estafas (Art.248.2.b CP)	3	2	2	5
Delito de usurpación del estado civil	37	54	70	102
Delito de falsificación de tarjetas de crédito y débito y cheques de viaje	0	101	5	6
Delitos de estafa (Art.248.1 CP)	88	214	229	437
Total general	**1399**	**3160**	**2643**	**4132**



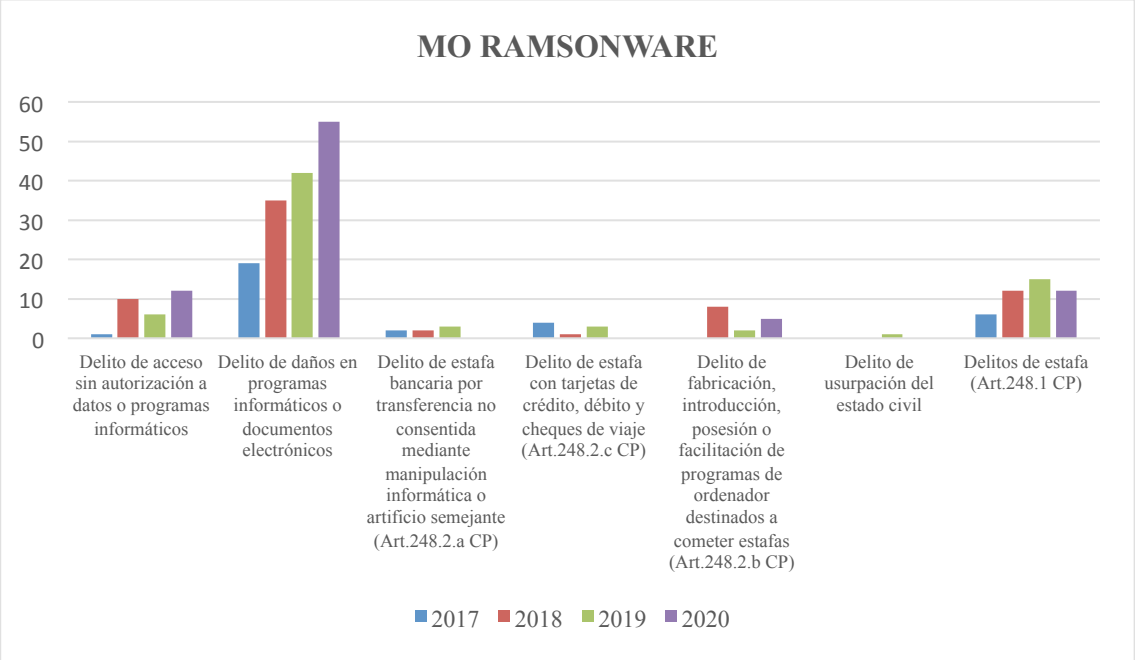
DELITOS 2020	TRIM 1	TRIM 2	TRIM 3	TRIM 4
Delito de acceso sin autorización a datos o programas informáticos	4	5	10	7
Delito de daños en programas informáticos o documentos electrónicos	2	1	2	1
Delito de estafa bancaria por transferencia no consentida mediante manipulación informática o artificio semejante (Art.248.2.a CP)	193	236	278	247
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	616	649	644	693
Delito de fabricación, introducción, posesión o facilitación de programas de ordenador destinados a cometer estafas (Art.248.2.b CP)	0	2	3	1
Delito de falsificación de tarjetas de crédito y débito y cheques de viaje	0	2	3	0
Delito de usurpación del estado civil	20	24	30	28
Delitos de estafa (Art.248.1 CP)	95	112	101	129
TOTAL	**930**	**1031**	**1071**	**1106**

El Phishing sin lugar a dudas, es el Modus Operandi que ha tenido uno de los crecimientos más significativos, ya que ha sido de más de un 100% respecto al año 2019. Nuevamente sumamos un indicio más para esa relación directa entre el aumento de ciberdelitos y la Covid 19.

