Universidad Internacional de La Rioja (UNIR)

ESIT

Máster universitario en Seguridad Informática

CIBERPOL. METODOLOGÍA PARA LA INVESTIGACIÓN DEL CIBERCRIMEN.

Trabajo Fin de Máster

Presentado por: BARRERA IBÁÑEZ, Silvia

Director/a: MARTÍNEZ GARCÍA, Manuel

Ciudad: Logroño

Fecha: 12/12/2019

Índice de contenidos

Índice de ilustraciones y tablas

Resumen

Si se observa con detenimiento las estadísticas ofrecidas por el Ministerio del Interior sobre los últimos informes sobre cibercriminalidad así como las Memorias presentadas al inicio del año judicial por la Fiscalía General del Estado, en los que se ponen de manifiesto los ratios de esclarecimiento de los delitos cometidos a través de Internet o mediante el uso del mismo, se puede observar un descenso proporcional progresivo lineal claro de los hechos esclarecidos. Si seguimos la tasa lineal de disminución, en el año 2021 habrá un 15% de tasa de esclarecimiento y para el 2025, rondará el 4%.

Simplemente, a través de estas cifras se pueden extraer una serie de conclusiones preocupantes que ponen de manifiesto la disminución de la efectividad en la lucha contra el cibercrimen a la vez que el aumento en las cifras de la cibercriminalidad y su impunidad. Además, los datos estadísticos mencionados no recogen una información lo suficientemente concreta y extensa que permitan describir, clasificar y analizar que está ocurriendo realmente con el cibercrimen y esas preocupantes tasas tan elevadas, de forma que se puedan estudiar, plantear e implementar medidas eficaces contra su lucha.

Si bien es cierto que la patente ventaja técnica está contribuyendo a la impunidad del cibercrimen, es posible aportar soluciones procedimentales de carácter técnico y procesal que pudieran mitigar, y en ciertos casos, solventar aquellas limitaciones que impiden el buen curso de las investigaciones así como el aumento de la mencionada tasa de esclarecimiento.

Por ello, a través del presente trabajo, se pretende realizar una propuesta objetiva de implementación de técnicas y metodologías concretas de investigación para el cibercrimen y mejora de asignación de recursos tanto humanos como técnicos.

Palabras clave: cibercrimen, metodología, investigación, aplicación, ciberpol

Abstract

Looking closely at the statistics offered by the Ministry of Interior on the latest cybercriminality reports as well as the Memoirs submitted at the beginning of the judicial year by the State Attorney General's Office, which show the clarification ratios of the crimes committed through the Internet or through the use of it, a clear linear progressive proportional decrease of the clarified facts can be observed. If we follow the linear rate of decline, in 2021 there will be a 15% clarification rate and by 2025, it will be around 4%.

Simply, through these figures a series of worrisome conclusions can be drawn that highlight the decrease in effectiveness in the fight against cybercrime as well as the increase in cybercriminality figures and their impunity. In addition, the aforementioned statistical data do not collect sufficiently concrete and extensive information that allows describing, classifying

and analyzing what is really happening with cybercrime and these worrying rates so high, so that effective measures can be studied, raised and implemented against fight.

While it is true that the patent technical advantage is contributing to the impunity of cybercrime, it is possible to provide procedural solutions of a technical and procedural nature that could mitigate, and in certain cases, solve those limitations that prevent the good course of investigations as well as the increase of the mentioned clarification rate.

Therefore, this work pretends to make an objective proposal for the implementation of specific research techniques and methodologies for cybercrime and the improvement of the allocation of human and technical resources.

Keywords: cybercrime, methodology, research, application, cyberpol

1. Introducción

1.1 Antecedentes. Evolución de los índices de cibercriminalidad.

Las investigaciones en el mundo virtual están marcadas por variables de carácter técnico que elevan la probabilidad de fracaso. El tiempo, la posibilidad de eliminar los rastros digitales, la multiplicidad de casos que se pueden dar y el delicado tratamiento de las evidencias digitales son variables o factores que siempre han repercutido sobre el buen curso o éxito de una investigación en la Red.

Aunque a veces se realizan todos los esfuerzos por llevar a buen puerto una investigación, es posible que por negligencias, desconocimiento o falta de experiencia tanto del usuario que realiza el reporte o del agente que recibe la información, se pierdan evidencias; datos que, por su propia volatilidad, provocan que la pérdida sea irreversible.

Además, la complejidad de las investigaciones y el uso de cada vez más recursos que dificultan o imposibilitan la navegación y el rastreo en la Red, resultan investigaciones cibernéticas cada vez más complejas y prolongadas en el tiempo. Requieren cooperación internacional, dependen de la información aportada por los proveedores de servicios ajenos, se articulan sobre tiempos judiciales y procesales que no se ajustan a esta realidad delincuencial y las técnicas de ocultación, anonimización o la propia evolución de la Red son cada vez más sofisticadas.

La policía judicial está facultada para llevar a cabo las indagaciones que sean necesarias en la Red siempre que la información a la que acceda sea pública, de la misma forma que se lleva a cabo una inspección ocular en el mundo físico mediante la observación del entorno.

Quizás uno de los momentos más importantes y decisivos del proceso es captar correctamente la información o evidencias digitales de la que se dispone para interponer una denuncia, querella o demanda. Cientos de denuncias son archivadas a diario por falta de información, recursos para identificar los hechos en la Red y concreción en los datos. Las estadísticas, como veremos más adelante, confirman que la ratio entre las denuncias recibidas y los atestados que son enviados a la Autoridad Judicial es de un 20% por lo que el 80% de trabajo ya realizado, se pierde, perdiéndose, en igual porcentaje, la efectividad. Es decir, el procedimiento existente es claramente ineficaz. Veremos por qué.

Las posibilidades de éxito en una investigación se desvanecen con la misma rapidez que los datos existentes en la Red así que desde el momento inicial que se detecten conductas sospechosas, ya se está poniendo en peligro la investigación si se permite cierto lapso de tiempo sin actuar.

Antes de empezar con el proceso de investigación, existe una labor delicada de recopilación y extracción de evidencias digitales. Esta labor consiste en la búsqueda y

obtención de datos personales de fuentes de acceso público o privado en Internet que serán incorporadas a una denuncia, proceso o informe posterior, a modo de declaración testifical o como prueba indiciaria indirecta y que ayudarán al esclarecimiento de los hechos.

Para la elaboración de este trabajo y a falta de menciones, normativas o conclusiones específicas en este asunto, como muchas otras imprecisiones en el tema tecnológico, se mencionarán ciertas referencias de interés que abordan casuísticas similares fruto de la dilatada experiencia personal (y privilegiada) de la alumna desde el año 2006 en su lucha contra el cibercrimen, donde ha podido detectar limitaciones y procesos ineficaces y que hará extensible a la aplicación de la metodología que se está abordando.

En todo caso, las variables de este trabajo lo serán las evidencias digitales, ya sean las aportadas directamente por la víctima o perjudicado así como las obtenidas desde aplicaciones de escritorio, tanto web como móvil, páginas web, redes sociales y motores de búsqueda, tanto de acceso público como dato privado. Todas ellas pueden ser utilizadas a los efectos de investigación e identificación personal.

La información relativa a los proveedores de servicio que haya sido obtenida a posteriori como consecuencia de los subsiguientes requerimientos oficiales policiales o judiciales no podrá ser incorporada a la plataforma que se va a proponer pues de lo que se trata es de recoger solo aquello disponible y que puede ser susceptible de tratamiento sin revelar fuentes o datos obtenidos procedentes de informes de carácter personal o confidencial, vulnerando el secreto profesional y poniendo en riesgo la legitimidad de las investigaciones. Abordaremos la metodología desde su fase inicial que es la recolección de las evidencias, donde se produce el gran cuello de botella y la pérdida de ese 80% de las investigaciones.

No se va a profundizar en temas jurídicos más que lo necesario para el objetivo del presente trabajo, sin que ello sea óbice para la mención necesaria de aquellos a tener en cuenta si están relacionados con la privacidad y el tratamiento de la información y sus límites legales, sobre todo, si no queremos confundirnos con otros conceptos.

Por otra parte, hay que tener cuidado con el tratamiento o uso de información digital en el ámbito penal, el derecho de información y la obtención lícita de datos personales de la Red sin vulnerar la intimidad de terceros y por tanto, sin necesidad de autorización judicial, de modo que la prueba obtenida para un procedimiento no sea declarada nula y pueda servir de cara al desarrollo de la metodología y la plataforma.

El hecho de que esté incidiendo tanto en la importancia, la certeza, los medios y la legalidad de la identificación de personas a través de fuentes abiertas no es por capricho. El uso frecuente de los sistemas de anonimización como los enrutamientos de TOR, los *proxies*, las VPN (redes privadas virtuales), la tecnología NAT empleada por los dispositivos móviles, etc. cuestionan la identificación de un usuario únicamente por titularidad de dirección IP. Por

otro lado, los plazos judiciales imposibles y otras dificultades para obtener la evidencia digital por los motivos que se han ido exponiendo, hacen plantearse lo siguiente.

La dificultad técnica a la hora de establecer conexiones de red y atribuir su titularidad a un usuario concreto unido a la masiva implantación de dispositivos informáticos conectados a la Red, (nos referimos a los *smartphones*, y no a los 11.000 millones de IoT) están invirtiendo el peso de la validez legal de la obtención de una dirección IP en favor de los diferentes indicios que permitan la identificación de una persona en la Red dejados por su rastro *online*.

Se está pasando de buscar una dirección IP utilizada por un usuario, que también y según qué casos, puede contribuir a una identificación, a seguir el rastro o huella *online* que los usuarios hemos ido conformando durante estos últimos años.

Hace una década esto era impensable con las pocas referencias o inexistentes a datos identificativos en la Red. Ahora, es precisamente la riqueza de los datos y la utilidad de su explotación lo que permite el planteamiento de la plataforma y la consiguiente metodología. El avance del mundo virtual, la aparición y uso de redes sociales y la infinidad de servicios digitales que ya se están ofreciendo en Internet, provocan la impronta de una huella digital, y por consiguiente, un posible rastro digital bastante prolijo.

Si defendemos la propia idiosincrasia de la red, no podemos asimilar su funcionamiento al mundo físico. Partiendo de ese hecho y de que cada vez son más los rastros de navegación y huellas *online* presentes en la Red los que pudieran ser tomados en consideración por la autoridad judicial y valorados como prueba anticipada para la determinación de autorías, no deberían desecharse indicios por el mero hecho de que existan motivos técnicos que lo cuestionen y más, si existen otras pruebas de cargo aportadas que refuercen una acusación. De hecho, ya hay sentencias en este sentido. Ahora más que nunca, se advierte una ventaja que debe ser explotada por los agentes investigadores a través de una plataforma que los recoja y explote a través de la metodología que se va a plantear.

Por tanto, la identificación de perfiles por fuentes abiertas tiene dos utilidades muy valiosas durante el proceso de investigación. Por una parte, constituye una diligencia de investigación reveladora que permite indagaciones posteriores. En una investigación, no es lo mismo disponer de un único pseudónimo como punto de partida que obtener números de teléfono, domicilios postales, descripciones físicas, ubicaciones posteriores, de las cuales se pueden derivar en resultados esclarecedores.

Por otra parte, una identificación cuasi o completa de una persona es una prueba indiciaria directa. En el segundo caso, lograr una identificación de la titularidad de un perfil directamente a través de su búsqueda en fuentes abiertas, perfectamente motivada y razonada, ha servido para que haya sentencias condenatorias como así ha podido comprobar esta alumna durante juicios a los que ha asistido en calidad de testigo, habiendo sido la instructora de las propias investigaciones.

En este sentido y por último, finalizamos con un ejemplo práctico. Ya hay sentencias que disponen la suficiencia de la prueba presentada relativa a las identificaciones llevadas a cabo por los diferentes indicios provenientes de fuentes abiertas mediante proceso deductivo como afirma la reciente sentencia del 19 de julio de 2016 de la Sala de lo Penal número 24/ 2016 de Audiencia Nacional y que pasamos a comentar.

En este procedimiento, la defensa del acusado identificado responsable negaba la autoría de su defendido criticando la falta de pruebas, aduciendo que todo eran suposiciones policiales. El tribunal negaba esta suposición ya que, además, en ese caso, dos equipos de investigación (de diferentes cuerpos policiales) alcanzaron la misma conclusión inequívoca sobre la identidad del responsable directo.

En la identificación llevada a cabo a través de una cuenta de Twitter, el acusado interactuaba con familiares y éstos con él a través de sus cuentas en redes sociales, ofrecía sus datos personales e insertó imágenes de su propia persona realizadas a través de Periscope.

1.2. Justificación del estudio.

El desconocimiento del ámbito de la cibercriminalidad y de los retos que plantea por parte del Estado y los correspondientes órganos administrativos y policiales, está provocando una falta de dotación de recursos, tanto humanos como técnicos para su afrontamiento. En consecuencia, se ha generado un notable estancamiento en la evolución de la técnica y el enfoque que requiere el surgimiento de nuevas formas de criminalidad y los procedimientos forenses de obtención de evidencias y pruebas en el mundo digital.

Ello es debido, no solo al elevado y constante esfuerzo que requiere la actualización de técnicas y procedimientos en la ciberinvestigación, sino al impacto que el cibercrimen genera en el ciudadano y la víctima, no percibiéndose la inseguridad y el riesgo de forma directa. La falta de alarma social y el poco impacto "físico" generado a nivel social han relevado este tipo de criminalidad a "criminalidad de segunda", no siendo, por tanto, una prioridad a nivel político ni policial, con el impacto que ello genera, sobre todo a la hora de destinar recursos.

Además, y también en parte, sus víctimas directas contribuyen al encubrimiento del cibercrimen, teniendo al mundo empresarial como su mejor ejemplo. Desde hace años, la empresa viene ocultando los incidentes sufridos, las brechas de información o las situaciones que han comprometido su seguridad por temor a miedos reputacionales, pérdidas económicas o desconfianza de sus clientes. Hay cientos de ejemplos donde solo gracias a los medios de comunicación y las redes sociales, hemos podido conocer que la ciberseguridad de una entidad pública o privada había sido vulnerada, no constando puesta en comunicación de las autoridades públicas ni tampoco a sus clientes.

Si bien es cierto que, desde la aprobación de normativas como el RGPD, que obligan a la notificación de incidentes ante el órgano administrativo competente, parece que esta situación está empezando a revertir, los cambios de mentalidad, por el momento, se están produciendo muy lentamente y los progresos son escasos.

Por otro lado, los ciudadanos tampoco contribuyen a visibilizar este fenómeno criminológico en creciente aumento. Según estudios[1] de la empresa de ciberseguridad mundial Norton, el 43% de las víctimas encubren estos hechos por miedo a represalias, victimización, vergüenza, impotencia o porque, simplemente, creen que la situación de víctima ha sido generada por ellos mismos.

Y los datos ofrecidos por los informes estadísticos del Ministerio del Interior, encargados de la persecución de la criminalidad informática son un claro ejemplo de la situación existente y la necesidad acuciante de poner en marcha medidas y procedimientos

[1] https://www.nortonlifelock.com/content/dam/nortonlifelock/docs/about/2017-ncsir-global-results-en.pdf

que garanticen un afrontamiento de esta problemática delincuencial de forma concreta y efectiva.

Según el último informe del Gabinete de Coordinación y Estudios del Ministerio del Interior[2], teniendo en cuenta la totalidad de infracciones penales registradas en el 2018 y el estudio de cibercriminalidad de 2018[3] del Ministerio de Interior, se han registrado 540.786 delitos cometidos en el mundo analógico o físico sobre un índice de criminalidad total de 1.025.863 delitos. 583.401 Hechos se han definido como "Resto de infracciones penales", como si fuera una partida residual. Este dato es igual de relevante que de preocupante ya que ese "Resto de infracciones" supone una cifra aun mayor que las identificadas.

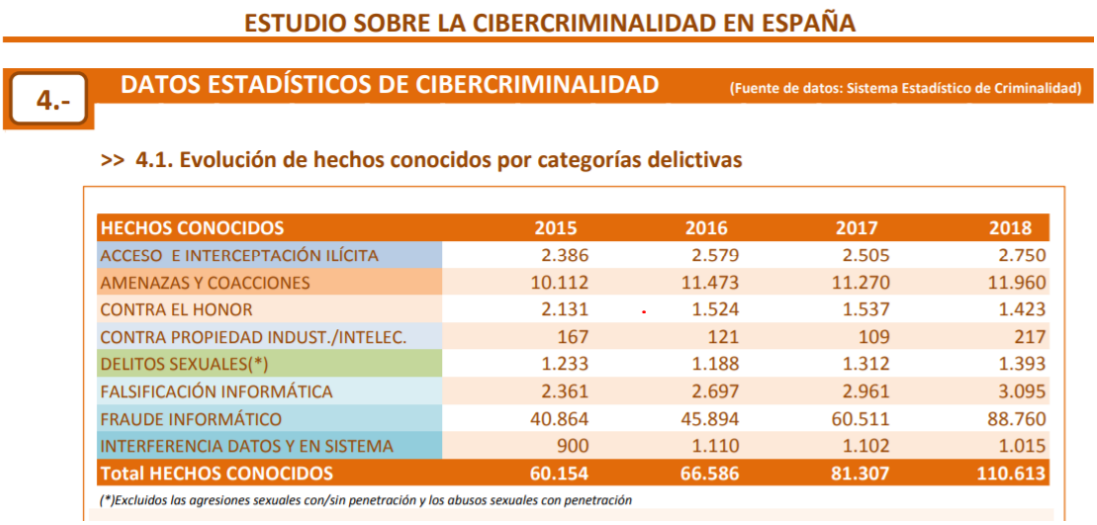
Esto significa que se está obviando o ignorando la etiología del 57% de las infracciones contabilizadas incluso, superando ya a las infracciones sí clasificadas por tipologías de la delincuencia tradicional. Por tanto, en este sencillo reporte se está poniendo de manifiesto el nulo interés por determinar el origen y causa de esa criminalidad "oculta" y menos aún, el interés policial en iniciar nuevas políticas para combatir nuevas formas de criminalidad.

Según el mismo estudio de cibercriminalidad, 110.613 infracciones se refieren a diferentes tipologías. En este informe se confirma el ascenso proporcional del 20% cada año de hechos denunciados, habiéndose casi duplicado en los 4 últimos años.

En ambos informes no se ha incluido de forma específica los hechos denunciados calificados como delito de acoso a mayores y menores de edad, infecciones por malware, la conocida como *sextorsion,* delitos contra la intimidad como descubrimiento y revelación de secretos, o las suplantaciones de identidad o usurpación del estado civil en la Red, denunciados habitualmente. Es por ello que cabe pensar que estos mismos conforman una parte considerable de la cifra expresada de 540.786, aun no especificada.