4.2.4 Ramsonware

DELITOS	2017	2018	2019	2020
Delito de acceso sin autorización a datos o programas informáticos	1	10	6	12
Delito de daños en programas informáticos o documentos electrónicos	19	35	42	55
Delito de estafa bancaria por transferencia no consentida mediante manipulación informática o artificio semejante (Art.248.2.a CP)	2	2	3	0
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	4	1	3	0
Delito de fabricación, introducción, posesión o facilitación de	0	8	2	5

programas de ordenador destinados a cometer estafas (Art.248.2.b CP)				
Delito de usurpación del estado civil	0		1	0
Delitos de estafa (Art.248.1 CP)	6	12	15	12
Total general	**32**	**68**	**72**	**84**

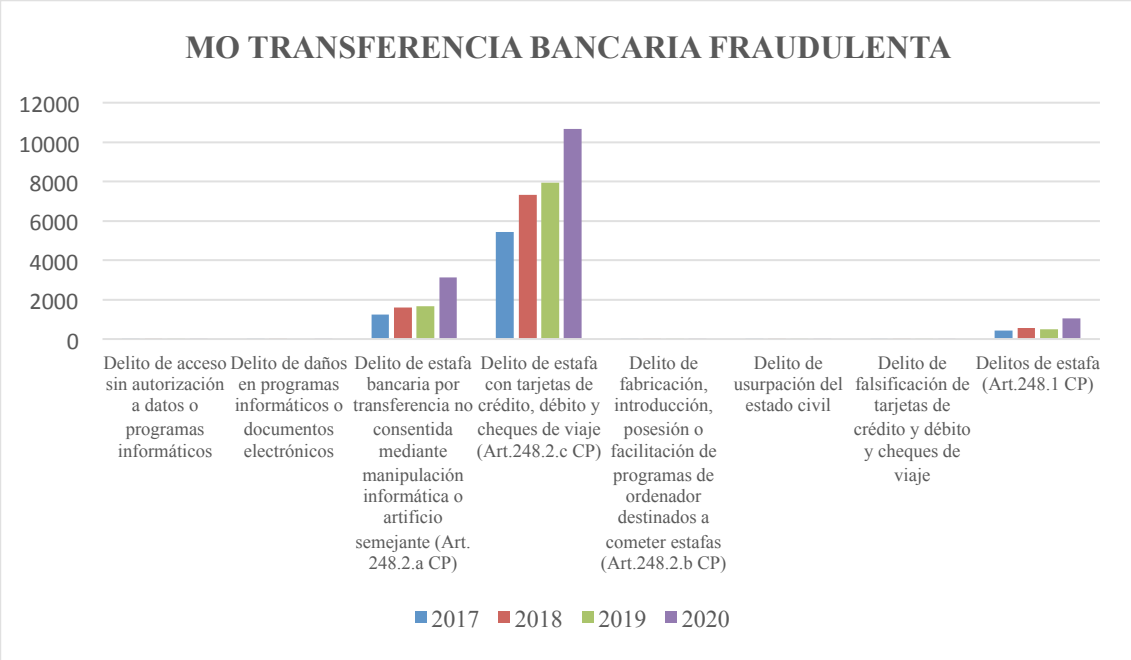


En este modus Operandi, no se encuentran datos que sean especialmente significativos.

4.2.5 Transferencia bancaria fraudulenta

DELITOS	**2017**	**2018**	**2019**	**2020**
Delito de acceso sin autorización a datos o programas informáticos	4	2	7	6
Delito de daños en programas informáticos o documentos electrónicos	3	1	0	1
Delito de estafa bancaria por transferencia no consentida mediante manipulación informática o artificio semejante (Art.248.2.a CP)	1242	1604	1668	3141
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	5429	7310	7950	10652
Delito de fabricación, introducción, posesión o facilitación de	5	5	1	6

programas de ordenador destinados a cometer estafas (Art.248.2.b CP)				
Delito de usurpación del estado civil	25	31	42	56
Delito de falsificación de tarjetas de crédito y débito y cheques de viaje	38	20	24	18
Delitos de estafa (Art.248.1 CP)	420	573	504	1064
Total general	**7128**	**9526**	**10172**	**14926**