[2] http://www.interior.gob.es/documents/10180/9814700/informe+balance+2019+2%C2%BA%20trimestre.pdf/a21e6daf-c6c4-4b2b-9c11-5ec15cd57954

[3] http://www.interior.gob.es/documents/10180/8736571/Informe+2018+sobre+la+Cibercriminalidad+en+Espa%C3%B1a.pdf/0cad792f-778e-4799-bb1f-206bd195bed2



ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

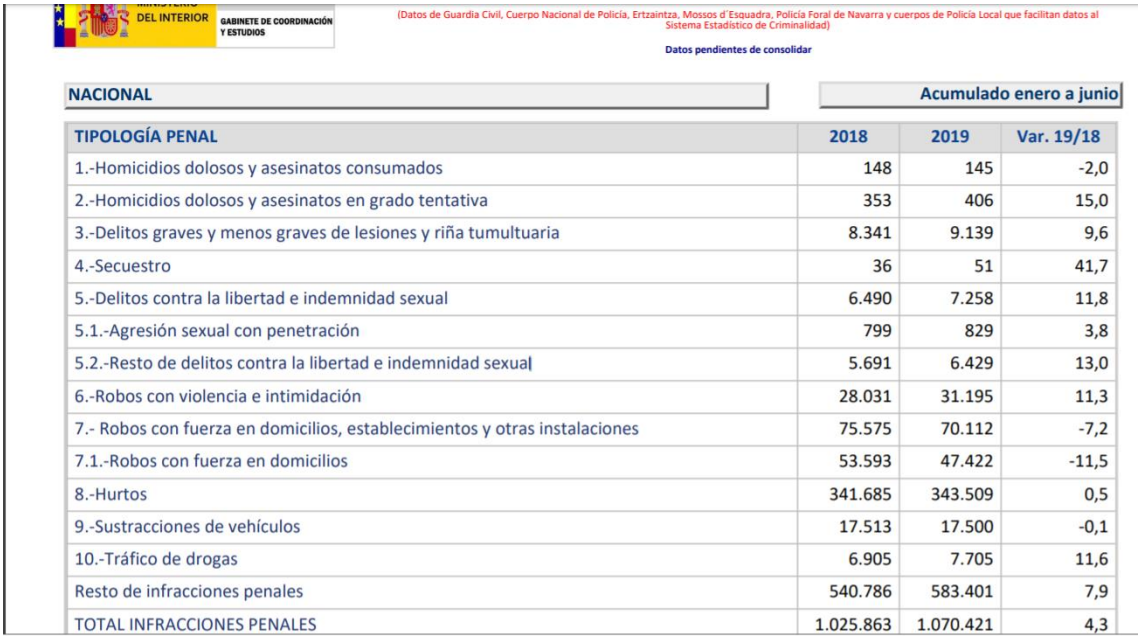
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD (Fuente de datos: Sistema Estadístico de Criminalidad)

>> 4.1. Evolución de hechos conocidos por categorías delictivas

HECHOS CONOCIDOS	2015	2016	2017	2018
ACCESO E INTERCEPTACIÓN ILÍCITA	2.386	2.579	2.505	2.750
AMENAZAS Y COACCIONES	10.112	11.473	11.270	11.960
CONTRA EL HONOR	2.131	1.524	1.537	1.423
CONTRA PROPIEDAD INDUST./INTELEC.	167	121	109	217
DELITOS SEXUALES(*)	1.233	1.188	1.312	1.393
FALSIFICACIÓN INFORMÁTICA	2.361	2.697	2.961	3.095
FRAUDE INFORMÁTICO	40.864	45.894	60.511	88.760
INTERFERENCIA DATOS Y EN SISTEMA	900	1.110	1.102	1.015
Total HECHOS CONOCIDOS	60.154	66.586	81.307	110.613

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

Figura 1. Estudio sobre la cibercriminalidad en España de 2018.
http://www.interior.gob.es/documents/10180/8736571/Informe+2018+sobre+la+Cibercriminalidad+en+Espa%C3%B1a.pdf/0cad792f-778e-4799-bb1f-206bd195bed2



DEL INTERIOR GABINETE DE COORDINACIÓN Y ESTUDIOS

(Datos de Guardia Civil, Cuerpo Nacional de Policía, Ertzaintza, Mossos d´Esquadra, Policía Foral de Navarra y cuerpos de Policía Local que facilitan datos al Sistema Estadístico de Criminalidad)

Datos pendientes de consolidar

NACIONAL — Acumulado enero a junio

TIPOLOGÍA PENAL	2018	2019	Var. 19/18
1.-Homicidios dolosos y asesinatos consumados	148	145	-2,0
2.-Homicidios dolosos y asesinatos en grado tentativa	353	406	15,0
3.-Delitos graves y menos graves de lesiones y riña tumultuaria	8.341	9.139	9,6
4.-Secuestro	36	51	41,7
5.-Delitos contra la libertad e indemnidad sexual	6.490	7.258	11,8
5.1.-Agresión sexual con penetración	799	829	3,8
5.2.-Resto de delitos contra la libertad e indemnidad sexual	5.691	6.429	13,0
6.-Robos con violencia e intimidación	28.031	31.195	11,3
7.- Robos con fuerza en domicilios, establecimientos y otras instalaciones	75.575	70.112	-7,2
7.1.-Robos con fuerza en domicilios	53.593	47.422	-11,5
8.-Hurtos	341.685	343.509	0,5
9.-Sustracciones de vehículos	17.513	17.500	-0,1
10.-Tráfico de drogas	6.905	7.705	11,6
Resto de infracciones penales	540.786	583.401	7,9
TOTAL INFRACCIONES PENALES	1.025.863	1.070.421	4,3

Figura 2. Datos estadísticos sobre infracciones penales de 2018. Gabinete de Coordinación y Estudios
http://www.interior.gob.es/documents/10180/9814700/informe+balance+2019+2%C2%BA%20trimestre.pdf/a21e6daf-c6c4-4b2b-9c11-5ec15cd57954

Por los datos expuestos con anterioridad, bastante significativos, y la práctica policial de esta alumna durante casi 15 años en ciberinvestigación, se puede concluir que el sistema de investigación actual es eficaz ni existen políticas de seguridad criminal orientadas a combatir los delitos cometidos en el ciberespacio. De hecho, por lo que se puede ver, la intención, por el momento, es no mostrar los datos reales sobre este problema.

Además, esta alumna, basándose en la experiencia adquirida durante ese tiempo en el que campo de la investigación del cibercrimen, en la que ha tenido oportunidad de

desarrollar y participar en decenas de investigaciones con implicación nacional e internacional, ha podido identificar los siguientes problemas y/o carencias:

- La falta de un sistema o aplicación concreta que permita la obtención concreta y guiada de evidencias digitales durante el proceso. Esta carencia provoca que muchas de las mismas no se detallen o se pierdan, simplemente, por su alta volatilidad y riesgo de pérdida, borrado o destrucción.
- Inexperiencia y falta de formación de agentes especializados en la recepción e investigación de la criminalidad informática que provoca la recepción y elaboración de manifestaciones de hechos o denuncias de los ciudadanos estén incompletas e inexactas o erróneas.
- La falta de unanimidad de criterios en las toma de denuncias y de una metodología concreta que provoca la incorrecta identificación de los hechos criminales, dando lugar a esas "Otras infracciones" o a que se identifiquen hechos de similares características, como por ejemplo, en la estafa, que den lugar a causas separadas que no ponen de manifiesto la entidad real y el alcance de la actuación de los autores y, por tanto, sea más difícil su persecución policial y judicial, sintiéndose impunes.
- Descoordinación entre las diferentes demarcaciones policiales, investigándose denuncias con idénticos autores, y realizándose, por ello, comprobaciones similares, ocasionando duplicidades en el trabajo.
- Víctimas que, pese a la obligación, no ponen en conocimiento de las autoridades los presuntos hechos delictivos porque no creen en la efectividad del sistema de investigación ni en que puedan ser resarcidos del prejuicio ocasionado por el cibercrimen.

A modo de ejemplo ilustrativo, y como reflejo de las graves deficiencias por la carencia de una metodología efectiva y eficiente en la lucha contra el cibercrimen, vamos a exponer dos de las investigaciones instruidas por esta alumna.

La denominada "Operación Siglo XXI"[4] o el timo de las revistas de policia, en el que se empleaban webs maliciosas como reclamo, se investigó una estafa masa continuada a través de la supuesta edición de revistas policiales donde fueron halladas en la contabilidad de los registros más de 15.000 víctimas, 15 millones de euros de beneficios ilegítimos y el fraude continuado de sus autores durante 14 años. En los registros policiales de denuncias así como en las bases de datos internas, solo se identificaron siete denuncias interpuestas.

[4] https://www.lasexta.com/noticias/sociedad/detenidas-personas-macroestafa-millones-euros-mas-150000-victimas_201409175725ead24beb28d44601c0a7.html

De igual forma, la estafa masa y continuada de un casino online español 21 Kbet[5], en el que se identificaron más de 400 víctimas por un fraude de 500.000 euros, solo se pudieron localizar cuatro denuncias relacionadas con los hechos.

En este trabajo, por los objetivos concretos que se persiguen y la extensión del mismo, no se va a incluir la valiosa contribución del analista forense. Si bien es cierto que la figura de este agente es determinante en la obtención de evidencias digitales, su trabajo no se circunscribe solo al ámbito del cibercrimen. De hecho, la participación de estos expertos forenses se suele producir en la fase avanzada de la instrucción de las diligencias o el procedimiento judicial, ya sea en la extracción de evidencias durante la entrada y registro así como en momentos concretos a modo de informes técnicos o peritajes. Por ello, no se van a incluir en el presente trabajo, dado que nos vamos a centrar en la fase de aportación por el usuario- denunciante y la recopilación previa de información por parte de los agentes, donde se aprecia la mayor pérdida significativa de información.

En un mundo ideal donde el valor de la evidencia digital fuere tomado en consideración, se podría diseñar otra metodología de procedimiento para tratar la información recopilada tras la operativa policial y convertirla en inteligencia, o lo que es lo mismo, aprovechar la información obtenida de las evidencias para obtener datos de interés para la investigación. Aunque parezca tarea sencilla, nada más lejos de la realidad, posiblemente se trata de la tarea más complicada y que más recursos tanto humanos como técnicos precisa. En una sola operación policial se pueden extraer varios terabytes de información en bruto, información que hay que tratar para poder determinar cuál es de interés y cual no. Lo más apropiado y dada la especialización y volumen de información a tratar, lo más práctico para realizar esta tarea sería utilizar software especializado capaz de automatizar el tratamiento de la información para extraer solamente los datos que son de interés.

[5] https://elpais.com/politica/2014/06/13/actualidad/1402647945_476524.html

1.3. Planteamiento del trabajo.

A través del presente trabajo, en primer lugar se pretende identificar de forma concreta aquellas limitaciones técnicas y procedimentales que pueden constituirse en variables de análisis y tratamiento de un problema. No se puede plantear una metodología si antes no entendemos cómo funciona un procedimiento y las limitaciones que plantea, algunas de ellas insalvables como el uso de todo tipo de conocimientos y habilidades para evitar ser descubiertos o eliminar indicios.

Se sabe que el mundo virtual ofrece más técnicas para obstruir conscientemente la labor investigativa y facilitar la impunidad que el mundo físico. Algunas de estas herramientas son el uso de las redes TOR, las redes virtuales privadas o los *proxies*. Además, el anonimato inicial, las conexiones hombre-máquina identificadas a través de la dirección IP, las limitaciones legales y procedimentales, la falta de formación de personal policial especializado, la internacionalización del cibercrimen, descoordinación entre países y baja o nula colaboración de los proveedores de servicios de Internet están resultando las preocupantes cifras.

Después, veremos que con el planteamiento de esta metodología, se podrán mejorar ciertos procedimientos policiales como identificar con mayor exactitud comportamientos criminales en la Red, reducir ese cuello de botella tan elevado del 80% de denuncias archivadas, sobre todo por fallos en la identificación y recolección de la evidencia digital en la fase de reporte o puesta en conocimiento de las autoridades y mejorar la efectividad del trabajo policial, al reducir la demanda de denuncias en las oficinas de atención al ciudadano (que suponen ya un 60% de las denuncias).

Tras hacer una exposición del estado actual del proceso e identificar las limitaciones, vamos a realizar una propuesta objetiva de implementación de una metodología concreta que se centrará en la propuesta de un aplicativo sencillo para el momento clave de la recepción de la información de los hechos reportados y su posterior investigación, mejorando la asignación de recursos tanto humanos como técnicos ya existentes.

La Dirección General de Policía y otros cuerpos policiales encargados de la represión del delito y el esclarecimiento de infracciones penales ya poseen aplicaciones integradas en sus redes corporativas que sirven para la recepción de denuncias y tramitación de diligencias policiales de investigación. Pero estas aplicaciones están adaptadas a la necesidades procedimentales de la represión del delito tradicional, en el mundo físico o analógico, concretando aquellos aspectos de determinadas tipologías como el robo con violencia, la sustracciones de vehículos donde se solicitan de forma concreta la descripción y características físicas de determinados autores, el número de matrícula y bastidor de un vehículo, o el número de serie de objetos robados. Pruebas o evidencias, todas ellas sin las

cuales nadie en su sano juicio no considerarían como obvias de obtener si queremos recuperar un vehículo robado, unas joyas o identificar a un atracador por sus características físicas o el arma de fuego utilizada.

Sin embargo, por muy lógico y obvio que puedan resultar estas apreciaciones, la ignorancia, el desconocimiento real de problema, el funcionamiento del ciberespacio y la falta de experiencia, hacen que estos mismos aplicativos de recepción de denuncias no se hayan adaptado aun a las necesidades reales investigativas, llegando a manos de los investigadores denuncias de cuatro líneas en los que se explicitaba lo siguiente: “que una persona había sufrido una estafa al alquilar un apartamento pesando que lo estaba haciendo a través de la famosa plataforma de reservas de inmuebles AirBnB y, sin embargo, al contactar con éstos, le informaron que estaba operando en una web desconocida no perteneciente a la mencionada web.

A día de hoy, con estos datos, e igualmente extensible a otras muchas más situaciones, se pretende que el ciberinvestigador pueda ubicar un recurso, es decir la web exacta, o algún dato más sobre los autores cuando han empleado una web falsa de cuyo dominio no se dispone, porque el agente ni el usuario han sido formados para ello y desconocen que ese sería un dato decisivo para la investigación, al menos para tener un punto de partida del que partir. Sorprendentemente, y a pesar de la obviedad, ninguno de esos datos consta en la denuncia.

Este es el día a día del delito tecnológico y la dura realidad de una criminalidad que no hace más que aumentar en un 20% y de la que aun no se ha propuesto ni siquiera unas líneas o bases metodológicas desde las que partir o una asignatura obligatoria que enseñar en las escuelas de formación de los futuros agentes.

Por ello, a través de la propuesta de este trabajo, se va a exponer un sencilla metodología, a través de una aplicación de recepción de hechos en ciberespacio, en las fases previas de la intervención policial, que permita la obtención de la información concreta y necesaria en cada caso, discrimine por suceso o hecho delictivo, permita un empleo más eficaz de los recursos humanos y técnicos y permita, a través de la posterior estadística, ofrecer resultados más concretos y datos más acertados y cercanos a este tipo de realidad delincuencial.

1.4. Estructura de la memoria

La memoria consta de cuatro partes destacables. La primera de ella, referida a la explicación técnica y procedimental de la investigación del cibercrimen, exponiendo por qué la lucha contra esta criminalidad supone un reto, con una exigencia mayor de recursos humanos y técnicos la verdadera implicación de los actores policiales en su lucha.

La segunda, la concreción de unos objetivos generales y específicos que pondrán de manifiesto la ganancia en efectividad y empleo de recursos técnicos y humanos en la lucha contra el cibercrimen tan solo estructurando la lucha contra el cibercrimen con una nueva metodología y un aplicativo sencillo.

En el tercer apartado se expondrá una metodología que centrará el grueso de la exposición en un aplicativo que hemos denominado “CIBERPOL” y que no es más que una plataforma para la recepción de información sobre hechos presuntamente delictivos de los ciudadanos que redundará en una mayor eficacia para una posterior investigación. Se planteará un estudio de caso sencillo en el que se expondrá un ejemplo de una denuncia actual y en el sistema de tratamiento de la misma en el día a día actual y el avance que supondría para la eficacia policial hacerlo a través de la metodología planteada o similar.

Por último, se mencionarán posibles desarrollos evolutivos de la herramienta para una mejora de la eficacia y explotación de la información así como el que se posibilite la investigación de casos de mayor envergadura, permitiendo detectar y luchar contra las verdaderas organizaciones que subyacen a todo este negocio criminal y no sean consideradas sus acciones como aisladas.

2. Contexto. Análisis de las limitaciones en la investigación tecnológica.

Qué mejor forma de ponernos en contexto que repasar, en líneas generales, cuál es el proceso investigativo del cibercrimen, sin entrar a especificar cada una de las especialidades, que sí serán tenidas en cuenta a la hora de abordar la metodología en concreto. De esta forma podremos conseguir una mayor comprensión del contexto y la necesidad del planteamiento del presente trabajo.

2.1. Tipo de hecho, clasificación de la infracción penal y cauce de la denuncia.

Algo tan básico como catalogar un suceso y cuál empieza siendo ya una dificultad. Ni el ciudadano ni el agente están familiarizados con los tipos penales y su encuadre en la realidad. De hecho, algunos comportamientos delictivos lo son solo desde hace cuatro años por lo que ¿Cómo vamos a abordar un problema delincuencial si no somos capaces de detectarlo y calificarlo correctamente?

Al iniciar una investigación tenemos que considerar tres cuestiones iniciales:

1. Tipicidad de la conducta. Los hechos denunciados ¿Constituyen infracción penal? Aunque parezca una obviedad, es la primera y más importante pregunta que debemos realizarnos. En el campo de las redes sociales, más concretamente, podemos encontrar infinidad de contenidos que si bien son reprobables o moralmente reprochables, no son delito según lo previsto en nuestro Código Penal. Éstas son las que se conocen con el nombre de conductas alegales que en principio no pueden perseguirse penalmente, tales como las apologías y deben ser diferenciadas de las ilegales, que sí conllevan un reproche penal.

También puede haber diferencias jurídicas a la hora de abordar las suplantaciones de identidad, que a diferencia de muchos países de la Unión Europea, en España no constituyen un delito por sí mismos. Es decir, una suplantación de identidad sería delictiva cuando hubiese sido empleada con el fin de cometer otro delito, por ejemplo para consumar una estafa se suplanta la identidad de otra persona y así se constituye el engaño bastante o en los delitos de pornografía infantil, se suplanta la identidad de un menor para poder acceder a la víctima.

2. Acceso a medios de prueba. Una vez que tenemos claro que la conducta investigada es delictiva, podemos pasar a la segunda fase: los medios de prueba. No siempre vamos a poder demostrar que un hecho penal se ha cometido realmente y aunque consigamos probarlo, esto no garantiza que podamos identificar y localizar al responsable. Esto es así debido a la volatilidad de la información difundida en la Red y la facilidad para borrar, alterar o eliminar los vestigios que se generan, dificultando así las investigaciones policiales.

En primer lugar hay que tener en cuenta cuándo tuvieron lugar los hechos, ya que a mayor tiempo, más posibilidades de que desaparezcan las evidencias, es decir, más probabilidad de que se haya eliminado, borrado el vestigio objeto del delito, la compañía proveedora de servicios haya eliminado el contenido por contravenir sus normas o reportado

por algún usuario o haya pasado demasiado tiempo y las compañías de telecomunicaciones ya no guarden datos técnicos de las conexiones investigadas.

Si para evitar que los vestigios desaparezcan, en el mundo analógico preservaríamos la escena del crimen, en el mundo virtual también. Es de vital importancia que, en el momento en el que detectemos los hechos delictivos, preservemos la escena, para lo cual debemos solicitar la salvaguarda de contenidos a la proveedores, mediante servicios de *timestamping*, capturas de pantalla, copiado, filtrado o volcado de información, descargas de videos, documentos, etc. Con esto, evitaremos perder la información cuando los autores de los hechos investigados traten de borrar su rastro deshaciéndose de las pruebas generadas.

3. Dónde judicializar. Si hemos llegado a esta cuestión es porque hemos resuelto con éxito las dos anteriores. Una vez en este punto, lo primero que debemos preguntarnos es ¿Dónde han tenido lugar los hechos? Si la respuesta es fuera de España, tenemos dos opciones, abandonar la investigación antes de empezarla o según la gravedad del delito solicitar una Comisión Rogatoria Internacional. En la mayoría de los casos no es eficaz destinar recursos y esfuerzos porque se trata de un procedimiento largo y costoso. Tampoco suele concederse esta solicitud de auxilio judicial por delitos menos graves o leves como en muchos casos están penados los delitos cometidos a través de Internet. Por lo tanto, y dado que los recursos son muy limitados, deberemos ser muy selectivos a la hora de abordar una investigación ubicada, presumiblemente, en el extranjero y destinarla para casos de mayor entidad o gravedad.

Si los hechos han tenido lugar en España, entonces hay que reformular la pregunta, ¿en qué localidad? y ¿qué juzgado es competente? Una de las peculiaridades de la Red es que es un medio global, es decir los hechos no se cometen en un lugar concreto, sino en Internet, es decir, en varios lugares con efectos también en diferentes territorios. En ausencia de este dato, debemos fijarnos en el lugar donde se encuentra el responsable y judicializarlo en esa demarcación. Sin embargo, no siempre conocemos este dato, en cuyo caso trataremos de dirigirnos a los juzgados de lugar de residencia de la víctima, o si hay más de una, donde se encuentre la primera de ellas.

Aun así, habiendo judicializado en el Juzgado correcto, siempre cabe la posibilidad de que aparezca en mitad del proceso, una denuncia anterior interpuesta en otro lugar en base a lo cual el Juzgado tratará de inhibirse en esa demarcación, lo que supondrá un límite considerable en la investigación.

Por otro lado, existe poca jurisprudencia en relación a estos delitos, ya sea por su novedad y, en muchos casos, reciente tipificación. De ello se deriva que los mismos hechos tengan una repercusión completamente diferente dependiendo del juzgado que asuma la competencia, hasta el punto que uno puede no incoar diligencias y proceder al sobreseimiento de la causa y en otros, solicitar calificaciones provisionales que conllevan penas de prisión.

Después, pasaremos a la siguiente fase: qué tipo de investigación vamos a llevar a cabo.

El modo de iniciar una investigación suele ser común para casi todos los delitos en la Red. Una vez se tiene conocimiento de unos hechos que presuntamente podrían ser delictivos por denuncia, se inician una serie de gestiones tendentes a la comprobación de los mismos y al descubrimiento del autor.

En primer lugar, podemos diferenciar dos tipos de investigaciones:

1. Identificación por fuentes abiertas. Se trata de identificar al autor de los hechos a través de fuentes abiertas, a partir de los datos iniciales de los que se dispone y se han recopilado. Si se consigue una buena identificación y no existen dudas razonables, se procede a la detención del responsable y se pone a disposición judicial junto al atestado y a las pruebas correspondientes.
2. Identificación por mandamiento judicial. Esta modalidad suele darse por dos razones fundamentales. Bien porque no se consigue una identificación plena por fuentes abiertas o bien porque la investigación es complicada y es preciso obtener los datos técnicos que asocien sin ningún género de dudas una dirección IP con el hecho delictivo investigado. En ambas situaciones se elabora el correspondiente atestado solicitando a la autoridad judicial mandamiento para que las proveedoras de servicios faciliten las direcciones IP desde las que en una fecha y hora determinada se produjo una conexión a Internet, conexiones relacionadas con la comisión de los hechos que se investigan. Las compañías telefónicas nos darán el nombre o nombres de las personas que tienen asociada esa dirección IP en las fechas concretas, por lo que se consuma la identificación y así se puede proceder a la detención y puesta a disposición judicial.

Por lo tanto, es posible que la localización del hecho se pueda determinar al inicio o bien, si no se dispone de esa información, será, inicialmente, el domicilio de la persona que denuncia. En el caso de los fraudes, es más fácil localizar el hecho, pues los cargos fraudulentos en una tarjeta de crédito determinarán un lugar concreto o el domicilio del destinatario de las transferencias fraudulentas realizadas a una determinada cuenta.

2.2. Anonimizadores, protocolos de comunicación, direcciones IP y nateado de red.

La navegación anónima supone un problema añadido para las investigaciones, entendiendo como tal no solamente la navegación a través de redes como TOR, sino también el uso de medidas de seguridad que dificultan o imposibilitan la identificación. El uso de un proxy a la hora de conectarse a Internet, por ejemplo, hace anónima la navegación ya que no se puede obtener ningún dato de conexión. Lo mismo sucede cuando nos conectamos a través de una VPN. En estos casos, solo se puede identificar a los autores de los hechos

delictivos investigados aprovechando las vulnerabilidades del sistema o confiando en que exista algún error humano que revele, en un descuido del autor, la verdadera dirección IP desde la que se está conectando. Esto es el caso de delincuentes profesionales que hacen del cibercrimen su modus vivendi, lo que se conoce como el *Crime as a Service* (CaaS) y que dejan finalmente, para fortuna de los investigadores, una prolija huella online con mayores posibilidades de trazabilidad digital. Por ello, en este tipo de casos, cada conexión es importante y debemos revisar cada una de ellas de forma pormenorizada.

Como seguramente es de imaginar al hablar de delitos tecnológicos, uno de los principales datos que más se necesita conocer es la titularidad de una dirección IP, es decir, averiguar a qué persona se le asignó una dirección IP en un momento concreto. Para particulares, normalmente las direcciones IP se asignan de forma dinámica, es decir, un usuario cuando se conecta a internet, no tiene por qué tener siempre la misma dirección IP pública, si no que esta puede cambiar según la demanda de la propia compañía, y no solo eso, actualmente con la escasez de direcciones IP públicas tipo v4, existen compañías telefónicas que tienen más clientes que direcciones IP públicas contratadas (las compañías telefónicas disponen de un rango limitado de direcciones IP públicas para asignárselas a sus clientes, y en función del tipo de compañía que sea, dispondrá de más o menos direcciones IP para utilizar).

Estas compañías telefónicas que tienen muchos más clientes contratados que direcciones IP disponibles para asignar, hacen uso de la tecnología NAT, esto es, la asignación de una misma dirección IP pública a miles de clientes distintos, con la salvedad de que a cada uno de esos clientes se le asignará un puerto de conexión único para que se conecten a internet, por lo que hay que tener en cuenta este factor a la hora de gestionar direcciones IP tipo NAT dentro de una investigación.

A la hora de solicitar las titularidades de las direcciones IP desde las que se llevan a cabo los hechos delictivos es importante aportar el puerto, si lo conocemos, ya que hoy en día cada vez es más frecuente que se realicen las conexiones a Internet desde los teléfonos móviles y que debido al agotamiento de las direcciones IPv4 las proveedoras de servicios asignes una misma IP a más de un usuario. Por este motivo, cuando solicitamos una dirección IP a una compañía, es posible que presenten un listado de personas asociados a la misma IP en la fecha y hora solicitada siendo la única diferencia el puerto de salida. Para poder identificar al verdadero culpable, si desconocemos el puerto, es necesario filtrar los datos y compararlos con otras respuestas facilitadas, siempre y cuando hayamos solicitado más de una conexión, ya que si tenemos únicamente una, la identificación es imposible.

Una vez tengamos el nombre del titular de la línea desde la que se realizaron las conexiones, lo normal es que el autor de los hechos investigados sea dicha persona o bien alguno de su núcleo familiar. En este punto juega un papel importante la investigación

tradicional, entrando en juego la consulta a las bases de datos y registros policiales tradicionales como antecedentes policiales, denuncias previas, empadronamientos, etc. a través de la cual se debe determinar si la persona identificada es realmente la autora de los hechos.

2.3. Identificación, obtención y salvaguarda de evidencias en la Red.

En este apartado nos vamos a referir a la captura de contenidos con seguridad jurídica. Es uno de los momentos más importantes y sensibles del proceso de recolección de evidencias digitales. Ya hemos hablado de su alta volatilidad y la facilidad con la que puede ser manipulada por lo que si no se actúa con celeridad y no se ponen a disposición del ciudadano determinadas herramientas, es posible que nos quedemos sin algo tan importante como es el objeto del delito y, por tanto, sin una evidencia de la que poder partir una investigación o con la que poder acreditar un hecho.

Lo recomendable para dejar constancia de la publicación de contenidos y las comunicaciones electrónicas sería la utilización de un software o aplicación corporativa desarrollada por la propia Administración Pública. De esta forma, el software estaría controlado por la autoridad firmante, permitiría acreditar la autenticidad del contenido capturado, la identidad del solicitante o denunciante y los documentos electrónicos generados permanecerían almacenados en servidores bajo control y custodia policial o judicial.

A través de este software, el denunciante, ya sea persona física, empresa o corporación de derecho público podría obtener certificados digitales reconocidos por las autoridades judiciales, cumpliendo con todos los requisitos impuestos y actualizados por la Ley 59/2003 de 19 diciembre de Firma Electrónica.

Esta plataforma de gestión de certificados digitales “policial o judicial” podría incorporar la tecnología de timbrado digital de documentos denominada timestamping (o sellado de tiempo) basado en un mecanismo criptográfico que asocia una fecha inalterable a la generación de un documento digital. En otras palabras, la certificación de que una publicación albergaba el contenido denunciado en fecha y hora determinada, firmada electrónicamente mediante un algoritmo criptográfico y emitida por una institución pública con plena validez legal. De esta forma, se podrían descartar posibles manipulaciones.

Pero lo cierto es que, de momento, entre las principales Autoridades de Certificación españolas que emiten certificados electrónicos no se encuentra un prestador de servicios que brinde esta utilidad específica a la Administración Pública para certificar contenidos procedentes de la Red y que puedan ser incorporados en un proceso penal con plena validez jurídica.

Por ello, para cubrir esta carencia, se recurre a lo que se denomina “terceros de confianza”, empresas ajenas a la declaración de las partes (al denunciante y denunciado) que incorporan en sus máquinas estas solicitudes de certificación a través de una plataforma online de acceso cómodo y rápido. Cuando hablamos de contenidos digitales altamente volátiles, se hace necesario contar con sistemas que incorporen estas funcionalidades y servicios.

Existen otros sistemas alternativos de certificación a los terceros de confianza que no incorporan ninguna plataforma telemática ni garantía técnica de recogida pero poseen plena validez legal, al estar legitimados por el firmante. Nos referimos a las actas expedidas por el Secretario Judicial, al que le corresponde en exclusiva el ejercicio de la fe pública judicial; el acta notarial de una página web que permite acreditar con fe pública notarial lo que el Notario puede ver publicado en una página web en un momento determinado; y las autoridades policiales, cuya diligencia de contenidos posee la validez de mera denuncia, redactada bajo el principio de veracidad que se nos presupone y que se adjunta con el atestado policial.

No obstante, a pesar de la legitimidad de los firmantes, Secretario Judicial, Notario o funcionario de policía, hay que mirar con ciertas reticencias la incorporación de estos documentos al procedimiento ya que la falta de formación tecnológica puede ocasionar que se levante acta de meras impresiones de capturas de pantalla o de lo que el funcionario está viendo en ese momento.

Aunque provengan de entidades con fé pública o de funcionario público en el ejercicio de sus funciones, se debe dejar constancia de cómo se ha obtenido y se ha llegado al contenido en cuestión. Recordemos que, en la Red, cualquier contenido es modificable y por tanto, no nos podemos fiar de lo que ven o perciben nuestros sentidos.

Estos procedimientos también se pueden emplear para certificar otro tipo de actuaciones en la Red como envío de correos electrónicos, actas de navegación web, etc. pero, en este trabajo, vamos a detallar los elementos de los que interesa dejar constancia para poder dar inicio a una investigación ciber y cuál es el procedimiento a seguir. De ello hablaremos específicamente en el apartado “Salvaguarda de evidencias” de la metodología propuesta.

Una vez expuestas las garantías procesales que ofrece este sistema, lo más importante es que el proceso se puede llevar a cabo de forma telemática, en el momento en el que se localiza el contenido, minimizando al máximo el riesgo de que se pierda.

Lo negativo es que se genera un documento que, aun custodiado por un tercero de confianza, no está sometido a la fe pública. Si el contenido es eliminado, no existe la posibilidad de reproducir la prueba por lo que queda a la sana crítica (a criterio) de la Autoridad Judicial la asunción de este documento como prueba indiscutible.

2.4. Sistemas de cifrado, comunicaciones e interceptación.

Esta es una limitación que va a intervenir principalmente con el proceso de investigación ya iniciado pero hay ciertos aspectos que conviene resaltar porque van a estar relacionados con la importancia de aportar correctamente el contenido exacto de conversaciones, correos electrónicos o cualquier otro tipo de conversación en el momento de reportar el suceso.

La parte interesada debe constatar la existencia de las comunicaciones electrónicas cuando estas sean una evidencia digital o fuente de prueba en el proceso. En la actualidad, no hay un solo proveedor de servicio de comunicaciones, ya sea web, correo electrónico, mensajería instantánea o red social que no incorpore un sistema de cifrado de tipo RSA, por bloques o de tipo de Diffie- Hellman de intercambio de clave, sistemas actuales robustos que hacen imposible atacar de forma efectiva el sistema de cifrado y obtener el texto en claro en una comunicación cifrada, manteniendo la integridad, la confidencialidad y la autenticidad del mensaje.

La integridad garantiza que el contenido del mensaje no ha sido alterado por el camino; la autenticación asegura la identidad del remitente del correo, y que no ha sido falsificado; y la posibilidad de negar su participación en la comunicación, que nos protege frente a que posteriormente el que envió el correo (o lo recibió de nosotros) alegue posteriormente no haberlo enviado (o recibido si era el destinatario). Estos últimos servicios se prestan mediante las firmas digitales.

Gracias a estos sistemas de cifrado, las comunicaciones entre usuarios son más seguras y por ende, no solo viajan ya cifradas sino que su almacenamiento se hace, presumiblemente, de la misma forma. Esto significa que, hoy por hoy, es imposible interceptar una comunicación cifrada que está teniendo lugar en ese preciso momento (ni siquiera de forma no autorizada o maliciosa) y acceder a su contenido de forma legible así como recuperar cualquier comunicación que no haya sido entregada por su legítimo poseedor o alguien que haya intervenido en el mismo proceso de comunicación y las haya almacenado en un dispositivo informático o de almacenamiento.

Ya en el año 2006, una de las primeras investigaciones (en esta ocasión sobre producción y distribución de pederastia) en las que participó esta alumna, durante la fase ejecutiva de la denominada “Operación Ruber”, la mayoría de los miembros de la organización disponían en sus ordenadores de contenedores virtuales cifrado con la aplicación *bestcrypt* donde almacenaban los archivos y datos reveladores de su actividad delictiva. En algunos de los casos no se ha conseguido, hasta el momento, obtener la contraseña que dé acceso a los contenedores virtuales y por tanto la obtención de más pruebas documentales.

2.4.1. ¿Qué ocurre con las cuentas de correo electrónico gratuitas basada en la web o "web based"?

El correo electrónico se ha convertido en una de las formas más utilizadas para contactar con víctimas, ya sea a través de phishing, spam o mediante ataques o fraudes dirigidos.

Mayoritariamente, las direcciones de correo electrónico se obtienen de servidores que brindan un servicio "gratuito"; algunos ejemplos son outlook.com, o gmail.com, etc. Ello sin mencionar los dominios genéricos como @dr.com, @emailaccount.com @gmx.com, y cientos de ellos. La gratuidad de estos servicios y la serie de características que llevan aparejadas como estar administradas por proveedores extranjeros o *bullet- proof hostings* (proveedores que no colaboran con las autoridades) y el cifrado, le confieren bastante atractivo para llevar a cabo un uso ilícito o irregular, lo que dificulta especialmente la investigación policial, a saber:

- Inexistencia de un vínculo comercial o financiero entre prestador y prestatario del servicio. No requieren aportar datos de cuentas bancarias o tarjetas de crédito (como es el caso de servidores de pago) y por consiguiente el proveedor no va a disponer de referencia con la que contrastar la veracidad de los datos aportados por los usuarios.
- En el proceso de creación de la cuenta, el servicio de suscripción solicita al usuario la aportación de unos datos de identidad que en la mayoría de los casos, como así corroboran las investigaciones, son falsos.
- Por otra parte, dichos servidores facilitan la creación de varias direcciones y permiten que las direcciones se cambien en forma constante, lo que lleva a que una dirección aparezca y desaparezca en cuestión de días, convirtiendo el uso de estas casillas de correo electrónico en algo muy difícil de rastrear.
- La empresa comercial y los servidores del servicio de correo se ubican en el extranjero, no existiendo de momento, mecanismo que permita la urgente intervención judicial y evitar así posibles pérdidas de información.

Aun con todo esto, la misma dirección de correo electrónico y su dominio será una evidencia digital de vital importancia ya que se puede rastrear, al igual que otras, su actividad y será conveniente que el ciudadano reporte toda la información de la que disponga.

Por último, ya lo mencionamos en párrafos anteriores, la firma digital, en el cibercrimen y su investigativa cobran especial relevancia como funciones resumen las funciones hash.

La criptografía asimétrica permite identificar al emisor y al receptor del mensaje pero para identificar el mensaje propiamente dicho se utilizan las llamadas "funciones resumen". El resultado de aplicar una función resumen a un archivo (ya sea texto o imagen) es un número

grande, el “número resumen” o “hash”, para evitar duplicidades (un número hash puede ser “3bffa4ebdf4874e506c2b12405796aa5”) y tiene las siguientes características:

- Todos los hash generados con un mismo método tienen el mismo tamaño, sea cual sea el archivo utilizado como base.
- Dado un archivo base, su cálculo es fácil y rápido (para un ordenador).
- Es imposible reconstruir el archivo a partir del hash.
- Y tal vez para la investigación policial el más importante: es imposible que dos archivos diferentes tengan el mismo hash.

Esto hace que presentar un hash en el reporte de ciertos archivos permita mantener la trazabilidad de los mismos o mantener la cadena de custodia**,** por lo que es necesario incluirlo también como evidencia en la aplicación CIBERPOL.

¿Qué interés tiene este identificador hash de archivos para la investigación policial? Existe la posibilidad de clasificar e identificar mediante las funciones hash las miles de imágenes y vídeos con contenido pedófilo hallados durante los registros en los domicilios de los detenidos. Posteriormente, mediante una aplicación informática que rastrea direcciones IP de las redes P2P, se localizan esas imágenes mientras están siendo intercambiadas por los usuarios de las redes.

En relación a los rastreos policiales en un sitio público (entiéndase internet) existe ya diversa jurisprudencia del Tribunal Supremo que le otorga legitimidad a esta medida de investigación.

2.5. Trazabilidad virtual de los beneficios ilícitos obtenidos del cibercrimen.

Si existe un rastro de trazabilidad criminal importante que determinar es el rastro de los beneficios ilícitos obtenidos por los autores. Por ello, es prioritario determinar la titularidad de determinados mecanismos de pago, ya sean tarjetas de crédito, cuentas bancarias, etc. y, por tanto, la recogida de cuantos datos identificativos puedan ser de valor. Ahora bien, no todos los métodos de pago garantizan una trazabilidad o puede identificar al titular de la cuenta, es más, todos aquellos métodos de pago con un mayor componente digital como las tarjetas prepago, las criptomonedas, son ampliamente empleados en el mundo del cibercrimen al no estar asociada a una identidad digital cada uno de los medios de pago.

En primer lugar, cualquier tipo de cuenta o producto bancario contratado a través de una entidad están perfectamente identificados, siendo necesaria la pertinente documentación de identidad para aperturar o contratar cualquiera de este tipo de servicios. No obstante, como siempre, los criminales se las ingenian con argucias, algunas delictivas para tratar de perder el seguimiento de las fuerzas policiales.

Por un lado, la solicitud fraudulenta de tarjetas de crédito mediante la apertura on-line de cuentas bancarias utilizando documentación falsificada y domicilios preparados para la recogida de la documentación bancaria y recepción de las tarjetas, controlados por los estafadores. Una vez preparada la logística anterior, los autores de la estafa solicitan tarjetas de crédito, aportado datos laborales y financieros falsos, que permitan un límite de crédito elevado en las tarjetas, para finalmente dejarlas en descubierto, por distintos procedimientos, a través de la ejecución de compras físicas o virtuales de bienes o servicios, recarga a crédito de otras tarjetas de tipo virtual o cuentas bancarias intermediarias, remisión de dinero a través de entidades money-transfer, etc.

Por otro lado, la titularidad de las cuentas bancarias pertenece a la apertura de cuentas intermediarias, las denominadas mulas de dinero. De forma previa o simultánea a la captura de las credenciales bancarias de las víctimas de este fraude, se efectúa la apertura de cuentas puente o intermediarias. Las cuentas intermediarias, pueden estar aperturadas o tituladas por miembros de la organización o bien por personas ajenas a la misma, captadas a través de supuesta ofertas de trabajo, denominadas “moneymules” o “mulas de dinero”.

Estas mulas son las receptoras en primera instancia de los importes transferidos ilícitamente desde las cuentas de las víctimas para después quedarse con la comisión que les corresponde por la participación y resto volverlo a transferir a mas mulas de la organización o retirarlo en efectivo a través de cajero.

Los sistemas de pago electrónicos conocidos como "canales de pago alternativo", para la transferencia de beneficios económicos (E-Gold, WebMoney, Western Union, MoneyGram, etc.) son un buen cauce para el traspaso de fondos obtenidos de forma fraudulenta por las

organizaciones criminales. De hecho, los criminales explotan al máximo sus posibilidades de funcionamiento para eludir los controles bancarios y obtención de información por los investigadores policiales.

Existen decenas de empresas que ofrecen sistemas bancarios basados en Internet que permiten que el dinero se mueva al instante por todo el mundo, con un alto grado de anonimato. Estas empresas, según los expertos , de servicio “e-moneda” tienen, a menudo, su enclave en países con un grado mínimo de supervisión financiera, permitiendo a las empresas eludir las prácticas habituales del sistema financiero para descubrir el blanqueo de capitales y la financiación de actividades ilegales.

Por último, reseñar las criptodivisas o monedas virtuales como una entidad descentralizada que utiliza la criptografía y el esquema de red *peer to peer*. No existe una entidad que la regule, sino que es la propia comunidad la que garantiza su funcionamiento. En Internet se usan como medio de pago en los mercados clandestinos de la Darknet, para pagar los “rescates” del ransomware e incluso como forma de pago de extorsiones realizadas por cibercriminales.

El bitcoin es la criptodivisa más utilizada. La base tecnológica para el funcionamiento del Bitcoin es la criptografía de clave asimétrico y el registro público *blockchain* o cadena de bloques.

Blockchain está formado por bloques, conteniendo cada uno una serie de transacciones realizadas. Al ser completamente público todos los usuarios pueden ver cuánto dinero hay en una determinada dirección, cuánto se ha gastado, a qué dirección ha enviado dinero o desde cuál lo ha recibido o cuánto dinero ha movido en total, entre otras. Sin embargo, dado que las direcciones Bitcoin no tienen ningún dato identificativo, no revela la identidad de quien realiza las transacciones.