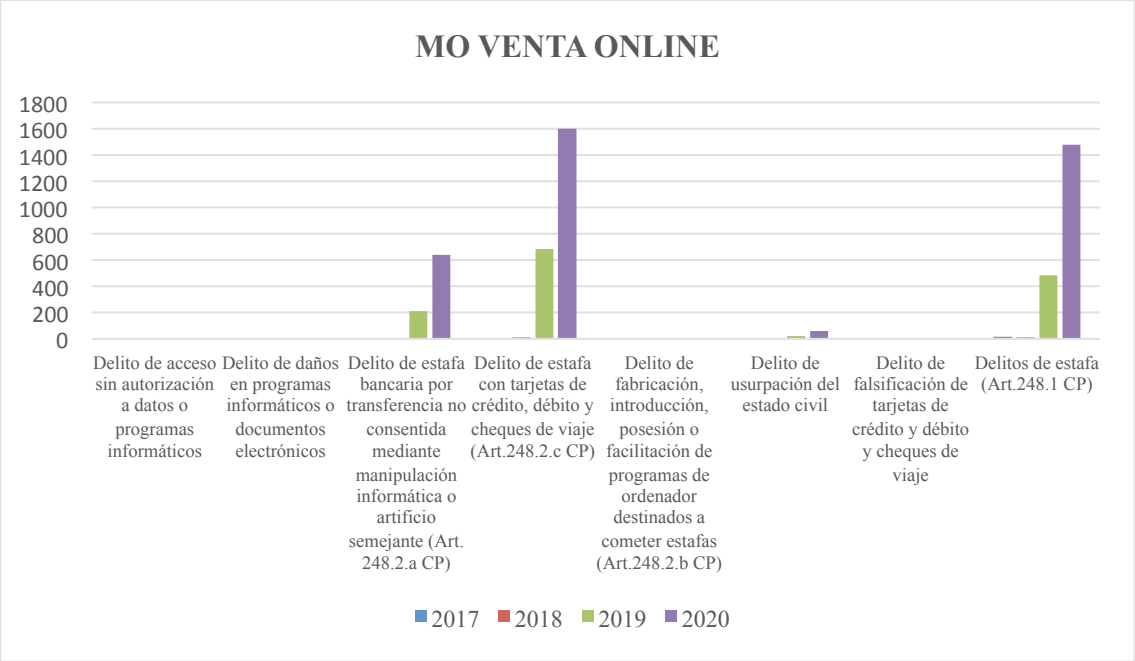
DELITOS 2020	**TRIM 1**	**TRIM 2**	**TRIM 3**	**TRIM 4**
Delito de acceso sin autorización a datos o programas informáticos	1	0	2	3
Delito de estafa bancaria por transferencia no consentida mediante manipulación informática o artificio semejante (Art.248.2.a CP)	475	632	1	1088
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	1853	2305	946	3600
Delito de fabricación, introducción, posesión o facilitación de programas de ordenador destinados a cometer estafas (Art.248.2.b CP)	1	4	2891	1

Delito de falsificación de tarjetas de crédito y débito y cheques de viaje	5	4	3	6
Delito de usurpación del estado civil	9	11	14	22
Delitos de estafa (Art.248.1 CP)	148	225	328	363
TOTAL	**2492**	**3181**	**4185**	**5083**

En esta ocasión el Modus Operandi por Transferencia Bancaria fraudulenta sufre un aumento significativo ya que respecto al año 2019 ha habido un aumento de un casi 50% durante el año 2020. Un crecimiento mayor, respecto a los años anteriores. Nuevamente sumamos otro indicio que podría demostrar que hay correlación entre Covid19 y ciberdelitos.

4.2.6 Venta Online

DELITOS	**2017**	**2018**	**2019**	**2020**
Delito de acceso sin autorización a datos o programas informáticos	0	0	2	0
Delito de daños en programas informáticos o documentos electrónicos	0	0	0	0
Delito de estafa bancaria por transferencia no consentida mediante manipulación informática o artificio semejante (Art.248.2.a CP)	1	2	213	642
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	0	9	683	1602
Delito de fabricación, introducción, posesión o facilitación de programas de ordenador destinados a cometer estafas (Art.248.2.b CP)	0	0	0	3
Delito de usurpación del estado civil	0	0	20	62
Delito de falsificación de tarjetas de crédito y débito y cheques de viaje	0	1	1	4
Delitos de estafa (Art.248.1 CP)	15	11	484	1480
Total general	**16**	**22**	**1402**	**3789**