Otras monedas virtuales más actuales son *Ethereum*, o por sus capacidades de anonimato, que las hacen un instrumento ideal para los cibercriminales, como Monero y *Zcash.*

2.6. Colaboración con los proveedores de servicio en Internet.

Las conocidas ISP (*Internet Service Provider*) son las compañías que proporcionan servicios de Internet. La mayoría de ellas, por no decir todas, poseen sus servidores fuera de España, en la mayor parte de los casos en Estados Unidos, lo cual obliga a adecuarnos a su legislación para realizar las peticiones de datos.

Con las empresas proveedoras de servicios existe el problema de la conservación de los datos, ya que según la ley, los datos no deben guardarse por tiempo superior a un año por lo que una conexión de hace 13 meses ya no proporcionarían un rastro digital que trazar. Esto es cuando se trata de adecuarse a la normativa española porque se da el caso frecuente de no adecuarse a la normativa de nuestro país, no colaborando con las autoridades judiciales si no es a través de la Comisión Rogatoria Internacional.

Si seguimos una metodología, se buscarán y extraerán de un blog particular, páginas web profesionales, servicios web de correo, redes sociales, o cualquiera de estos servicios, datos personales, es decir, “cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables procedente de todas ellas cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social”.

Todos estos servicios de alojamiento van a almacenar ficheros con toda esa información, es decir, un “conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso" y alguien, ya sea el editor de código, el administrador o titular del dominio, el desarrollador o el abogado, va a ser el responsable del tratamiento de ese fichero. En cualquier caso, puede ser un particular o una persona jurídica, pública o privada u órgano administrativo, que sólo o conjuntamente con otros, decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realice directamente.

En el caso de que los datos se vayan a ceder a la Policía Judicial en el ejercicio de sus funciones, la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, impone la exigencia de autorización judicial, siempre que se trate de datos vinculados a procesos de comunicación (por ejemplo, una conversación por chat o mensaje directo entre usuarios de Facebook, Twitter, etc., por mensajería instantánea, WhatsApp, o correo electrónico), que garantice el derecho inviolabilidad de las comunicaciones.

Sin embargo, según la modificación de Ley Orgánica 13/2015, de 5 de octubre, de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, no es necesaria la autorización de un

juez para la cesión de datos desvinculados de los procesos de comunicación concernientes a la titularidad o identificación de un dispositivo electrónico, es decir, la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, que precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación.

Los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, estarán obligados a cumplir el requerimiento bajo apercibimiento de incurrir en el delito de desobediencia. Es decir, cualquier empresa que reciba una petición de los actores policiales o judiciales relativa a la cesión de datos, está obligada a cederlos si ejerce su actividad comercial en España.

Por tanto, teniendo en cuenta las salvedades del apartado anterior en los que las autoridades policiales y el Ministerio Fiscal en sus funciones indagatorias requieren orden judicial, tanto particulares como autoridades policiales y judiciales pueden extraer información personal que sea pública. Es decir, aquella que tras aceptar (a veces muy alegremente), términos, condiciones y políticas de privacidad, estés dispuesto a que conste públicamente: nombre, apellidos, número de teléfono, dirección postal, dirección de correo electrónico, nombre de usuario, intereses, preferencias, material audiovisual, etc.

En todo caso, los proveedores de servicio deben especificar en sus términos qué información de la que proporcionas será pública, visible y accesible a cualquier otro usuario de la Red y cuál se almacena de forma privada.

2.7. Intercambio de información entre Fuerzas y Cuerpos de Seguridad y cooperación internacional.

Como ya se ha comentado, Internet es un fenómeno global y el cibercrimen un modo de vida por lo que es habitual, salvo en determinados casos como el ciberbullying, el acoso o la violencia de género digital, que están orientadas al círculo más personal y cercano de la víctima, que los delitos tengan un componente internacional. O bien el autor, las víctimas, las plataformas digitales y los servicios de Red empleados, o bien parte de ellos, son de origen extranjero.

Los delitos que se cometen a través de Internet también son globales, lo que significa que un mismo hecho puede tener víctimas en todas las partes del planeta o lo que es lo mismo una persona puede cometer un delito desde cualquier parte del planeta. En el delito tradicional, una estafa, como el famoso timo de la estampita, necesariamente, requería que ambos actores, defraudador y víctima, estuviesen en el mismo lugar. En el mundo virtual, el estafador y el estafado pueden encontrarse a miles de kilómetros y aún así, perpetrarse el fraude con total normalidad. Esto supone otra limitación para las investigaciones ya que cuando se trata de delitos menos graves y el autor o autores se presume se encuentran fuera de nuestras fronteras, muchos juzgados ni siquiera incoan diligencias previas y si lo hacen, son las proveedoras de servicios las que no facilitan datos si los hechos apuntan a conexiones fuera de la jurisdicción del país solicitante.

Por todo lo mencionado anteriormente, muchas conductas delictivas no reciben el reproche penal que merecen porque algunas investigaciones no prosperan y las que lo hacen es gracias a la no menos complicada cooperación internacional.

No obstante, la cooperación internacional es un elemento necesario para poder llevar a cabo investigaciones en las que existen víctimas en más de un país y cuando parte de los autores o de la infraestructura de la organización o bien la totalidad de los mismos se encuentra fuera de nuestras fronteras. En este caso hay que recurrir a los canales de comunicación y colaboración de organismos como Europol o Interpol o a equipos de investigación conjuntos (JIT), lo que genera demoras exageradas en las investigaciones y complicaciones derivadas de la diferencia de legislación entre los países intervinientes. En la actualidad, también se articulan las OEI, las Órdenes Europeas de Investigación, para el territorio Schenguen, las cuales son tramitadas a través de las autoridades judiciales de cada país.

3. Objetivos concretos y metodología de trabajo.

3.1. Objetivo general.

El objetivo general es analizar el contexto del cibercrimen y su persecución, extrayendo un listado de ítems evaluables, relevantes, escalables a los que se le pueda asignar un valor con los que proponer una metodología de tratamiento de la información en fases previas que permitan abordar eficazmente la investigación del cibercrimen.

Dentro de este objetivo general descrito, podemos establecer los siguientes:

- Conseguir una mayor tasa de esclarecimiento de los delitos durante su investigación.
- Unificar la información recibida facilitando la puesta en conocimiento y reporte de los ciudadanos sobre hechos sospechosos y delictivos.
- Facilitar la puesta en conocimiento y tramitación de denuncias con un componente técnico tanto para el ciudadano como para las FCSE.
- Mejorar la coordinación de las investigaciones policiales a nivel nacional.
- Agilizar los tiempos de investigación por hechos cometidos a través de la Red.
- Recoger con mayor exactitud la estadística de casos generados, pudiendo diferenciar entre los casos denunciados y su tipología delictiva más concreta, archivados en comisaría, investigados con resultado o sin resultado.

3.2. Objetivos específicos.

- Plantear una metodología de trabajo aplicada a la problemática específica diaria policial en la lucha contra el cibercrimen.
- Garantizar la obtención de evidencias digitales en el momento de la recepción de las denuncias y, por lo tanto, evitar su pérdida, alteración o borrado.
- Unificar hechos delictivos que puedan estar siendo cometidos por los mismos autores al detectar similitudes por modus operandi, ya sea por mismos objetivos o recursos comisivos empleados.
- Reducir el trabajo empleado en las oficinas de denuncias o de recepción de estos incidentes así como a posterior por los grupos de investigación especializados.
- Evitar la pérdida de evidencias digitales por negligencia, dilaciones indebidas, volatilidad de la propia evidencia digital y falta de profesionalización.
- Centralizar la obtención de información para su posterior explotación por cualquier cuerpo policial situado en cualquier demarcación del territorio nacional.
- Evitar duplicidades de trabajo por la indagación de hechos idénticos o similares denunciados por diferentes víctimas en las distintas demarcaciones territoriales.
- Elaborar estadísticas y realizar *big data* con la información obtenida de la aplicación.

- Valorar y cuantificar el índice de fiabilidad y tasas de esclarecimiento que pudiera alcanzarse con la metodología.
- Describir una interfaz de fácil uso, con exportación de datos a Excel y generación de informes automáticos a PDF para facilitar los datos de los ciberinvestigadores y poder aportar estos informes adjuntos con el atestado policial.
- Posibilidad de escalar y/o compartir los resultados con otras plataformas incluso, aplicabilidad en otras fuentes digitales que permitan acceso a su API REST.
- Desarrollar la metodología para rastrear y monitorizar cualquier fuente de Internet, de forma automática (prensa, foros, blogs…), incluso, como posible fuente de evidencias.
- Evitar que la falta de formación, experiencia y personal cualificado tanto técnico como investigador en Internet redunde en la calidad de la investigación y el éxito de esclarecimiento, al establecer una metodología pautada.

3.3. Identificación de los requisitos técnicos. Herramientas empleadas.

En línea de la descripción de los diferentes ficheros policiales[6], la finalidad de la herramienta que forma parte de la metodología propuesta es la identificación y prevención de peligros reales concretos para la seguridad pública en plataformas digitales y la represión de infracciones penales relacionadas con el uso de la Red y la tecnología mediante la recuperación, evaluación, tratamiento, coordinación y análisis de toda la información generada por las unidades operativas del Cuerpo Nacional de Policía, así como la creación de inteligencia criminal derivada de ello.

El uso previsto irá dirigido al ciudadano como usuario desde acceso vía web y actuaciones de Fuerzas y Cuerpos de Seguridad con fines policiales. La plataforma propuesta no estará conectada ni intervenida por los órganos judiciales, como es la plataforma desarrollada por el Ministerio de Justicia, Lexnet o la integración con otras plataformas digitales de recepción de información sobre ciberincidentes como es la Oficina de Coordinación Cibernética, (OCC) del Centro Nacional de Infraestructuras Críticas y Ciberseguridad (CNPIC) dependiente de la Secretaría de Estado de Seguridad del Ministerio del Interior o la plataforma HELIOS, desarrollada por el Instituto de Ciberseguridad (INCIBE) dependiente del Ministerio de Agenda Digital.

El uso principal será el de gestión informatizada de trámites necesarios que llevan las denuncias en las dependencias policiales relacionadas con los delitos cometidos en Internet o con el uso del mismo. La información será grabada por los agentes o por otros gestores como puede ser el propio ciudadano y si es por este último, supervisada y confirmada por los propios agentes especializados en la investigación de este tipo de delincuencia.

[6] https://www.boe.es/buscar/doc.php?id=BOE-A-2002-13741

Integraciones. No está previsto que se integre con otras plataformas del sistema como SIDENPOL (sistema policial de almacenamiento y gestión de denuncias). La aplicación recoge los datos necesarios para generar informe con valor de denuncia y otros trámites procesales para gestionar un atestado al completo.

No significaría la destrucción e integración de datos contenidos en otros ficheros policiales, valorándose la posibilidad de integrar solo algunos de los datos recabados relacionados con este tipo de criminalidad, por ejemplo, con operación Telémaco ya existente, relacionada con fraudes y una amplia base de datos de numeraciones de tarjetas de crédito y cuentas bancarias.

La información contenida recopilará datos de personas o colectivos sobre los que se pretenden obtener datos de carácter personal o que resulten obligados a suministrarlos como personas detenidas e investigadas, o relacionadas con éstas, así como víctimas de infracciones penales, testigos y denunciantes de las mismas o cualquier reporte o comunicación realizada a través de la web corporativa de Policia vía online que emplee el soporte o canal de denuncia online creada para estos efectos con tres sistemas de identificación.

Sistema de acceso mediante DNIe o certificado electrónico, clave PIN[7] y con usuario y contraseña (necesario ratificar la denuncia mediante exhibición de DNI en la oficina de atención al ciudadano de una comisaría).

Las medidas de seguridad, teniendo en cuenta los tres niveles, básico, medio o alto exigible, será alto al contener datos de carácter personal y de infracciones penales.

El órgano responsable del fichero será la Comisaría General de Policía Judicial sita en la calle Julián González Segador, s/n, 28033 de Madrid.

3.3.1. Plataforma de recepción de denuncias para hechos penales o de interés policial cometidos en el ciberespacio. CIBERPOL.

Esta plataforma está destinada a recoger información de los delitos cometidos a través de Internet o con implicación de la misma.

La plataforma consistirá en una base de datos de tipo relacional con campos cerrados donde se proveerá al usuario de menús y submenús con alternativas y campos de texto libre desarrollados para la introducción de datos validados del tipo: numeraciones de tarjetas, dominios de cuentas de correo electrónico, direcciones de bitcoin, números de referencia de medios de pago electrónicos, etc. de forma que el procedimiento de reporte esté completamente guiado por la plataforma y el margen de error en la introducción de datos sea por errores de transcripción o documentación de usuario pero no que permita errores sintácticos.

[7] https://clave.gob.es/clave_Home/PIN24H/Que-es.html

El ciudadano deberá de completar un formulario guiado en el que se le irán mostrando los campos a rellenar. Existirán determinados apartados y campos obligatorios dentro de esos apartados que lo permitirán validar ni enviar el formulario si no están correctamente rellenados pues la aplicación entenderá que no se disponen de los datos necesarios o concretos para determinar la existencia del ilícito penal y su posterior investigación.

Hay que incidir que se debe de realizar una campaña informativa hacia el ciudadano para que conozca la existencia de esta aplicación, las ventajas de completar este formulario vía web como mecanismo de denuncia y se ponga a su disposición la herramienta.

3.3.2. Variables a considerar en el delito y su recepción por parte de agentes o ciudadanos.

Por una parte, como hemos mencionado, el usuario que acceda a la aplicación generará un “Nuevo caso”, con su propio identificador y tendrá que rellenar apartados de la aplicación únicamente destinados a la recopilación de los datos personales del usuario que reporta como identidad, domicilio, lugar, fecha y descripción del hecho, etc. Además, existirán otros datos que definirán lo que hemos denominado el “Suceso”, datos relativos al hecho denunciado concreto (descripción del hecho, lugar y fecha de comisión, circunstancias concurrentes, objetos sustraídos o afectados, modus operandi, etc.) y que hemos denominado “Objetos”.

Además, la aplicación permitirá un apartado para “texto libre” de forma que el usuario o el agente pueda narrar los hechos acontecidos que estimen oportuno y adjuntar archivos y ficheros como documentos acreditativos de indicios o prueba como justificantes de compra, cabeceras de emails, conversaciones de mensajería, documentos bancarios, oficiales, etc.

Estos “objetos” se configurarán en las variables que puedan ser objeto de análisis y tratamiento posterior (no se incluye en el presente trabajo) para su explotación de forma que puedan ser catalogados e integrados en un sistema de procesamiento natural del lenguaje para detectar patrones de comportamiento delictivos específicos que puedan ser catalogados como *phishing, carding, ransomware* o pueda detectar acciones presumiblemente cometidos por los mismos autores al mostrar indicadores de repetición en determinados patrones. Por ejemplo, una banda criminal organizada que lleva actuando desde el 1 de diciembre hasta el 21 de diciembre en todo el territorio nacional realizando cargos en tarjetas bancarias de crédito tipo *contacless* para la extracción de dinero en salas de recreativos, salones de juego y bingos que permiten este tipo de obtención de dinero a crédito como si fuera un cajero.

4. Desarrollo específico de la metodología de trabajo.

Teniendo en cuenta las limitaciones planteadas en los primeros dos apartados del presente trabajo, se va a realizar una propuesta metodológica para la recepción de hechos presuntamente delictivos y posibles conductas sospechosas. Como se ha incidido desde el principio, uno de los problemas más acuciantes en este tipo de criminalidad es la forma en la que se recolecta, clasifica y trata la información recibida desde el inicio procedente de los reportes de ciudadanos y empresas que notifican, reportan o denuncian un ciberdelito.

Dado que es imposible evitar que las investigaciones fracasen por motivos procesales y procedimentales, también expuestos, como son el uso de anonimizadores para la navegación, conexiones nateadas para dispositivos móviles, limitaciones territoriales, cuestiones procesales de competencia judicial, falta de cooperación de los proveedores de servicio, etc. , incidiremos, por tanto, en esa fase previa así como en la posterior, pudiendo establecer un criterio estadístico que permita proponer clasificaciones más concretas dentro de la casuística criminal para este tipo de hechos cibernéticos.

A continuación, vamos a mostrar un esquema general de la metodología que se propone y que pasaremos a comentar en el apartado de 4.1. del desarrollo de la misma de forma pormenorizada.

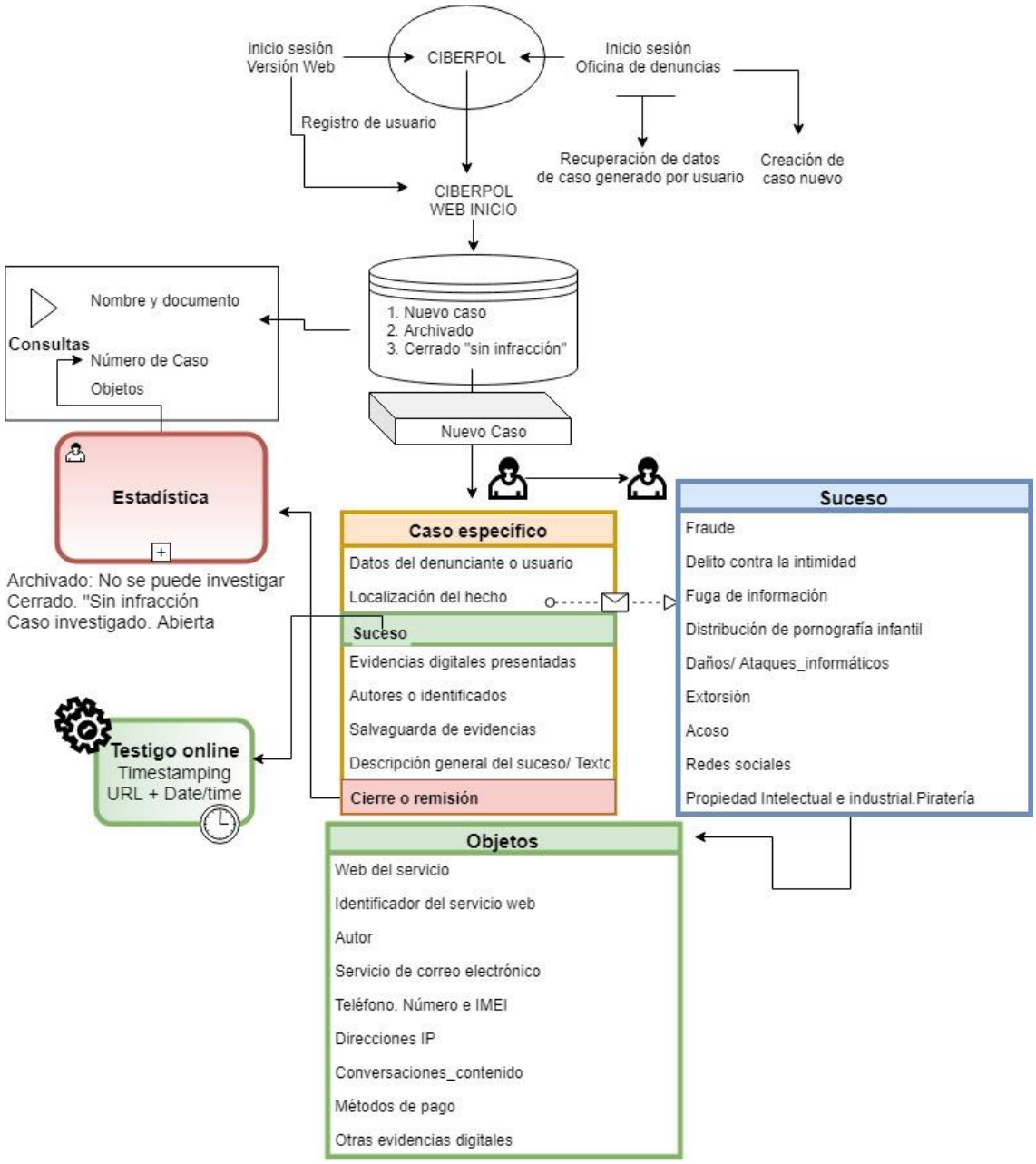


Fig 3. Esquema de la metodología propuesta diseñado en https://www.draw.io/

4.1. Identificación de requisitos. Plataforma CIBERPOL.

Se va a proceder a describir la aplicación, desde el proceso de registro hasta la generación y explotación del caso a posteriori con fines investigativos. Aunque se entrará en detalle, sobre todo en el momento de la recolección de las evidencias digitales asociadas a una tipología de caso (delito), habrá campos y apartados que queden por definir de forma más precisa teniendo en cuenta la extensión limitada de este TFM que es proponer una metodología que de forma objetiva pueda mejorar la eficacia en la lucha contra el cibercrimen desde la toma de los hechos evidenciados.

Hemos incidido en que será un proceso guiado, ayudado por ventanas emergentes que ofrezcan información sobre cómo ejecutar el proceso de la forma más precisa posible e intuitiva, evitando campos, denominaciones excesivamente técnicas y activando los siguientes campos en el caso de que no se haya completado el formulario denuncia de la forma adecuada que permita su seguimiento posterior.

A partir de este momento, al ciudadano o víctima que desee utilizar este servicio, le llamaremos "Usuario". Los hechos que el ciudadano desea poner en conocimiento de las autoridades se denominarán "Suceso" y los documentos generados por la aplicación, denominados en la jerga procesal como "atestado", se le denominarán "Caso". Estas nuevas denominaciones obedecen a una jerga tecnológica, más contemporánea con la sociedad digital actual.

4.1.1. Descripción de la metodología

4.1.1.1. Acceso y registro a la aplicación.

Distinguiremos dos tipos de acceso:

- **Acceso desde la web principal y el dominio .es de atención al ciudadano.**

Es necesario, crear una página de INICIO explicativa en la que se informe al ciudadano de las circunstancias en las que debe poner en conocimiento unos hechos tales así como la información que deberá aportar y los motivos de ello. Es importante guiar en todo el proceso al ciudadano para evitar la pérdida de información

La pasarela de acceso será a través de un proxy que se conectará al servidor del Ministerio del Interior. El usuario dispondrá de las siguientes alternativas:

DNIe / Certificado electrónico

- Cl@ve PIN. Un sistema de autenticación a través de DNI/NIE que solicitará utilizar la App Cl@ve PIN para obtener el PIN (recomendado),

usar el navegador para obtener el PIN y recibir un SMS al terminal telefónico indicado

- No estoy registrado en Cl@ve. En ese caso, el ciudadano podrá interponer su denuncia de forma online pero tendrá que personarse en su comisaría más cercana para ratificar el documento y acreditar su identidad.

El proceso de recogida de datos sobre el suceso será muy similar, tanto para el agente de la autoridad encargado de la recepción de la denuncia como para el usuario, de forma que se evite la pérdida u omisión de información así como los datos relevantes para el seguimiento y la investigación.

Una vez finalizada la denuncia, el sistema ofrecerá un número de caso inicial empezando por W- Nº Caso, que el usuario deberá presentar en el momento de su denuncia a modo de localizador.

4.1.1.2. Acceso a la aplicación CIBERPOL a través de enlace en intranet corporativa.

El acceso a la aplicación se realizará desde el mismo escritorio que el resto de aplicaciones policiales y este tipo de acceso profesional requerirá la identificación del agente mediante usuario y contraseña, debidamente autorizada. No servirá el número de identificación de agente o carné profesional ya que deberá estar autorizado en su condición de investigador o agente destinado en la Oficina de Denuncias y Atención al Ciudadano. Al pulsar sobre el enlace, se mostrará la pantalla de inicio de la aplicación.

Una vez que el usuario ha accedido a la aplicación y si no realiza ninguna acción sobre la misma durante 120 minutos le expira la sesión, mostrándole la pantalla de expiración de sesión.

4.1.1.3. Uso de la aplicación

En la página de Inicio, se mostrarán los datos del agente de policía que vaya a proceder a generar un nuevo caso con una denuncia o a validar la ejecutada por el usuario sin registro de Cl@ve. Al pulsar "**Aceptar**" se vuelve a la página de Inicio.

- Opciones de menú "Usuario".
- Datos de "Usuario" y de "Caso".

Los datos de usuario que se muestran son los del 'Usuario' (Obligatorio) y los del 'Agente' si se ha introducido sus datos en la pantalla de Inicio.

También figurará un número de caso generado o de registro por el usuario si se ha registrado desde la aplicación web. En ambos casos, no serán correlativos y la identificación del caso será "U- Nº de caso" si es tomada desde las dependencias policiales o "W- Nº Caso" si es tomada desde la versión Web. Recordemos que el ciudadano deberá presentar el número de caso obtenido de la aplicación.

4.1.1.4. Opciones de menú "Consulta".

Hay una serie de consultas que podrán ser asignados al agente en la aplicación (dependiendo del nivel atribuido). Son las siguientes:

- Partes de Casos:
  - Parte de Sucesos
  - Parte de detenidos/identificados
  - Casos por Plantilla
  - Peticiones judiciales
  - Nº de Registro de Caso
- Denuncias – Estadística
  - Denuncias por demarcación
  - Estadística genérica
- Identificación por tipología delictiva

Pero a partir de la consultas "**Número de registro de caso**", éstas se realizan a nivel de toda España no teniendo en cuenta el nivel que tiene el usuario asignado para la aplicación, es decir, que dependiendo del nivel, cualquier agente de investigación podrá acceder a un número de caso pero no generar estadísticas de caso por cualquiera de las plantillas.

- **Partes de comisaría.**
  - **Parte de Sucesos.**

Esta consulta considera el nivel del usuario para realizar la consulta. Permite consultar casos asociados a una comisaría en una fecha y hora determinada.

Se puede configurar para que los partes de sucesos por defecto se muestren en un período o rango concreto de fechas o seleccionar el usuario el deseado sin que sea menor a 24 horas. La aplicación listará todos los realizados por número de caso, demarcación de la oficina que ha tomado la denuncia o del domicilio de la víctima así como la tipología delcitiva puesta en conocimiento según formulario Si el usuario no ha validado en comisaría aún su caso, aparecerá una indicación de "sin asignar" de modo que el agente podrá acceder al contenido del suceso y llamar a la víctima si el caso es

de mucho interés para solicitar su comparencecnia o la aportación de documentación extra. Todos los casos se pueden visualizar en un documento ,pdf que se genera.

Además, estos casos, se irán incorporando a un sistema estadístico de forma automatizada por hecho delictivo, teniendo el funcionario actuante que marcar si el caso ha sido asignado para investigación o archivado en comisaría (por falta de indicios, imposiblidad de investigar, etc.) cerrado con resultados, tanto si se ha esclarecido con identificado o detenido o se ha aportado información relevante al usuario y, finalmente, cerrado "sin infracción" (al tratarse de un reporte, una tentativa o una comunicación o faltar algunos de los elementos del tipo delictivo). Al lado del caso, figurará un icono "EST" que el funcionario deberá clicar para acceder al estado de la misma. Para visualizar el "caso" se pincha encima del número que queremos ver. Se pueden visualizar casos abiertos y cerrados.

En todo caso, el sistema ofrecerá una estadística de los casos que permanecen abiertos por ser objeto de investigación, y que pasarán a "cerrados" una vez se tenga resolución de los mismos.

El sistema identificará si un escrito es "ampliatorio" por investigaciones posteriores a las ya denunciadas en el caso inicial y aparecerá en color azul o caso de que algún caso sea ampliatorio de otro, en el listado que se genera al realizar la consulta se muestra junto con el número de caso las siglas "Amp" de color **azul**.

También se incorporará un icono a la izquierda del caso para poder saber si el caso ha sido remitido a la Autoridad Judicial correspondiente por LexNet.

- **Pestaña de Detenidos/ Identificados.**

Se incluye también como criterio de consulta básica. Permite consultar detenidos y/o investigados no detenidos o identificados que hayan sido dados de alta, de baja por estos hechos. De esta forma, y teniendo en cuenta que la gran mayoría de partícipes en un suceso a través de Internet no se encuentran ubicados en la demarcación territorial del usuario que denuncia, el agente investigador podrá tener conocimiento de los encartados y su posible ubicación en relación a un número de caso concreto y no por demarcación, como se hace en los sucesos físicos.

Una vez determinados los posibles encartados, investigados, investigados no detenidos, se incluirán dentro de la aplicación Ciberpol, incluyendo el número de Caso al que hacen referencia. Se incluirán todos los datos disponibles sobre el mismo como identidad, documento, domicilio y tipo de suceso. También se podrá consultar por demarcaciones y fechas.

Además, se grabará la decisión judicial de los detenidos que pasan "A disposición judicial", introduciendo los datos sobre el detenido que facilita el Juzgado.

- **Denuncias-Estadísticas.**
  - **Sucesos por plantilla- demarcación.**

Esta consulta considera el nivel del usuario, para restringir las búsquedas, que se podrán llevar a cabo por fechas, limitado a 7 días, y concretar por suceso y demarcación.
Se obtendrá el número de casos abiertos total, por registro online de usuario o abierto en dependencias policiales.

  - **Estadísticas por tipo de suceso- suceso.**

Esta consulta considera el nivel del usuario, para restringir las búsquedas. Permite consultar el número de casos recogidos en una comisaría en una fecha determinada o bien por hecho delictivo concreto en siete días para acotar oleadas de sucesos con incidencia por temporadas como determinados tipo de phishing como la campaña de la renta, muestras de ransomware, etc.

- **Número de Caso.**

Esta consulta no considera el nivel del usuario, para restringir las búsquedas sino que se pueden consultar los casos a nivel nacional.

En esta pantalla seleccionaríamos la provincia, municipio y la plantilla donde queremos realizar la consulta, así como el año y escribiríamos el número de caso a consultar. Se puede visualizar el caso, tanto si está abierto o cerrado, en un fichero descargable tipo .pdf.

- **Usuarios.**

Se pueden consultar los casos a nivel nacional que haya podido realizar el usuario que se ha introducido a través del tipo de documento o apellidos del usuario.

- **Detenidos, investigados no detenidos e identificados.**

Esta consulta al igual que en Usuarios se puede realizar tanto por el tipo de documento como por los apellidos, es decir, visualizaremos la mismas pantallas que para la opción anterior pero para un detenido, investigado o identificado. El motivo de incluir identificados es debido a que la identificación se puede llevar a cabo por el investigador si bien no dispone de domicilio conocido.

- **Identificados.**

Esta consulta al igual que en Detenidos se puede realizar tanto por el tipo de documento como por los apellidos, es decir, visualizaremos la mismas pantallas que para la opción anterior pero se podrá seleccionar Identificado o Menor.

- **Número de agente.**

En esta consulta no considera el nivel del usuario para restringir las búsquedas, por lo que se pueden consultar casos a nivel nacional.

- **Consulta de objetos.**

Esta consulta no considera el nivel del usuario para restringir las búsquedas sino que se pueden consultar los casos a nivel nacional en los que figure el objeto en concreto de la búsqueda. Se van a considerar diferentes niveles de consulta.

Las consultas se realizarán por nivel o campo principal, de modo que una vez seleccionado el mismo, se podrá concretar por subniveles o campos secundarios. Por ejemplo, se podrá hacer una búsqueda por sitio web, y una vez dentro consultar por referencia o alias puesto que si se admiten búsquedas por campos secundarios, por ejemplo, nombres de usuario, pueden parecer cientos de búsquedas que no van a guardar relación entre sí.

En esta pantalla, se abrirá un menú desplegable que permitirá la consulta de varios objetos según el nivel de consulta, presionando el botón de "Buscar". Si el dato es correcto, nos mostrará una ventana con un listado por número de caso donde aparece vinculado el objeto y que podrá consultar, visualizando el mismo a través de pdf. Se podrán visualizar Casos abiertos y cerrados.

Además, del número de caso, aparecerán las características más importantes del objeto o entidad. Por ejemplo, dirección IP, tipo dinámico, operadora MOVISTAR, fecha de consulta, ubicación geográfica.

Cada opción del menú inicial desplegable, estará compuesto de X consultas que aparecerán en subsiguientes pestañas:

A	B	C	D	E	F	G	H	I
CAMPO PRINCIPAL	**Datos web**	**Red social**	**Correo electrónico**	**Teléfono de contacto**	**Direeciones IP**	**Métodos de pago**	**Mensajería Instantánea**	**Otras evidencias digitales**
CAMPO SECUNDARIO	Dominio	Red social	Servicio de correo	Número de teléfono	Dirección IP	Dinero en efectivo	Tipo de serivico	Función hash
	URL exacta de la Página web	Identificador	Dirección remitente	Operador asociado	Localización	Transferencia bancaria	Número	Metadatos
	Identificador o referencia del anuncio o publicación	Usuario	Dirección destinatario	Nombre contacto	Operadora	Tarjeta de crédito/débito o prepago	Conversaciones	
	Persona de contacto	Seudónimo	Iotras direcciones en campos CC/ CCO	Titular		Tarjetas prepago		
			Direcciones IP si es correo coporativo	IMEI		Otros medios de pago: Western Union, PaySafe Card		
						Criptomonedas		

Fig. 4. Hola de Excel con relación esquemática de objetos de Ciberpol.

1.1. Datos web.

- Dominio: especificar el dominio principal
- URL exacta de la página web, correspondiente a la publicación concreta.
- Identificador o referencia del anuncio o publicación
- Persona de contacto

1.2. Red social

- Red social
- Identificador
- Usuario
- Seudónimo

1.3. Correo electrónico

- Servicio de correo
- Dirección remitente
- Dirección destinatario
- Otras direcciones en campos CC/ CCO
- Direcciones IP si es correo corporativo

1.4. Teléfono de contacto

- Número de teléfono
- Operador asociado
- Nombre contacto
- Titular
- IMEI

1.5. Direcciones IP

- Dirección IP. Protocolo IPV4 e IPV6
- Localización
- Operadora

1.6. Métodos de pago

- Dinero en efectivo
- Transferencia bancaria
- Tarjeta de crédito/débito o prepago
- Tarjetas prepago
- Otros medios de pago: Western Union, PaySafe Card
- Paypal, Ebay, etc..
- Criptomonedas
- Cantidad o importe total del beneficio ilícito exigido o pagado.

1.7. Mensajería Instantánea

- Tipo de servicio
- Número
- Conversaciones

1.8. Otras evidencias digitales

- Función hash
- Metadatos
- Grabaciones, vídeos, imágenes, etc.
-

2. Opciones de menú "Formularios".

Referidos a escritos o documentos que acompañarán, o bien a la denuncia, una vez interpuesta, o se entregarán al usuario- denunciante una vez formulada la misma. Cuando clicamos sobre esta opción nos abrirá un documento de Word que una vez completado con los campos correspondientes, generará un documento .pdf.

- Justificante de la denuncia para presentación ante entidad bancaria
- Citación para comparecer en calidad de testigo
- Información de Derechos a la Víctima en el caso de ser víctima o perjudicado por delito.
- Justificante de denuncia.
- Identificación de Detenidos, con la hoja de reseña de Policía Científica.
- Otras formalidades procesales que no son objeto de interés en esta metodología como el Acta de Información de Derechos al Detenido, si lo hubiera.

3. Opciones de menú Caso por web.

3.1. Listado de Casos.

Se muestran los casos abiertos por el usuario vía web en estado "Pendientes" y Listadas asignadas a la plantilla del usuario, en el tercer caso del sistema de registro: DNI y filiación sin certificado o clave digital.

Al acceder al número de caso escogido, permanecerá abierto 15 días a la espera de ser ratificado en dependencias policiales, tras lo cual *pasará a "Sin infracción",* siendo objeto, no obstante de explotación y uso por parte de los investigadores

En la ventana de "Inicio" de la web se advertirá al usuario de la necesidad de firmar el formulario y que, en caso negativo, no dará lugar al inicio de una investigación y/o puesta en conocimiento de la Autoridad Judicial, luego no tendrá validez. Tampoco se incluirá en el sumatorio estadístico sino como parte del apartado "Sin infracción".

En esta pantalla, si clicamos sobre el botón “Cargar Datos”, nos abrirá una pantalla con la diligencia de la que se trata para que el agente pueda completarlo o modificar alguno de los datos de la misma. No obstante, como ya indicamos al inicio, se generará un número de caso que comenzará por W.

SI el denunciante comparece en dependencias policiales, una vez ratificada por el agente y que figuraba como pendiente, desaparece del listado, pasando la misma a tramitación.

Se puede consultar cualquier caso vía Web desde la opción “buscar” conociendo el número de caso correspondiente.

4. Opciones de menú “Casos”.

4.1. Nuevo.

Se desplegará un menú del principal “Casos” que se ampliará a posteriori en el apartado del menú de la aplicación principal número siete. Cuando pinchamos sobre esta opción se muestra una pantalla donde aparece un número de caso y en la barra de Menú tenemos otra opción que es la de “Casos”, que se tratará de forma amplia en el punto 7. Opciones de menú “Casos”.

En este caso, se tomará un número nuevo de caso si el ciudadano comparece directamente en comisaría.

4.2. Abierto.

Nos mostrará un listado de todos aquellos casos que permanecen abiertos. Se puede dejar abierto para continuar con la investigación o cerrarlo sin remisión a la autoridad judicial, clasificándolo con la etiqueta “sin infracción”.

Una vez se cierre cualquier caso, se generará una pantalla para “Confeccionar estadística”.

4.3. Salir del Caso.

Utilizaremos esta opción para salir del caso Nuevo o Abierto.

4.4. Gestión de detenidos, investigados no detenidos e Identificados

4.4.1. Añadir Nuevo.

En la pantalla introduciremos todos los datos necesarios para poder dar de alta al sujeto rellenando los Datos de Entrada, Datos de Identificación y los Datos de Salida.

Una vez introducidos todos los datos necesarios, contrastaremos con la base de datos de SIDENPOL, de denuncias ciudadanas, para cumplir con la función de autocompletado, generando el resto de datos si se dispone de ellos, desde la aplicación.

5. Opciones de menú "Casos"

Otra de las opciones importantes de la aplicación será la posibilidad de cargar plantillas previamente confeccionadas por modus operandi o tipología delictiva, a lo que hemos denominado "Caso".

5.1. Para Caso Nuevo

Si pulsamos sobre Casos nos aparecen todas las plantillas que se pueden generar. Lo importante de estas plantillas es que, debido a los tecnicismos y complejidad de ciertas materias y comportamientos criminales, es necesario el empleo de ciertos registros configurados previamente para que soliciten los datos necesarios que no pueden ser obviados en la toma de la denuncia.

De la misma forma, cuando el usuario ingrese desde la web externa, podrá acceder a estas plantillas configuradas por defecto que le servirán de guía para el completado de los campos solicitados. Además, al lado de cada campo figurará un menú de ayuda para saber cómo debe introducirse el dato requerido, el formato adecuado y el lugar desde dónde debe obtenerse el mismo en la web. Por ejemplo, en el "campo URL": "*colóquese sobre la dirección web específica en la que puede observar el contenido denunciado y copie íntegramente la dirección en el formulario*".

- **Campos genéricos del Caso Específico**

Se rellenarán los datos correspondientes a la identidad del denunciante una vez cargada la plantilla y asignado un número de caso. Por motivos de espacio y temática de este Trabajo, se van a obviar cuestiones de desarrollo más específicas sobre el rellenado de ciertos campos que no aporten detalles sobre la propia metodología expuesta.

Todos los casos estarán compuestos de varias pestañas o subapartados, si bien, por el carácter específico del mismo, pueden añadir o modificar otros campos, siendo éstos:

- **Datos del usuario o denunciante**. Correspondientes a la identidad y domicilio.
- **Localización del hecho**. En el caso de desconocerlo, se tendrá en cuenta el domicilio del denunciante. Se indicará, en mayor medida, la fecha y hora exacta en la que ocurrieron los hechos.
- **Suceso:** Tipo de hecho o delito cometido, que veremos más detalladamente.
- **Salvaguarda de evidencias.** Servicio de timestamping a través de un tercero de confianza que preste servicio al Ministerio del Interior.
- **Descripción general del suceso.** Un campo de libre redacción para describir

cualquier circunstancia de relevancia en la denuncia.

- **Cierre o remisión.** Quedará en el estado de "pendientes", a la espera de ser revisado por el grupo de tecnológicos o policia judicial encargada de su investigación o será remitido, si procediere, directamente a la Autoridad Judicial. Además, se incluirá un botón para volcar la información precisa del caso en la Estadística.

5.2. Apartado "Suceso" por Caso Específico.

A continuación, vamos a exponer cómo sería el apartado "Suceso" de los diferentes casos específicos que se pueden realizar dentro de este apartado.

Una vez que lleguemos a la pestaña "Suceso", se ofrecerán en el mismo apartado, una serie de indicaciones dirigidas al agente o usuario, de forma que pueda identificar qué tipo de Suceso penal podría estar incardinada la actividad que pretende denunciar.

Se mostrará un "Aviso" para que en el caso de que no se reporte el hecho en el Suceso adecuado, la denuncia será "recalificada" convenientemente, por lo que el usuario no debe preocuparse nada más que de reportar y comunicar la mayor cantidad de datos posible y de la importancia de que se realice correctamente.

Durante el proceso de reporte, se le mostrarán los campos convenientes necesarios para su investigación posterior. Si el sistema no le permite continuar, al no rellenar los campos obligatorios marcados con una asterisco *, es porque con la información que puede aportar, no existen datos o evidencias digitales suficientes para ubicar el hecho concreto en la Red y proceder con la investigación pertinente.