DELITOS 2020	TRIM 1	TRIM 2	TRIM 3	TRIM 4
Delito de estafa bancaria por transferencia no consentida mediante manipulación informática o artificio semejante (Art.248.2.a CP)	77	173	177	215
Delito de estafa con tarjetas de crédito, débito y cheques de viaje (Art.248.2.c CP)	294	405	446	457
Delito de fabricación, introducción, posesión o facilitación de programas de ordenador destinados a cometer estafas (Art.248.2.b CP)	1	0	1	1
Delito de falsificación de tarjetas de crédito y débito y cheques de viaje	3	0	0	1
Delito de usurpación del estado civil	12	13	21	16
Delitos de estafa (Art.248.1 CP)	261	377	371	471
TOTAL	**648**	**968**	**1016**	**1161**

El aumento de un 300% durante el año 2020 frente al año 2019, demuestra de una manera patente que no es casual, ese incremento de delitos, siendo una cifra visiblemente notoria. El año de la Covid 19, ha hecho que los ciberdelitos hayan aumentado de una manera sustancial.

5.- DISCUSIÓN

La evolución del delito en el ámbito del ciberespacio, no se puede negar que ha avanzado tal y como se ha podido observar.

Los datos tan significativos del aumento de los delitos en el año 2020 frente al periodo de los años 2017 al 2019, se puede apreciar que probablemente haya una relación directa de la pandemia con los ciberdelitos. Por lo que los informes referidos del aumento de los ciberdelitos, pueden trasladarse a España en el ámbito de Guardia Civil.

Con ello podría quedar demostrado que la hipótesis H1 planteada en este trabajo, en el que propone un aumento de los ciberdelitos denunciados en España, en el ámbito de Guardia Civil es cierta, tal y como queda reflejado en los datos.

Lo referido a la H2 que se propone que no todos los ciberdelitos han aumentado durante la pandemia de Covid19, queda reflejado en los datos obtenidos, tal y como se ha podido testear. Como son los delitos en el que el Medio Empleado son Páginas de Internet, donde la cifra de delitos ha mantenido un crecimiento constante frente a años anteriores. Por otro lado en Modus Operandi, los ataques contra sitio web, han mantenido la misma dinámica de aumento o el Modus Operando por Malware, Ramsonware y Transferencia Bancaria Fraudulenta, donde el aumento ha sido ligeramente superior al incremento lineal.

En lo que respecta a la H3 Los ciberdelitos relacionados con la venta online han aumentado durante la pandemia de COVID-19, podemos decir que tal y como se puede apreciar en el apartado 4.2.6 los delitos en este caso se han triplicado, algo que es muy reseñable y que queda patente esa relación sobre las denuncias en ese tipo de delitos.

Algo que considero que es reseñable respecto a este tipo de ciberdelitos, es esa cifra negra que muy probablemente esté ahí y que debido a diversos motivos pueda existir de una manera sustancial. Hay estafas en tarjetas de crédito, que son

importes tan ínfimos que el coste beneficio de la víctima, podría hacer pensar que no merece la pena trasladarse hasta dependencias policiales por ese importe estafado. La perspectiva debe ser más amplia, ya que si sumamos todas las víctimas que hayan tenido ese importe mínimo, hacen que los estafadores tengan un gran lucro.

Hay que añadir, que durante los meses de marzo y abril de 2020, en el que el confinamiento estricto estaba implantado en España, es posible que muchas personas, no denunciaran muchos hechos delictivos, entre ellos los relacionados con el presente trabajo, por lo que podría haber una gran cifra negra alrededor de esto.

Por otro lado, aquí aporto mi experiencia profesional, en la que casos de cifras elevadas de dinero, no son denunciadas ya sea por vergüenza, o por no creer en el sistema policial.

6.- CONCLUSIONES

La Covid 19 ha incidido de una manera directa en lo que respecta a los ciberdelitos. Como se ha podido ver el aumento durante el año 2020 de ciertos ciberdelitos han tenido un gran incremento significativo, llegando a triplicar el año anterior.

Es importante promover una cultura de alfabetización digital en cuanto a todos los usuarios de las TIC,s. Muchos de los ataques que se realizan a las víctimas, podrían reducirse o minimizarse de una manera sustancial con formación desde a nivel de la escuela, hasta campañas informativas a personas más mayores.