Antes de proceder al envío del "Formulario", la aplicación le solicitará que envíe los archivos de los que disponga e indique el origen o la forma de obtención de los mismos.

El usuario se introduce clicando sobre el icono con un lápiz que nos va a mostrar una lista o menú desplegable con todas las calificaciones posibles sobre ciberdelitos para poder seleccionar las que sean necesarias para este tipo de denuncia. Este menú constará de los siguientes submenús:

1. Fraude.
2. Delito contra la Intimidad.
3. Fuga de información.
4. Daños y ataques informáticos. Intrusiones en sistemas e infecciones por malware o virus informático.
5. Distribución de pornografía infantil.
6. Extorsión.
7. Acoso.
8. Redes sociales.

9. Propiedad intelectual e industrial.
10. Otros delitos.

Por “Suceso”, se activarán una serie de campos que deberán ser rellenados por el usuario o el agente. Algunos de ellos, y dependiendo del tipo de “Suceso” serán preceptivos (lo que indicaremos en el presente trabajo con “*”), de forma que si esa información se desconoce o no se aporta, no se permitirá el envío del formulario.

En cada uno de los campos se ofrecerá un “Menú contextual” o un apartado de “Ayuda” para que el usuario o agente detallen correctamente el dato solicitado.

5.2.1. Apartado “Suceso”. Fraude.

“Ayuda”. Qué se incluye en este “Suceso”. Definición de fraude. Usted ha realizado el pago de una contraprestación por un servicio o bien que no ha recibido, mediando cualquier tipo de engaño entre la víctima y el autor. Están incluidas otras formas de actuación del delincuente pero siempre que medie un engaño hacia el perjudicado y una afectación real de su patrimonio. Si no se ha llegado a producir la pérdida patrimonial, reporte a través de los canales de reporte de la página oficial por correo electrónico.

- ***** Campo: Web del servicio donde se ha producido el servicio o la compra.
  “Ayuda o menú contextual”: Compruebe con exactitud la barra de direcciones del navegador de la página web donde ha adquirido el servicio, la compra o transacción. Algunos atacantes simulan ser empresas conocidas para generar confianza. Copie y pegue el nombre de la web o dominio principal con formato: www.XXX.es/.com/etc de la barra de direcciones del navegador mediante botón derecho del ratón “Copiar” y péguelo en este campo mediante el mismo proceso.
- ***** Campo: Identificador o referencia del anuncio o publicación. Ayuda. Localizar el identificador del anuncio, el usuario, el canal, el número de referencia que consta en el perfil del autor. En caso de no identificarlo, sitúese sobre la barra de direcciones exacta del navegador y copie la dirección del anuncio o servicio.
- Campo: Descripción del autor: identidad, identificador web, nombre o alias, domicilio. Aporte todos los datos de los que disponga. Serán campos tasados: Alias, nombre de usuario, nacionalidad, tono de voz, acento, etc.
- Campo: Servicio de correo utilizado. Autor y víctima.
  Gmail, Outlook, dominios corporativos, otros. Mantener formato: dominio@
- Campo: Número de teléfono e IMEI del terminal de autor y víctima.
- Campo: Direcciones IP.
  Formato IPV4 e IPV6. Especificar fecha y hora exacta (husos horarios).
- Campo: Contenido de conversaciones.

Mensajería instantánea, mensaje directo, o email. Detallar: servicio utilizado en la conversación (página web) o aplicación empleada.

- *Campo: Métodos de pago. Autor y víctima

Dinero en efectivo, transferencia bancaria. Entidad/es, tarjeta de crédito/débito o prepago, tarjetas prepago, otros medios de pago: Western Union, PaySafe Card y criptomonedas: bitcoin, monero.

Detallar importe total defraudado.

- Campo: Otras evidencias digitales

Archivo hash (firma digital), metadata, grabaciones, etc.

5.2.2. Apartado "Suceso". Delito contra la Intimidad

"Ayuda". Qué se incluye en este "Suceso". Definición de delito contra la intimidad. Puede darse entre parejas pero no necesariamente. Se trata de cualquier vulneración del derecho a la intimidad. ¿Y qué cubre este apartado? Espionaje dentro de la pareja, con acceso y captación o interceptación no autorizada o consentida a sus dispositivos informáticos o aplicaciones de información personal como emails, conversaciones, imágenes, etc., vulnerando o descubriendo su intimidad. No tiene por qué haber difusión posterior.

También está contenido el "sexting" consistente en el envío de mensajes por cualquier vía conteniendo imágenes de la víctima con el fin de dañar su honor e imagen.

En resumen, este apartado abarca cualquier situación que vulnere su intimidad y privacidad a través de la Red y que le cause un menoscabo grave.

- ***** Campo: Web del servicio donde se ha producido la publicación del texto, mensaje vídeo o imagen.

"Ayuda o menú contextual": Compruebe con exactitud la barra de direcciones del navegador de la página web donde se ha publicado el contenido que desea denunciar. Copie y pegue el nombre de la web o dominio principal con formato: www.XXX.es/.com/etc de la barra de direcciones del navegador mediante botón derecho del ratón "Copiar" y péguelo en este campo mediante el mismo proceso.

- ***** Campo: Identificador o referencia del anuncio o publicación donde ha visto sus datos o información personal expuesta.

"Ayuda": Localizar el identificador del anuncio, el usuario, el canal, el número de referencia que consta en el perfil del autor. En caso de no identificarlo, sitúese sobre la barra de direcciones exacta del navegador y copie la dirección del anuncio o servicio.

- Campo: Descripción del autor: identidad, identificador web, nombre o alias, domicilio. Aporte todos los datos de los que disponga. Serán campos tasados: Alias, nombre de

usuario, nacionalidad, tono de voz, acento, etc.

- Campo: Servicio de correo utilizado. Autor y víctima

  Gmail, Outlook, dominios corporativos, otros. Mantener formato: dominio@.
- Campo: Número de teléfono e IMEI del terminal de autor y víctima.
- Campo: Direcciones IP.

  Formato IPV4 e IPV6. Especificar fecha y hora exacta (husos horarios).
- *Campo: Contenido de conversaciones:

  Mensajería instantánea, mensaje directo, o email. Detallar: servicio utilizado en la conversación (página web) o aplicación empleada.

  "Ayuda": Se recomienda aportar en fichero adjunto la evidencia digital de las conversaciones o de las publicaciones que denuncia presentándolo ante funcionario de policía, realizar extracción con Perito Forense Informático o Notario.
- *Campo: Métodos de pago. Autor y víctima

  Dinero en efectivo, transferencia bancaria. Entidad, tarjeta de crédito/débito o prepago. Numeración y entidad, tarjetas prepago, otros medios de pago: Western Union, PaySafe Card y criptomonedas. Bitcoin.
- Campo: Otras evidencias digitales. Hash, metadata.

5.2.3. Apartado "Suceso". Fuga de información.

"Ayuda". Qué se incluye en este "Suceso". Definición de "Fuga de información". Se entiende por fuga de información al uso y/o publicación no autorizada o consentida de información (datos y/o archivos de cualquier tipo) de carácter personal o confidencial en relación a personas, empresas o identidades.

- * Campo: Web del servicio donde se ha producido la fuga de información o exposición de datos.

  "Ayuda o menú contextual": Compruebe con exactitud la barra de direcciones del navegador de la página web donde ha sido publicada o expuesta la información personal o confidencial. Copie y pegue el nombre de la web o dominio principal con formato: www.XXX.es/.com/etc de la barra de direcciones del navegador mediante botón derecho del ratón "Copiar" y péguelo en este campo mediante el mismo proceso.
- * Campo: Identificador o referencia del anuncio o publicación. "Ayuda o menú contextual": Compruebe con exactitud la barra de direcciones del navegador de la página web o perfil de usuario donde ha sido publicada o expuesta la información personal o confidencial. Copie y pegue de la barra de direcciones del navegador mediante botón derecho del ratón "Copiar" y péguelo en este campo mediante el mismo proceso.

- Campo: Descripción del autor: identidad, identificador web, nombre o alias, domicilio. Aporte todos los datos de los que disponga. Serán campos tasados: Alias, nombre de usuario, nacionalidad, tono de voz, acento, etc.
- Campo: Servicio de correo utilizado. Autor y víctima
  Gmail, Outlook, dominios corporativos, otros. Mantener formato: dominio@
- Campo: Número de teléfono e IMEI del terminal de autor y víctima.
- Campo: Direcciones IP.
  Formato IPV4 e IPV6. Especificar fecha y hora exacta (husos horarios).
- Campo: Contenido de conversaciones o información publicada.
  Mensajería instantánea, mensaje directo, o email. Detallar: servicio utilizado en la conversación (página web) o aplicación empleada.

  Se recomienda aportar en fichero adjunto o indicar su ubicación si no tiene acceso directo a la evidencia digital de las conversaciones. Presentarlo ante funcionario de policia, o realizar extracción con Perito Forense Informático o Notario.
- Campo: Métodos de pago. Autor y víctima

  Dinero en efectivo, transferencia bancaria. Entidad, tarjeta de crédito/débito o prepago. Numeración y entidad, tarjetas prepago, otros medios de pago: Western Union, PaySafe Card y criptomonedas. Bitcoin.

  Ayuda: Si hay una solicitud de pago a cambio de la información divulgada, especificar la cantidad. Si consta de pagos fraccionados, incluirlo en el relato libre posterior de los hechos.
- Campo: Otras evidencias digitales. Hash, metadata.

5.2.4. Apartado “Suceso”. Daños y ataques informáticos. Intrusiones en sistemas e infecciones por malware o virus informático.

“Ayuda”. Qué se incluye en este “Suceso”. Definición de daño y ataque informático.

Acceso sin autorización al conjunto o una parte de los sistemas de información, cuando se haya realizado violando alguna medida de seguridad.

Otra de las conductas consiste en borrar, dañar, deteriorar, suprimir, alterar o hacer inaccesibles datos informáticos contenidos en un sistema de información, intencionalmente y sin autorización.

Por último, hace referencia a la utilización de artificios o instrumentos técnicos, sin estar debidamente autorizado, interceptar transmisiones no públicas de datos informáticos que se produzcan desde, hacia, o dentro de un sistema de información.

- *****Campo: Vector inicial de ataque. Especifique la forma en que se ha podido producir el ataque inicial: *insider,* infección por correo electrónico, infección por navegador,

archivo adjunto, vulneración de claves y sistemas de protección de software, código malicioso, virus, sobrecarga del sistema, etc.

- ***** Campo: Web del servicio o sistemas afectados.

  "Ayuda o menú contextual": Compruebe cuáles son los dispositivos y sistemas que han quedado inicialmente inaccesibles, dañados o alterados. Incluya si se trata de hardware o software, servicios web de la empresa, aplicaciones, etc.
- Campo: Descripción del autor: identidad, identificador web, nombre o alias, domicilio.

  Aporte todos los datos de los que disponga. Serán campos tasados: Alias, nombre de usuario, nacionalidad, tono de voz, acento, etc.
- Campo: Servicio de correo utilizado. Autor y víctima

  Gmail, Outlook, dominios corporativos, otros. Mantener formato: dominio@
- Campo: Número de teléfono e IMEI del terminal de autor y víctima
- Campo: Direcciones IP.

  Formato IPV4 e IPV6. Especificar fecha y hora exacta (husos horarios).
- Campo: Contenido de conversaciones:

  Mensajería instantánea, mensaje directo, o email. Detallar: servicio utilizado en la conversación (página web) o aplicación empleada.

  Ayuda: Se recomienda aportar en fichero adjunto la evidencia digital de las conversaciones, los emails recibidos así como una muestra del malware originarios si se conociera o los ficheros infectados. Presentarlo ante funcionario de policia en un dispositivo de almacenamiento externo, o realizar extracción con Perito Forense Informático o Notario.
- *Campo: Métodos de pago. Autor y víctima

Dinero en efectivo, transferencia bancaria. Entidad, tarjeta de crédito/débito o prepago. Numeración y entidad, tarjetas prepago, otros medios de pago: Western Union, PaySafe Card y criptomonedas. Bitcoin.

- Campo: Otras evidencias digitales. Hash y metadata.

5.2.5. Apartado "Suceso". Distribución de pornografía infantil

"Ayuda". Qué se incluye en este "Suceso". Imágenes, vídeos o cualquier tipo de dispositivos que contenga o almacene agresiones, abusos a menores así como la prostitución y corrupción de menores, especialmente en relación con la facilitación de intercambio de material pedófilo y sus redes.

Sea especialmente cuidadoso con el reporte y no distribuya, difunda o almacene material de este tipo en sus dispositivos informáticos.

* Campo: Web del servicio donde se ha identificado o detectado el material pornográfico.

"Ayuda o menú contextual": Compruebe con exactitud la barra de direcciones del navegador de la página web donde ha detectado este contenido. Puede ser también un sistema de mensajería online, red social, juego online, o cualquier servicio conectado a la Red que permita la distribución de contenidos.

Copie y pegue el nombre de la web o dominio principal con formato: www.XXX.es/.com/etc de la barra de direcciones del navegador mediante botón derecho del ratón "Copiar" y péguelo en este campo mediante el mismo proceso.

- Campo: Identificador o referencia del anuncio o publicación.
- Campo: Descripción del autor: identidad, identificador web, nombre o alias, domicilio. Aporte todos los datos de los que disponga. Serán campos tasados: Alias, nombre de usuario, nacionalidad, tono de voz, acento, etc.
- Campo: Servicio de correo utilizado. Autor y víctima
  Gmail, Outlook, dominios corporativos, otros. Mantener formato: dominio@
- Campo: Número de teléfono e IMEI del terminal de autor y víctima
- Campo: Direcciones IP.
  Formato IPV4 e IPV6. Especificar fecha y hora exacta (husos horarios).
- Campo: Contenido de conversaciones:
  Mensajería instantánea, mensaje directo, o email. Detallar: servicio utilizado en la conversación (página web) o aplicación empleada.

  Se recomienda aportar en fichero adjunto la evidencia digital de las conversaciones. Presentarlo ante funcionario de policía, o realizar extracción con Perito Forense Informático o Notario.
- *Campo: Métodos de pago. Autor y víctima

  Dinero en efectivo, transferencia bancaria. Entidad, tarjeta de crédito/débito o prepago. Numeración y entidad, tarjetas prepago, otros medios de pago: Western Union, PaySafe Card y criptomonedas. Bitcoin.
- Campo: Otras evidencias digitales. Hash y metadata.

5.2.6. Apartado "Suceso". Extorsión.

"Ayuda". Qué se incluye en este "Suceso". Definición de extorsión. Una extorsión es obligar a otro a realizar un acto de disposición patrimonial, generalmente una exigencia de dinero o cualquier otro tipo de beneficio, no tiene por qué ser económico, a cambio de realizar u omitir una acción que no es deseada por la víctima. En este apartado incluimos la sextorsion o el ransomware, en el que le obligan a pagar una cantidad de dinero determinada por no divulgar imágenes o archivos de contenido personal o bien al pago de una cantidad para recuperar archivos que han sido cifrados.

Le recomendamos que no negocie ni interactúe con sus extorsionadores; no pague la cantidad demandada; no borre ninguna evidencia digital o conversación que haya mantenido con ellos**.**

- ***** Campo: Web del servicio donde se ha producido o se está produciendo la extorsión.

  "Ayuda o menú contextual": Compruebe con exactitud la barra de direcciones del navegador del servicio web donde ha detectado o recibido la extorsión. Copie y pegue el nombre de la web o dominio principal con formato: www.XXX.es/.com/etc de la barra de direcciones del navegador mediante botón derecho del ratón "Copiar" y péguelo en este campo mediante el mismo proceso.
- Campo: Identificador o referencia del anuncio o publicación. Copie y pegue en este campo la dirección exacta de la URL del perfil donde está publicada la extorsión.
- Campo: Descripción del autor: identidad, identificador web, nombre o alias, número de teléfono, domicilio
- Campo: Servicio de correo utilizado. Autor y víctima
  Gmail, Outlook, dominios corporativos, otros. Mantener formato: dominio@
- Campo: Número de teléfono e IMEI del terminal de autor y víctima
- Campo: Direcciones IP.
  Formato IPV4 e IPV6. Especificar fecha y hora exacta (husos horarios).
- Campo: Contenido de conversaciones:
  Mensajería instantánea, mensaje directo, o email. Detallar: servicio utilizado en la conversación (página web) o aplicación empleada.
  Se recomienda aportar en fichero adjunto la evidencia digital de las conversaciones. Presentarlo ante funcionario de policía, o realizar extracción con Perito Forense Informático o Notario.
- *Campo: Métodos de pago. Autor y víctima
  Dinero en efectivo, transferencia bancaria. Entidad, tarjeta de crédito/débito o prepago. Numeración y entidad, tarjetas prepago, otros medios de pago: Western Union, PaySafe Card y criptomonedas. Bitcoin.
  Detallar la cantidad total exigida o pagada a los extorsionadores.
- Campo: Otras evidencias digitales. Hash y metadata.

5.2.7. Apartado "Suceso". Acoso.

"Ayuda". Qué se incluye en este "Suceso". Definición de acoso. Se puede dar en varios ámbitos de su vida. En el seno de la pareja, en el ámbito escolar, laboral o por desconocidos. Acosar es acechar, hostigar, perseguir de forma continuada e intrusiva a una persona con el que se pretende establecer o restablecer un contacto personal en

contra de su voluntad. Este tipo de conducta llega a alterar gravemente el desarrollo de la vida cotidiana de la víctima.

- * Campo: Web del servicio donde se ha producido o se está produciendo el acoso. Puede incluir cualquier tipo de acoso, vía web, red social, videojuego o servicio de mensajería instantánea o varios de ellos.

  "Ayuda o menú contextual": Compruebe con exactitud la barra de direcciones del navegador de la página web donde se está produciendo el acoso. Copie y pegue el nombre de la web o dominio principal con formato: www.XXX.es/.com/etc de la barra de direcciones del navegador mediante botón derecho del ratón "Copiar" y péguelo en este campo mediante el mismo proceso.
- *Campo: Identificador o referencia del anuncio o publicación del usuario que le acecha.
- Campo: Descripción del autor: identidad, identificador web, nombre o alias, número de teléfono, domicilio. Especifique cualquier detalle así como si sospecha de alguien en concreto.
- Campo: Servicio de correo utilizado. Autor y víctima.
  Gmail, Outlook, dominios corporativos, otros. Mantener formato: dominio@
- Campo: Número de teléfono e IMEI del terminal de autor y víctima
- Campo: Direcciones IP.
  Formato IPV4 e IPV6. Especificar fecha y hora exacta (husos horarios).
- *Campo: Contenido de conversaciones.
  Mensajería instantánea, mensaje directo, o email. Detallar: servicio utilizado en la conversación (página web) o aplicación empleada.

  Se recomienda aportar en fichero adjunto la evidencia digital de las conversaciones. Este fichero es muy importante. Presentarlo ante funcionario de policía, o realizar extracción con Perito Forense Informático o Notario.
- Campo: Métodos de pago. Autor y víctima.

  Dinero en efectivo, transferencia bancaria. Entidad, tarjeta de crédito/débito o prepago. Numeración y entidad, tarjetas prepago, otros medios de pago: Western Union, PaySafe Card y criptomonedas. Bitcoin.
- Campo: Otras evidencias digitales. Hash y metadata

5.2.8. Apartado "Suceso". Redes sociales.

"Ayuda". Qué se incluye en este "Suceso". Vulneración a los límites a la libertad de expresión: amenazas, delitos contra el honor, contra la integridad moral, y cualquier expresión o conducta en ellas que vulnere los derechos individuales de la persona como la libertad, la integridad moral, dignidad, la intimidad, etc.y qu sean evidenciados o expresados de forma pública en la Red.

- *Campo: Web del servicio o red social.

  "Ayuda o menú contextual": Comprueba con exactitud la barra de direcciones del navegador de la página web donde ha adquirido el servicio, la compra o transacción. Algunos atacantes simulan hacerse pasar por empresas conocidas. Copie y pegue todo el código de la barra de direcciones mediante botón derecho "Copiar" y "pegar" en este campo.
- *Campo: Identificador o referencia del anuncio o publicación
- Campo: Descripción del autor: identidad, identificador web, nombre o alias, número de teléfono, domicilio
- Campo: Servicio de correo utilizado. Autor y víctima

  Gmail, Outlook, dominios corporativos, otros. Mantener formato: dominio@
- Campo: Número de teléfono e IMEI del terminal de autor y víctima
- Campo: Direcciones IP.

  Formato IPV4 e IPV6. Especificar fecha y hora exacta (husos horarios).
- Campo: Contenido de conversaciones.

  Mensajería instantánea, mensaje directo, o email. Detallar: servicio utilizado en la conversación (página web) o aplicación empleada.

  Se recomienda aportar en fichero adjunto la evidencia digital de las conversaciones. Presentarlo ante funcionario de policía, o realizar extracción con Perito Forense Informático o Notario.
- Campo: Métodos de pago. Autor y víctima

  Dinero en efectivo, transferencia bancaria. Entidad, tarjeta de crédito/débito o prepago. Numeración y entidad, tarjetas prepago, otros medios de pago: Western Union, PaySafe Card y criptomonedas. Bitcoin.
- Campo: Otras evidencias digitales. Hash y metadata

5.2.9. Apartado "Suceso". Propiedad intelectual e industrial

"Ayuda". Qué se incluye en este "Suceso". Definición de "piratería digital". Falsificaciones y vulneraciones de derechos de propiedad intelectual e industrial de marcas, nombres comerciales – signos distintivos, patentes, modelos de utilidad, todo tipo de productos. Así como material con propiedad intelectual como obras audiovisuales, piezas musicales, videojuegos, programas de ordenador, revistas, periódicos y libros. Incluye la descarga directa, el visionado en streaming o directos y las Redes P2P.

- *Campo: Web o aplicación del servicio donde se encuentra el material que incumple con los derechos.

  "Ayuda o menú contextual": Comprueba con exactitud la barra de direcciones del navegador de la página web donde ha adquirido el servicio, la compra o

transacción. Algunos atacantes simulan hacerse pasar por empresas conocidas. Copie y pegue todo el código de la barra de direcciones mediante botón derecho “Copiar” y “pegar” en este campo.

- *Campo: Identificador o referencia del anuncio o publicación o del canal donde se encuentre publicado.
- Campo: Descripción del autor: identidad, identificador web, nombre o alias, número de teléfono, domicilio
- Campo: Servicio de correo utilizado. Autor y víctima
  Gmail, Outlook, dominios corporativos, otros. Mantener formato: dominio@
- Campo: Número de teléfono e IMEI del terminal de autor y víctima
- Campo: Direcciones IP.
  Formato IPV4 e IPV6. Especificar fecha y hora exacta (husos horarios).
- Campo: Contenido de conversaciones:
  Mensajería instantánea, mensaje directo, o email. Detallar: servicio utilizado en la conversación (página web) o aplicación empleada.
  Se recomienda aportar en fichero adjunto la evidencia digital de las conversaciones. Presentarlo ante funcionario de policia, o realizar extracción con Perito Forense Informático o Notario.
- *Campo: Métodos de pago. Autor y víctima
  Dinero en efectivo, transferencia bancaria. Entidad, tarjeta de crédito/débito o prepago. Numeración y entidad, tarjetas prepago, otros medios de pago: Western Union, PaySafe Card y criptomonedas. Bitcoin.
  Detallar el coste del material que atenta contra la propiedad intelectual o industrial.
- Campo: Otras evidencias digitales. Hash y metadata.

5.2.10. Apartado “Suceso”. Otros delitos

“Ayuda”. Qué se incluye en este “Suceso”. Suplantaciones de identidad con fines delictivos posteriores. (Si ha sido víctima de un uso ilegítimo de su imagen o datos personales, repórtelo a la red social o medio afectado).

Ciberodio**:** Se alude a cualquier uso de las tecnologías de la información y comunicación (webs, redes sociales, blogs, mensajería instantánea) para difundir mensajes o informaciones antisemitas, xenófobas, homófobas, racistas, intolerantes, extremistas, etc.

- * Campo: Web del servicio donde se encuentra publicado el contenido.

"Ayuda o menú contextual": Compruebe con exactitud la barra de direcciones del navegador de la página web donde se encuentra publicado el contenido. Copie y pegue el nombre de la web o dominio principal con formato: www.XXX.es/.com/etc de la barra de direcciones del navegador mediante botón derecho del ratón "Copiar" y péguelo en este campo mediante el mismo proceso.

- Campo: Identificador o referencia del anuncio o publicación
- Campo: Descripción del autor: identidad, identificador web, nombre o alias, número de teléfono, domicilio
- Campo: Servicio de correo utilizado. Autor y víctima.
  Gmail, Outlook, dominios corporativos, otros. Mantener formato: dominio@
- Campo: Número de teléfono e IMEI del terminal de autor y víctima
- Campo: Direcciones IP.
  Formato IPV4 e IPV6. Especificar fecha y hora exacta (husos horarios).
- Campo: Contenido de conversaciones.
  Mensajería instantánea, mensaje directo, o email. Detallar: servicio utilizado en la conversación (página web) o aplicación empleada.
  Se recomienda aportar en fichero adjunto la evidencia digital de las conversaciones. Presentarlo ante funcionario de policia, o realizar extracción con Perito Forense Informático o Notario.
- *Campo: Métodos de pago. Autor y víctima
  Dinero en efectivo, transferencia bancaria. Entidad, tarjeta de crédito/débito o prepago. Numeración y entidad, tarjetas prepago, otros medios de pago: Western Union, PaySafe Card y criptomonedas. Bitcoin.
- Campo: Otras evidencias digitales. Hash, metadata.

6. Apartado Salvaguarda de evidencias. "Testigo online".

En este proceso técnico, un tercero (de confianza), que no tiene nada que ver con las partes, denunciante y denunciado, valida el momento en el que se produce una comunicación electrónica recogiendo la fecha y hora de inicio, finalización del proceso de captura y la integridad de la grabación resultante (proceso de timestamping). Lo único que permite demostrar es que ciertos contenidos que estuvieron publicados en un sitio web en concreto o una comunicación electrónica no se han modificado en ese intervalo concreto en el tiempo.

La definición legal de "tercero de confianza" se incluyó en el artículo 25 de la ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, que dice que "*las partes podrán pactar que un tercero archive las declaraciones de voluntad que integran los contratos electrónicos y que consigne la fecha y la hora en que*

dichas comunicaciones han tenido lugar (…). El tercero deberá archivar en soporte informático las declaraciones que hubieran tenido lugar por vía telemática entre las partes por el tiempo estipulado que, en ningún caso, será inferior a cinco años".

El proceso de captura y los parámetros utilizados por este tipo de servicio son rápidos y automáticos. El mínimo técnico y procesal recomendable para este tipo de servicios es que quede constancia de los siguientes datos:

- Nodos que han efectuado la captura. Lo deseable es que la captura se lleve a cabo desde nodos situados en diversas partes del mundo porque si lo hacemos, por ejemplo desde un nodo sito en España y la web está bloqueada para accesos desde nuestro país, la captura será infructuosa. Si el nodo es alemán por ejemplo, el proceso de captura será exitoso.
- Camino empleado por las peticiones. Aunque no vamos a explicar por qué, si nosotros hacemos una petición a un dominio, por ejemplo, www.facebook.com situado en Estados Unidos, el requerimiento va a pasar por otros servidores con diferentes direcciones IP hasta que resuelva el servidor de nombres inicial.
- Los datos relativos a las direcciones IP y dominios sobre los que se ha pasado la petición de captura de pantalla.
- Usuario que ha solicitado la captura, identificado.
- URL a la que se accede.
- Código fuente del contenido web junto con los ficheros generados cifrados mediante función hash SAH256 durante el proceso de captura.
- Capturas de pantalla.
- Fecha de creación del documento electrónico generado.

No obstante, la evidencia electrónica que se genera equivale a un documento privado. Para valorar la fuerza probatoria de estos documentos, debemos referirnos al artículo 326 de la Ley de Enjuiciamiento Civil: "*Los documentos privados harán prueba plena en el proceso cuando su autenticidad no sea impugnada por la parte a quien perjudiquen*".

Por tanto, la evidencia electrónica que se crea no tiene capacidad probatoria en un proceso pues el tercero de confianza solo custodia los documentos electrónicos que genera una de las partes, en este caso la que aporta el documento. Si se impugna la autenticidad de un documento privado, se podrá proponer un medio de prueba que resulte útil y pertinente al efecto. Si se recurre a un perito informático, al final acabas pagando el coste de uno y de otro.

Es por todo ello que, en caso de existir un procedimiento judicial, la cadena de custodia del documento electrónico deberá ser debidamente acreditada mediante una prueba pericial o, al menos, sería lo deseable.

No obstante, dice el mismo artículo 326 de la LEC que: "*Cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrón*ica", que considera al documento electrónico firmado por un tercero de confianza como un documento privado.

En este apartado, CIBERPOL incluye un campo con un servicio externo de timestamping que hemos denominado "Testigo online" a modo de tercero de confianza en el que se deberá insertar la URL exacta de la web, publicación, comentario que queramos capturar. Es necesario rellenar este apartado en los casos en los que el Campo de un determinado Suceso está marcado como Obligatorio con asterisco (*) siempre y cuando el dato que solicite sea la dirección de una URL.

Se ofrecerán las indicaciones adecuadas al usuario para realizar una captura correcta.

6.1. ¿Cómo funcionaría este aplicativo?

El servicio de timestamping ofrecido por un tercero de confianza es un servicio constituido por un tercero independiente que provee de la tecnología necesaria para generar documentos electrónicos que contienen la captura en tiempo real de datos junto a otros asociados a ellos sobre contenidos web y transacciones electrónicas entre el cliente y un tercero a modo de sistema de firma electrónica particular y servicio de timestamping o sellado de tiempo.

Este sistema garantiza la verificación de contenidos por un tercero independiente que garantiza la captura automatizada, íntegra, precisa, real y confidencial de los datos publicados en la Red así como ciertas comunicaciones generadas en ella sin intervención humana.

El propio cliente puede capturar contenidos en tiempo real evitando su posible pérdida ante la volatilidad de la evidencia digital en la Red, garantizando su exactitud e inalterabilidad, manteniendo la cadena de custodia en la adquisición de la evidencia digital.

Aunque inicialmente, el servicio de sellado de tiempo (timestamping) y autenticación web para la expedición de documentos electrónicos de sello o de autenticación de sitios web, garantizando que no han sido manipulados por un tercero de forma maliciosa sería el prestado en la plataforma CIBERPOL, lo deseable sería que esta plataforma externa incluyera en períodos más avanzados los siguientes servicios:

a) Firma digital privada para vincular los datos de verificación de firma a un firmante.
b) Servicio digital de entrega online, fundamentalmente para las comunicaciones electrónicas por ejemplo, envío de correos electrónicos.

6.2. ¿Cómo está configurado "Testigo online"?

Los datos de configuración y prestación de esta aplicación testigo online son los siguientes:

- Métodos de interacción con el servicio a nivel web (instalado en el cliente), por correo electrónico, por bots de aplicaciones de mensajería instantánea como Telegram.
- Queda constancia de la consulta realizada en el servicio, que puede quedar almacenada o no en el servidor o eliminada en cuanto se entregue el documento electrónico al denunciante.
- Almacena y copia los datos de creación de firma durante siete días, el tiempo durante el cual quedará en estado "pendiente" el caso hasta que se genere un nuevo caso, sea archivado o cerrado sin infracción, por lo que queda bajo la responsabilidad del cliente su almacenamiento y custodia para los usos que requiera una vez finalizado ese plazo si se procede a la descarga de la plataforma.
- El fichero generado con todos los archivos, será remitido a la carpeta del caso generada, de forma que solo se puede efectuar su descarga una vez haya sido admitido para investigación.
- El sistema de Testigo Online garantiza la integridad, confidencialidad y disponibilidad de los documentos generados.
- El sistema es fiable y mantiene unas medidas de seguridad técnicas y organizativas adaptadas a las necesidades.
- Está gestionado por personal técnico cualificado del Ministerio del Interior. A diferencia de los servicios de terceros de confianza que son empresas externas, y a pesar de las auditorías y cumplimiento de normativas a los que están sometidos, la alumna entiende que una empresa tercera no debe recibir información de carácter personal, confidencial y almacenar en sus bases de datos informaciones que hagan referencia a materias penales.

6.3. Especificaciones técnicas de "Testigo online".

A. Captura de sitios web. Opciones de configuración.

- Permite elegir la ubicación por país de un número determinado de nodos de salida para obtener la web, por ejemplo para certificar geobloqueos y para evitar manipulaciones del contenido.
- Otros terceros de confianza, prestadores de servicios no cualificados, utilizan unos rangos IP definidos que podrían ser identificados fácilmente para mostrar un contenido manipulado si fuera de interés del propietario de la web.
- Captura del tráfico de navegación desde el nodo de captura hacia la web objeto y firma de esta.
- Captura de la web objeto con tres motores distintos para prevenir errores de visualización respecto a un usuario real.

- Una vez se realiza la captura en el servidor, se genera un acta de navegación con el tráfico generado y las capturas en vídeo que son enviadas al usuario.
- Permite la captura de webs publicadas en la DeepWeb (Tor, I2P, Freenet).

B. Informe de actividad de cuentas de Twitter e Instagram (públicos)

- Descarga del timeline completo de un usuario y elaboración de un dossier firmado con el contenido obtenido y las métricas obtenidas según disponibilidad como puede ser: cliente utilizado, distribución geográfica, distribución horaria, etc.

6.4. Efectos jurídicos del documento que se genera.

Testigo online no constituye un sistema de firma electrónica cualificada (reconocida por el eIDAS) basada en un certificado cualificado y generada mediante un dispositivo cualificado de creación de firma por lo que, por sí solo, el documento generado no tiene una presunción de autenticidad: en un procedimiento judicial será la parte la que deberá demostrar que su validez (carga de la prueba) y no la contraparte.

Sin embargo, el tipo de firma electrónica simple aportado por Testigo Online no puede ser rechazada jurídicamente por el mero hecho de que:

- Se presente en forma electrónica;
- No se base en un certificado cualificado;
- No se base en un certificado expedido por un proveedor de servicios de certificación acreditado.

7. Apartado “Descripción general del suceso”.

Este apartado tendrá que ser rellenado por el usuario a través del servicio web o por el agente actuante en la oficina de denuncias. Será lo que aparezca posteriormente en el cuerpo central del Caso o denuncia, siendo de redacción libre.

8. Apartado Cierre y Remisión.

En este apartado se incluirán varios subapartadados. Una vez rellenado los campos anteriores, el usuario o agente tendrán la posibilidad de “Generar informe”, tras lo cual, se creará un archivo .pdf con los datos aportados durante el reporte del caso. Además, se habilitará un cauce para “Adjuntar archivos”, en formato documento de texto, imagen y vídeo para que se puedan adjuntar aquellos ficheros referidos con posible interés procesal para el caso como jusitificantes bancarios, de compra, etc. Recordaremos en una ventana emergente antes de adjuntar cualquier archivo que los pantallazos no tiene validez procesal, si bien podrán ser incluidos como valor investigativo.

Aquí cambia el procedimiento habitual ya que si bien el Art. 284 obliga al "archivo", a efectos procedimentales, una vez cumplimentada la denuncia, el agente de la oficina de atención sólo dispondrá de dos opciones: remisión a la Autoridad Judicial o curso "Investigación", permaneciendo abierto el mismo 72 horas desde su rececepción. Será el agente de policia judicial especializado quien determine si pasa a ser "Sin Infracción", " Archivado o cerrado" o " Investigación en curso" y remitirlo finalmente a la Autoridad Judicial en el curso de 72 horas o bien cerrarlo para abrir otro que figure como "Ampl*" (Ampliatorio") en la plataforma, ampliatorio al "Investigación en curso", ampliando al ya cerrado para dar cuenta a la Autoridad Judicial.

Si bien, a efectos estadísticos, el caso nuevo se incluye dentro del tipo de suceso que se le haya asignado inicialmente, puede ser "recalificado" por los agentes especializados ya que pueden darse errores o sesgos por falta de conocimiento tanto del ciudadano usuario que lo haya cumplimentado via web como del propio agente que lo haya confeccionado de forma manual o ratificado en la oficina de denuncias.

9. Otros menús fuera del apartado "Caso". "Diligencias procesales".

Por cuestiones procesales pero que no son de interés para el presente trabajo, incluiremos también algunas diligencias de carácter auxiliar que conforman tradicionalmente un atestado como "Diligencias de trámite". Además, también se incluirá un menú denominado "Encartados" para relacionar a nuestro caso aquellas personas que hayan tenido o vayan a tener algún tipo de participación ya sea en calidad de testigos, identificados, investigados no detenidos, detenidos y menores. Diligencias que requieren una tramitación procesal concreta y que seguirán el mismo tratamiento que la plataforma policial de denuncias SIDENPOL solo que encartados dentro del mismo número de caso.

Desde estos menús, se generarán las pertinentes Actas conformadas con todas las formalidades oportunas como son la presencia del Letrado de Oficio en la toma de declaración del investigado no detenido y detenido, el Acta de Información de Derechos al Detenido e investigado no detenido por infracción penal, Actas de citación, Derechos de las víctimas y perjudicados, etc. que generarán un documento .pdf por separado y que irán unidas al cuerpo del Caso investigado en la base de datos.

10. Opciones de menú "Administración".

10.1. Gestión de Caso.

Desde este menú podremos aperturar un caso siempre y cuando sea un caso "No calificado" o ya en la estadística, anularlo por defecto de forma, Buscar, editar, etc.

También podremos gestionar los campos de “Diligencias procesales” como buscar, darse baja identificados, detenidos,

Consulta de estadísticas por casos abiertos, cerrados, suceso, casos abiertos por web, de forma presencial, informes por Comisaría, demarcación territorial, listar casos en determinados períodos de tiempo, etc.

Se podrán hacer búsquedas selectivas sobre los campos de los objetos de forma que el investigador, una vez abierto el caso, de forma proactiva vaya introduciendo campos, pudiendo alimentar y grabando “objetos” en la base de datos y gestionar coincidencias de estos elementos con otros casos para detectar posibles modus operandi de bandas organizadas, conexiones entre autores, acceder a otra información ya existente en otras investigaciones que permitan la conexión entre plantillas y demarcaciones, etc.

4.1.2. Evaluación

Para evaluar esta metodología, vamos a describir un caso específico de un ejemplo de hecho concreto. Para ello, nos ceñiremos a las herramientas disponibles en la actualidad puestas a disposición por el Ministerio del Interior para que un ciudadano, empresa, víctima de un delito cometido a través de Internet denuncien los hechos.

1. Supuesto de hecho sin CIBERPOL:

Supongamos que la Sra. A ha recibido a las 10:00 horas del día 9 de diciembre, lunes, un mensaje por correo electrónico, supuestamente, de la entidad bancaria Tpres2, desde la dirección Tpress2@bank.com a su dirección de correo corporativo senoraA@spain.es con un enlace a una web falsa http://Tpress2.bank que simula ser la página web del banco TPres2 https://Tpres2.com en el que le solicitan introducir su usuario y contraseña para una actualización de la base de datos de la entidad. La Sra. A, administradora de la empresa SPAIN SL con sede en Logroño, procede con las indicaciones, enviando su clave y usuario a un servidor Apache gestionado por los criminales B. Una vez con las contraseñas en su poder, acceden a la banca online de la Sra. A del banco Tpres2 entre las 10:30 y las 10:45 horas del día 9 de diciembre de 2019 proceden a ordenar 4 transferencias por importe de 20.000 a una cuenta bancaria con número ES45 2100 6574 19 230000000 perteneciente a la entidad bancaria española INT Direct. En esa franja horaria, Sra. A de la empresa también ha recibido dos mensajes a su teléfono móvil personal 600102030 pidiendo la confirmación a dos de las transacciones realizadas, cada una de ellas por 5.000 euros. Asustada, accede a su banca online y se da cuenta que dos de las transacciones bancarias por 5.000 euros cada uno sí han sido autorizadas por banca online empresas sin introducir el código PIN recibido en su teléfono.

La señora A, afligida, llama a la Policia para ver qué puede hacer porque no sabe cómo actuar. En el 091 de Castellón le dicen que debe acudir a una comisaría a denunciar. La señora A pregunta si es posible denunciar por Internet que está de viaje fuera de Logroño y que hasta el viernes 14 de diciembre, no podrá acudir a la comisaría de Logroño a interponer la denuncia. El agente de policia de informa que puede interponer la denuncia en la misma comisaría de Castellón y que “ya se la harán llegar a los compañeros” porque no lo puede hacer por Internet.

Solución al caso SIN la plataforma CIBERPOL:

La señora A, siguiendo las indicaciones del agente de policia, acude a la comisaría de Castellón el martes 10 de diciembre para interponer la denuncia.

Es atendida allí por un agente de policia en prácticas, el cual emplea la aplicación existente para la recepción de denuncias “SIDENPOL”. El agente en prácticas, que no conoce la investigación de delitos cometidos a través de internet, apertura un nuevo caso o “atestado”

en la aplicación con texto libre, y anota en el campo de texto, (tras haber cumplido con ciertas formalidades procesales) que "*la Señora A, mientras trabajaba, a las 10:35 y 10:42 horas del día 9 de diciembre, recibe dos SMS en su número de teléfono móvil 6000102030 en el que le piden la confirmación para dos transacciones por 5.000 euros cada una por importe de 5.000 euros. Que sin saber lo que está pasando, accede a la banca online de su banco de la empresa y se percata que se han realizado de forma no autorizada dos transferencias de 5.000 euros cada una. Que no sabe cómo se ha podido ocurrir y que nunca ha perdido la documentación bancaria*". Fin de la denuncia.