Por otro lado se debería fomentar la cultura de seguridad ya que es necesario conocer las medidas concretas de ciberseguridad, así como los diferentes tipos de estafas que existen.

7.- BIBLIOGRAFÍA

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, *30*(1), 47-88.

Agustina, J. R. (2012). Premisas valorativas y enfoque práctico en la definición de una teoría criminológica: a propósito del modelo antropológico de la teoría de las actividades rutinarias. Revista Electrónica de Ciencia Penal y Criminología.

Agustina, J. R. (2014). Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización. Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización, 143-178.

Akers R., Ronald L., et al. (1979). «Social learning and deviant behavior: A specific test of a general theory». American Sociological Review, 44.

Akers, Ronald L. y Gary F. Jensen (eds.). 2003. Social Learning Theory and the Explanation of Crime: A Guide for the New Century, Advances in Criminological Theory, 11. New Brunswick, NJ: Transaction Publishers.

Andrés, M. B. (2011). La ciberdelincuencia en el Derecho español. *Revista de las Cortes Generales*, 273-305.

Arroyo, S. C. (2020). La Cibercriminología y el perfil del ciberdelincuente. *Derecho y Cambio Social*, (60), 470-512.

Berguer, A., Patchin J.W., & Hinduja S. (2015). Cyberbullying Prevention and Response. Expert Perspectives. Routledge, New York.

Choi, K.S. y Toro-Álvarez, M.M. (2017). Cibercriminología. Guía para la investigación del cibercrimen y mejores prácticas en seguridad digital (Cybercriminology Guide for the investigation of cybercrime and best practices in digital security). Universidad Antonio Nariño, Bogotá.

Cloward, R. A., & Ohlin, L. E. (2013). *Delinquency and opportunity: A study of delinquent gangs*. Routledge.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608.

Cohen, L., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review, 44(4), 588-608.

Cornish, D. B., & Clarke, R. V. (2002). Crime as a rational choice. *Criminological theories: Bridging the past to the future*, 77-96.

Downes, D., y Rock, P. (2012). *Sociología de la desviación: [una guía sobre las teorías del delito]*. Barcelona: Gedisa.

Felgueroso, F., et al. (2020). Aspectos económicos de la crisis del Covid-19. *Boletín de seguimiento*, *3*.

Fontanilla M. Cybercrime pandemic. Eubios Journal of Asian and International Bioethics 30(4), 164-165 (2020)

González, Abel (2016). "Cibercriminología, el futuro está aquí", en Briggs, D., Rámila, J., & Pérez, J.R. (Dirs.). La Criminología de hoy y del mañana. Dykinson, Madrid.

González, AG. (2016). Cibercriminología, el futuro está aquí. In *La Criminología de hoy y del mañana* (pp. 113-128). Dykinson.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

Guilabert, N. G. (2016). Actividades cotidianas de los jóvenes en Internet y victimización por malware. IDP. Revista de Internet, Derecho y Política, (22), 48-61.

Hinduja, S. & Patchin, J.W. (2007). "Offline consequences of online victimization: School violence and delinquency", Journal of School Violence, 6(3), pp. 89-112.

Landau, S. F., & Freeman-Longo, R. E. (1990). Classifying victims: A proposed multidimensional victimological typology. *International review of victimology*, *1*(3), 267-286.

Matsueda, R. L., & Lanfear, C. C. (2007). Differential association theory. *The Blackwell Encyclopedia of Sociology*, 1-3.

Miró, F. (2011). La oportunidad criminal en el ciberespacio. Revista Electrónica de Ciencia Penal y Criminología, 7, 1-07.

Miró, F. (2012). El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio. *El cibercrimen*, 1-332.

Miró, F. (2012). El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio. El cibercrimen, 1-332.

Miró, F. (2013). La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio. Revista española de investigación criminológica, 11, 1-35.

Miró, F. (2021). Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos. *IDP: revista d'Internet, dret i política*, (32).

Ozili, P. K., & Arun, T. (2020). Spillover of COVID-19: impact on the Global Economy. *Available at SSRN 3562570*.

Posada Maya, R. (2017). The cybercrime and its efects in the theory of typicity: from a physical reality to a virtual reality. *Nuevo Foro Penal*, *13*(88), 72-112.

Serrano Maíllo, A. (2009): Introducción a la Criminología. 6ª Ed., Dykinson, Madrid.

Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of research in crime and delinquency*, *34*(4), 495-518.

Stickle, B., Felson, M. Crime Rates in a Pandemic: the Largest Criminological Experiment in History. Am J Crim Just 45, 525–536 (2020).

Wikström, P. O. H., Oberwittler, D., Treiber, K., & Hardie, B. (2017). Situational action theory. In *Developmental and Life-course Criminological Theories* (pp. 125-170). Routledge.

Wilson, J. Q., & Kelling, G. L. (1982). Broken windows. *Atlantic monthly*, *249*(3), 29-38.

Xu, Z., Shi, L., Wang, Y., Zhang, J., Huang, L., Zhang, C., ... & Wang, F. S. (2020). Pathological findings of COVID-19 associated with acute respiratory distress syndrome. *The Lancet respiratory medicine*, *8*(4), 420-422.

7.1 Enlaces Web

Agencia de la Unión Europea para la Cooperación Policial (Europol). Recuperado de la UE el 3 de junio de 2021 de https://europa.eu/european-union/about-eu/agencies/europol_es

Becerra J. (2020) Covid-19: Análisis de los efectos de la pandemia en los fenómenos criminógenos (Criminología ambiental) Recuperado del Diario de Ronda el 06 de marzo de 2021 de https://www.diarioronda.es/2020/07/21/ronda/criminalidad-y-covid-19-analisis-criminologico-de-los-efectos-de-la-pandemia-en-los-fenomenos-criminogenos-criminologia-ambiental/

Campoy P. (2020) ¿Flu-ctuaciones delictivas? Los posibles efectos del COVID-19 en la criminalidad. Recuperado de Revista Española de Investigación Criminológica el 06 de marzo de 2021 de https://criminologia.net/2020/03/23/flu-ctuaciones-delictivas-los-posibles-efectos-del-covid-19-en-la-criminalidad/

Coronavirus disease (COVID-19) Weekly Epidemiological Update and Weekly Operational Update (2021) Recuperado de World Health Organization el 06 de marzo de 2021 de https://www.who.int/emergencies/diseases/novel-coronavirus-2019/situation-reports/

DGT (2021) Los accidentes de tráfico se cobran la vida de 870 personas durante el año pasado. Recuperado de la Dirección General de Tráfico de España el 22 de mayo de 2021 de https://www.dgt.es/es/prensa/notas-de-prensa/2021/Los_accidentes_de_trafico_se_cobran_la_vida_de_870_personas_durante_el_ano_pasado.shtml

European Cybercrime Centre (EC3) Recuperado de la UE el día 3 de junio de 2021 de https://www.europol.europa.eu/iocta-report

Internet Organised Crime Threat Assessment (IOCTA) Recuperado de la UE el día 3 de junio de 2021 de https://www.europol.europa.eu/iocta-report

Manual SPSS. Análisis de las variables categóricas. El procedimiento de tablas de contingencia. Capítulo 12. Universidad Carlos III (Madrid) Recuperado el 7 de abril de 2021 de http://halweb.uc3m.es/esp/Personal/personas/jmmarin/esp/GuiaSPSS/12contin.pdf

Martaviolat. (2020). El perfil del ciberdelincuente: los patrones del mal. Derecho de la Red web. Recuperado el 04/12/2020 de https://derechodelared.com/perfil-ciberdelincuente/

Personas que usan Internet (% de la población) Recuperado del Banco Mundial el 3 de junio de 2021 de https://datos.bancomundial.org/indicator/IT.NET.USER.ZS Portal estadístico de la Criminalidad de la Secretaría de Estado de Seguridad del Ministerio del Interior de España. https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/portal/datos.html?type=pcaxis&path=/Datos1/&file=pcaxis

Serious and Organised Crime Threat Assessment (SOCTA). Recuperado de la UE el día 3 de junio de 2021 de https://www.europol.europa.eu/socta-report#fndtn-tabs-0-bottom-1

SPSS en Wikipedia. Recuperado el 7 de abril de 2021, de https://es.wikipedia.org/wiki/SPSS

Teruel Q. (2020) Ciberdelincuencia en el Código Penal. Recuperado de Cibercrim el día 28 de mayo de 2021 de https://cibercrim.com/ciberdelincuencia-en-el-codigo-penal/