Por otro lado, la Señora A no sería la única víctima puesto que en esa campaña de phishing, los criminales habrían conseguido acceder durante los 4 días de esa semana a otras 10 cuentas bancarias y hacer trasferencias por importe total de 220.000 euros. Beneficios ilícitos que fueron retirados por las mulas, titulares de las cuentas bancarias ES45 2100 6574 19 230000000 y ES45 2100 6574 19 25000001.

A posteriori, por cauces internos y al comprobar inicialmente, a falta de otros datos, que la denunciante tiene domicilio en Logroño, la denuncia sería remitida al grupo especializado de investigación tecnológica de la Jefatura de la Rioja, donde varios días más tarde, aproximadamente el jueves, día 13, llegaría al grupo de policia judicial competente.

Posteriormente, los agentes encargados de su investigación con el número de atestado concreto, accederían a SIDENPOL para consultar la denuncia, disponiendo únicamente como línea de investigación de la numeración de la cuenta bancaria ES45 2100 6574 19 230000000 de INT Direct.

Posteriormente, habría que contactar con la denunciante para ampliar la denuncia, poder determinar cómo obtuvieron los criminales las contraseñas, esperar a la respuesta de INT Direct sobre la titularidad bancaria de la cuenta beneficiaria e identificar a su titular meses más tarde. Además, tampoco se tendría conocimiento de la existencia de otros ataques, al hacer la consulta al sistema de inteligencia policial por el número de cuenta bancaria y comprobar que solo consta una única denuncia más por hechos similares con transacciones por importe de 10.000 euros.

Hay alguna plantilla que no dispone de grupo especializado y el caso está pendiente de asignar y sin investigar. Los otros 8 casos empleaban la segunda cuenta beneficiaria con lo que no ha sido posible determinar si existe algún tipo de relación entre ambas cuentas y, por lo tanto, de determinar el alcance de la actuación de la banda criminal y consecuentemente, de reunir más indicios para determinar autorías.

2. Supuesto de hecho con CIBERPOL:

La Señora A llama al 091 y los agentes de policia le informan que a través de la web policia.es existe una plataforma de denuncia online para reportar los hechos.

La Señora A registraría en el formulario a través de alguna de las tres formas de acceso y tras validar su certificado, clave o identidad, la plataforma CIBERPOL le mostraría un menú para reportar el hecho. La señora A podría dudar inicialmente al optar por el tipo de Suceso pero gracias a la ayuda que cada Suceso aporta al inicio explicando en qué consiste cada acción delictiva, a pesar de que hay un perjuicio patrimonial, optaría por el menú del Suceso "Intrusiones en sistemas informáticos", solicitándole los datos correspondientes a los campos con los objetos vinculados a este tipo de Suceso:

- *****Campo: Vector inicial de ataque. Especifique la forma en que se ha podido producir el ataque inicial: *insider,* infección por correo electrónico, infección por navegador, archivo adjunto, vulneración de claves y sistemas de protección de software, código malicioso, virus, sobrecarga del sistema, etc.

  Al ofrecerle el sistema las anteriores alternativas, es probable que la Señora A recordara que minutos antes a la intrusión había recibido un correo electrónico solicitándole restaurar las contraseñas de su banca online, advirtiendo en ese acto cuál había sido el vector inicial de ataque.

  De este modo, y dado que es obligatorio para el sistema insertar la web de origen, la señora A recuperaría la web maliciosa http://Tpress2.bank.

- ***** Campo: Web del servicio o sistemas afectados.

  "*Ayuda o menú contextual": Compruebe cuáles son los dispositivos y sistemas que han quedado inicialmente inaccesibles, dañados o alterados. Incluya si se trata de hardware o software, servicios web de la empresa, aplicaciones, etc.*

  En este caso, la señora A, al no haber una falta de disponibilidad de alguno de los sistemas, señalaría la web del servicio de banca online de su banco.

- Campo: *Descripción del autor: identidad, identificador web, nombre o alias, domicilio.*

  Aporte todos los datos de los que disponga. Serán campos tasados: Alias, nombre de usuario, nacionalidad, tono de voz, acento, etc.

  En este caso, podría ser factible que indicara el contenido del mensaje de correo electrónico recibido solicitándole las contraseñas. Si hay falta de ortografía, está inglés, etc.

- Campo: *Servicio de correo utilizado. Autor y víctima*.

  En este campo, la víctima detallaría el email donde ha recibido el correo malicioso y un dato importante: el email de los presuntos autores Tpress2@bank.com. *Gmail, Outlook, dominios corporativos, otros. Mantener formato: dominio@*

- Campo: Número de teléfono e IMEI del terminal de autor y víctima.

  La víctima aportaría su teléfono donde ha recibido los SMS con la solicitud de autorización de transferencia

- Campo: Direcciones IP.

  Formato IPV4 e IPV6. Especificar fecha y hora exacta (husos horarios).

- Campo: Contenido de conversaciones:

  Mensajería instantánea, mensaje directo, o email. Detallar: servicio utilizado en la conversación (página web) o aplicación empleada.

  En este caso, la Señora A sabría que tiene que adjuntar los correos electrónicos recibidos así como los SMS a su teléfono.

  Ayuda: Se recomienda aportar en fichero adjunto la evidencia digital de las conversaciones, los emails recibidos así como una muestra del malware originarios si se conociera o los ficheros infectados. Presentarlo ante funcionario de policia en un dispositivo de almacenamiento externo, o realizar extracción con Perito Forense Informático o Notario.

- *Campo: Métodos de pago. Autor y víctima

  Transferencia bancaria de su cuenta a la cuenta de los autores así como la cantidad detraída de la Entidad INT. Además, el sistema le solicitaría adjuntar un informe de la entidad bancaria en el que se documenten las transferencias.

  Campo: Otras evidencias digitales. Hash y metadata. Sin rellenar.

Una vez rellenados los campos del Suceso, el sistema a través de “Testigo online” le solicitaría introducir la URL de la web maliciosa donde se introdujeron las credenciales, obteniendo también una copia sellada sobre el contenido de la web, una muestra exacta que poder analizar detalladamente el formato, aspecto y otros datos de la web maliciosa como teléfonos de contacto, etc.

Gracias a este sistema, en cuestión de unos minutos, la denuncia ya estaría en la base de datos de CIBERPOL con mucha información más que ha sido recogida, entre otras cosas, la posibilidad de poder analizar la web maliciosa en busca de datos.

Por otro lado, gracias a este sistema, las 8 víctimas captadas a través de la misma web, en el caso de reportar los hechos a las autoridades, se hubieran podido analizar los casos, comprobando que existen coincidencias con la web, con dos cuentas bancarias diferentes que están relacionadas con los mismos autores y además, poder agrupar la causa en un solo Juzgado, pudiendo valorar el comportamiento criminal en su conjunto, un mayor perjuicio económico causado y más datos técnicos con los que poder investigar.

Además, los hechos llegarían a conocimiento del grupo de investigación competente en unas horas que podría consultar por domicilio sin necesidad de perder cuatro días en remitir la denuncia al territorio correspondiente.

5. Conclusiones y trabajo futuro

5.1. Conclusiones

Como hemos podido comprobar del caso de uso mostrado con un simple suceso de un phishing con posterior intrusión en un sistema, unos hechos que, por sí solos, son difíciles de abordar y narrar bien en una denuncia, han sido recogidos correctamente a través de CIBERPOL con el único esfuerzo de completar los campos que la aplicación requiere.

Si nos retrotraemos en el tiempo al momento del suceso, hemos podido comprobar cómo el ciudadano, desde su propio domicilio, ha tenido a su alcance una sencilla plataforma con la que reportar un incidente de carácter técnico difícil de abordar. El propio sistema le orienta sobre cómo entender el hecho que acaba de suceder, recoger los datos necesariamente obligatorios para detectar el modus operandi y el origen de la intrusión, proveer a los investigadores de los datos e indicaciones técnicas suficientes para poder hacer indagaciones desde un primer momento y, además, una forma de preservar la evidencia del hecho de forma completa, segura, concreta y objetiva como es el servicio de timestamping.

Asimismo, la víctima no ha tenido que desplazarse, facilitándole un recurso rápido y cómodo para reportar una situación compleja y ha sabido, sin tener conocimientos técnicos, aportar la información necesaria y correcta para los investigadores.

A la fuerza policial le ha supuesto un ahorro de tiempo y recursos humanos, al no requerir de un agente para recoger la denuncia, con el consiguiente aumento de trabajo, y, además, reducir la lista de espera para otras denuncias; no ha tenido que remitirla a otra demarcación, llamar nuevamente a la víctima para que aporte más información y documentación y ha provocado que ocho casos diferentes se puedan investigar de forma coordinada y precisa gracias a la colaboración y los canales de transmisión y búsqueda de la plataforma.

Y por último, estadísticamente, se pueden analizar y tratar los datos de forma concreta, separados por tipos delincuenciales, establecer políticas de prevención, aportar información a entidades bancarias, plataformas de servicios web, etc. para detectar posibles focos de riesgo y vulnerabilidades, tanto técnicas como humanas.

5.2. Líneas de trabajo futuro

Por último, proponer el uso de técnicas de explotación como el análisis del lenguaje natural o el *machine learning* para lograr un mejor análisis y tratamiento de la información obtenida y sus evidencias, determinar modus operandi, la existencia de posibles organizaciones y casos aislados y predecir comportamientos futuros.

El programa podría procesar texto, extrayendo características útiles para su clasificación, utilizando técnicas de Procesamiento del Lenguaje Natural con palabras típicas de la jerga técnica del cibercrimen. Estas características se pasan a un modelo matemático que estima

la probabilidad de match con otros modus operandi en relación a la descripción del tipo delictivo.

Después, se planteará una metodología de trabajo para el establecimiento de posibles modus operandi, líneas de actuación, preservación de evidencias y cruces con otras denuncias presentadas en otras demarcaciones para el estudio de casos de forma individualizada o conjunta. Se intentará obtener unos patrones que puedan ser objetivados a posteriori para su estudio y análisis.

Alternativamente, partiendo del mismo objetivo, el trabajo podría consistir en escalar el estudio para desarrollar una aplicación con panel gráfico e interactivo con el agente de policia y ver qué otros usos se pueden derivar con esta misma metodología para el estudio de los datos de otros perfiles con interés investigativo, analítico y policial.

Se realizarán diferentes analíticas para la aportación de evidencias digitales concretas, así como segmentación de las mismas o ítems evaluables dentro de la propia denuncia mediante la utilización de técnicas Machine Learning y extrayendo tendencias a partir de métodos de *Natural Lenguaje Processing*, se busca encontrar similitudes y diferencias entre los perfiles estudiados, todo ello con el propósito de experimentar los campos de la ingeniería citados, y poder aportar diferentes enfoques para la obtención de resultados predictivos y abrir más caminos dentro de la investigación del cibercrimen.

6. Bibliografía

1. Symantec Corporation. (2018). Nortonlifelock.com. Recuperado el 2 de noviembre de 2019. /https://www.nortonlifelock.com/content/dam/nortonlifelock/docs/about/2017-ncsir-global-results-en.pdf

2. Ministerio del Interior. (Julio 2019). Interior.gob.es Recuperado el 5 de noviembre de 2019. http://www.interior.gob.es/documents/10180/9814700/informe+balance+2019+2%C2%BA%20trimestre.pdf/a21e6daf-c6c4-4b2b-9c11-5ec15cd57954

3. Ministerio del Interior. (Enero 2019). Interior.gob.es Recuperado el 7 de noviembre de 2019. http://www.interior.gob.es/documents/10180/8736571/Informe+2018+sobre+la+Ciber criminalidad+en+Espa%C3%B1a.pdf/0cad792f-778e-4799-bb1f-206bd195bed2

4. Medio de comunicación La Sexta. (19 de julio 2014). Lasexta.com. Recuperado el 9 de noviembre de 2019. https://www.lasexta.com/noticias/sociedad/detenidas-personas-macroestafa-millones-euros-mas-150000-victimas_201409175725ead24beb28d44601c0a7.html

5. Diario “El País”. (13 de junio 2014). Elpais.com. Recuperado el 9 de noviembre de 2019. https://elpais.com/politica/2014/06/13/actualidad/1402647945_476524.html

6. Boletín Oficial del Estado. (2002). Boe.es. Recuperado el 20 de noviembre de 2019. https://www.boe.es/buscar/doc.php?id=BOE-A-2002-13741

7. Identidad Electrónica para las Administraciones. Gobierno de España (2014). Clav@. Recuperado el 21 de noviembre de 2019. https://clave.gob.es/clave_Home/PIN24H/Que-es.html

ANEXO I

	SUCESO	Fraudes	Delito contra la Intimidad	Fuga de información	Daños y ataques informáticos. Intrusiones en sistemas y malware	Distribución de pornografía infantil	Extorsión	Acoso	Redes sociales	Propiedad intelectual e industrial	Otros delitos: apología del terrorismo, suplantaciones
OBJETOS	Web del servicio	* URL exacta de la Página web	* URL exacta de la Página web donde se ha publicado texto, mensaje vídeo o imagen.	* URL exacta de la Página web donde se ha publicado la información	* Vector inicial de ataque. Insider, infección por email, infección por navegador, archivo adjunto, vulneración de claves y sistemas de protección de software, código malicioso, virus, sobrecarga del sistema	* URL exacta de la Página web donde se ha localizado el material pornográfico	* URL exacta de la Página web donde se ha publicado la información	* Web del servicio donde se ha producido o se está produciendo el acoso.	* URL exacta de la red social o sus servicio web	*Web o aplicación del servicio donde se encuentra el material que incumple con los derechos	* Web del servicio donde se encuentra publicado el contenido.
	Identificador del servicio web	* Identificador o referencia del anuncio o publicación	* Identificador o referencia del anuncio o publicación	* Identificador o referencia del anuncio o publicación	* Web del servicio o sistemas afectados	* Identificador o referencia del anuncio o publicación	* Identificador o referencia del anuncio o publicación	* Identificador o referencia del anuncio o publicación	* Identificador o referencia del anuncio o publicación o del usuario o canal	*Identificador o referencia del anuncio o publicación	* Identificador o referencia del anuncio o publicación
	Autor	Persona de contacto y posible autor: identidad, identificador web, nombre o alias, número de teléfono, domicilio	Persona de contacto y posible autor: identidad, identificador web, nombre o alias, número de teléfono, domicilio	Persona de contacto y posible autor: identidad, identificador web, nombre o alias, número de teléfono, domicilio	Persona de contacto y posible autor: identidad, identificador web, nombre o alias, número de teléfono, domicilio	Persona de contacto y posible autor: identidad, identificador web, nombre o alias, número de teléfono, domicilio	Persona de contacto y posible autor: identidad, identificador web, nombre o alias, número de teléfono, domicilio	Persona de contacto y posible autor: identidad, identificador web, nombre o alias, número de teléfono, domicilio. Añadir posibles sospechosos.	Persona de contacto y posible autor: identidad, identificador web, nombre o alias, número de teléfono, domicilio	Persona de contacto y posible autor: identidad, identificador web, nombre o alias, número de teléfono, domicilio	Persona de contacto y posible autor: identidad, identificador web, nombre o alias, número de teléfono, domicilio
	Servicio de correo utilizado. Autor y víctima	Gmail, outlook, dominios corporativos, otros.	Gmail, outlook, dominios corporativos, otros.	Gmail, outlook, dominios corporativos, otros.	Gmail, outlook, dominios corporativos, otros.	Gmail, outlook, dominios corporativos, otros.	Gmail, outlook, dominios corporativos, otros.	Gmail, outlook, dominios corporativos, otros.	Gmail, outlook, dominios corporativos, otros.	Gmail, outlook, dominios corporativos, otros.	Gmail, outlook, dominios corporativos, otros.
	Número de teléfono e IMEI del terminal de autor y víctima	Teléfono e IMEI de contacto	Teléfono e IMEI de contacto	Teléfono e IMEI de contacto	Teléfono e IMEI de contacto	Teléfono e IMEI de contacto	Teléfono e IMEI de contacto	Teléfono e IMEI de contacto	Teléfono e IMEI de contacto	Teléfono e IMEI de contacto	Teléfono e IMEI de contacto
	Direcciones IP	Direcciones IP atacante	Direcciones IP atacante	Direcciones IP atacante	Direcciones IP atacante	Direcciones IP atacante	Direcciones IP atacante	Direcciones IP atacante	Direcciones IP atacante	Direcciones IP atacante	Direcciones IP atacante
	Conversaciones contenido	Contenido de conversaciones: Mensajería instantánea, mensaje directo, o email	Contenido de conversaciones: Mensajería instantánea, mensaje directo, o email	Contenido de conversaciones: Mensajería instantánea, mensaje directo, o email	Contenido de conversaciones: Mensajería instantánea, mensaje directo, o email	Contenido de conversaciones: Mensajería instantánea, mensaje directo, o email	Contenido de conversaciones: Mensajería instantánea, mensaje directo, o email	Contenido de conversaciones: Mensajería instantánea, mensaje directo, o email	Contenido de conversaciones: Mensajería instantánea, mensaje directo, o email	Contenido de conversaciones: Mensajería instantánea, mensaje directo, o email	Contenido de conversaciones: Mensajería instantánea, mensaje directo, o email
	Métodos de pago. Autor y víctima	*** Métodos de pago.** Especificar cuenta, numeración o billetera	**Métodos de pago.** Especificar cuenta, numeración o billetera	**Métodos de pago.** Especificar cuenta, numeración o billetera. Detallar cantidad defraudada.	***Métodos de pago.** Especificar cuenta, numeración o billetera. Detallar cantidad exacta	**Métodos de pago.** Especificar cuenta, numeración o billetera	*** Métodos de pago.** Especificar cuenta, numeración o billetera. Detallar la cantidad exacta pagada o exigida por los autores.	**Métodos de pago.** Especificar cuenta, numeración o billetera	**Métodos de pago.** Especificar cuenta, numeración o billetera	***Métodos de pago.** Especificar cuenta, numeración o billetera. Detallar el coste del material que atenta contra la propiedad intelectual o industrial	**Métodos de pago.** Especificar cuenta, numeración o billetera
		Dinero en efectivo	Dinero en efectivo	Dinero en efectivo	Dinero en efectivo	Dinero en efectivo	Dinero en efectivo	Dinero en efectivo	Dinero en efectivo	Dinero en efectivo	Dinero en efectivo
		Transferencia bancaria	Transferencia bancaria	Transferencia bancaria	Transferencia bancaria	Transferencia bancaria	Transferencia bancaria	Transferencia bancaria	Transferencia bancaria	Transferencia bancaria	Transferencia bancaria
		Tarjeta de crédito/débito o prepago	Tarjeta de crédito/débito o prepago	Tarjeta de crédito/débito o prepago	Tarjeta de crédito/débito o prepago	Tarjeta de crédito/débito o prepago	Tarjeta de crédito/débito o prepago	Tarjeta de crédito/débito o prepago	Tarjeta de crédito/débito o prepago	Tarjeta de crédito/débito o prepago	Tarjeta de crédito/débito o prepago
		Tarjetas prepago	Tarjetas prepago	Tarjetas prepago	Tarjetas prepago	Tarjetas prepago	Tarjetas prepago	Tarjetas prepago	Tarjetas prepago	Tarjetas prepago	Tarjetas prepago
		Otros medios de pago: Western Union, PaySafe Card	Otros medios de pago: Western Union, PaySafe Card	Otros medios de pago: Western Union, PaySafe Card	Otros medios de pago: Western Union, PaySafe Card	Otros medios de pago: Western Union, PaySafe Card	Otros medios de pago: Western Union, PaySafe Card	Otros medios de pago: Western Union, PaySafe Card	Otros medios de pago: Western Union, PaySafe Card	Otros medios de pago: Western Union, PaySafe Card	Otros medios de pago: Western Union, PaySafe Card
		Criptomonedas	Criptomonedas	Criptomonedas	Criptomonedas	Criptomonedas	Criptomonedas	Criptomonedas	Criptomonedas	Criptomonedas	Criptomonedas
	Otras evidencias digitales	Otras evidencias digitales	Otras evidencias digitales	Otras evidencias digitales	Otras evidencias digitales	Otras evidencias digitales	Otras evidencias digitales	Otras evidencias digitales	Otras evidencias digitales	Otras evidencias digitales	Otras evidencias digitales
		hash	hash	hash	hash	hash	hash	hash	hash	hash	hash
		Metadata	Metadata	Metadata	Metadata	Metadata	Metadata	Metadata	Metadata	Metadata	Metadata