Universidad Internacional de La Rioja
Facultad de Derecho

Máster Universitario en Ciberdelincuencia

Usurpación y suplantación de identidad en el ciberespacio y su impacto en el mundo físico

Trabajo fin de estudio presentado por: Francisco Javier Hortal Sainz De Ugarte
Tipo de trabajo: Trabajo Fin de Máster
Director/a: Dra. Aurelia Carrillo López
Fecha: 10 / 07 / 2023

Resumen

La ciberdelincuencia y la suplantación de identidad son dos de los mayores desafíos que enfrenta la sociedad actual en términos de seguridad y protección de datos. La creciente dependencia de la tecnología y la digitalización de la información han creado nuevas oportunidades para los delincuentes cibernéticos que buscan acceder a información confidencial y cometer delitos en la red.

La ciberdelincuencia hace referencia a cualquier actividad ilegal que se realiza mediante medios electrónicos, como internet o dispositivos digitales. La suplantación de identidad es una de las formas más comunes de ciberdelincuencia, y se produce cuando un sujeto utiliza la información personal de otra persona para llevar a cabo actividades ilegales o fraudulentas en línea. Los delincuentes cibernéticos utilizan diversas técnicas, como la ingeniería social, el phishing y el uso de programas maliciosos como troyanos y malware para cometer sus actividades delincuenciales. Estos delitos pueden tener graves consecuencias para las víctimas, incluyendo pérdida de datos, daños a la reputación y pérdidas financieras. Por lo tanto, es importante estar siempre alerta y tomar medidas para proteger nuestra información personal en línea.

Palabras clave: Ciberdelincuencia, suplantación de identidad, Phishing, Hacking, Spoofing.

Abstract

Cybercrime and identity fraud are two of the biggest challenges facing society today in terms of security and data protection. Increasing reliance on technology and the digitization of information have created new opportunities for cybercriminals seeking to access sensitive information and commit crimes online.

Cybercrime refers to any illegal activity that is carried out through electronic means, such as the Internet or digital devices. Impersonation is one of the most common forms of cybercrime, and occurs when a subject pretends to be someone else to conduct illegal or fraudulent activities online. Cybercriminals use a variety of techniques such as social engineering, phishing and the use of Trojans or other types of malware to commit their criminal activities. These crimes can have serious consequences for victims, including data loss, reputational damage and financial loss. Therefore, it is important to always be vigilant and take steps to protect our personal information online.

Keywords: *Cybercrime, identity fraud, Phishing, Hacking, Spoofing*.

Índice de contenidos

Índice de figuras

Índice de tablas

1. Introducción

El presente Trabajo de Fin de Máster pretende aportar información de principio a fin en torno a la problemática de la ciberdelincuencia y la suplantación de identidad en el mundo interconectado en el que actualmente vivimos.

Comenzando con unas estadísticas actualizadas a 2023 sobre la ciberdelincuencia en España. Trataremos la diferencia existente entre la suplantación y la usurpación de la identidad de un sujeto. Explicando en cada uno de los casos cual es el bien jurídico protegido.

Como afirma ZARATE (2018, p. 2), en los tiempos en que se redacta este artículo ya no correspondería afirmar que los delitos informáticos son un nuevo fenómeno, al menos socialmente. Sí podríamos aceptar que es algo nuevo para el derecho, y para el derecho penal en particular, al menos en relación con el desarrollo doctrinario histórico de esta materia.

Dentro de estos ciberdelitos existen numeras maneras de llevarlos a cabo, el presente trabajo definirá algunas de las actividades delincuenciales más perpetradas.

Existen numerosas herramientas legales y técnicas que pueden llevar a cabo los Jueces, Fiscales y Policías encargados de perseguir este tipo de delitos. Cada una de estas herramientas sería fuente suficiente para elaborar un trabajo en exclusivo para sí mismo, por lo que en esta ocasión se realizará una breve explicación de ellas.

Finalmente, y como colofón al proceso de investigación, se pretende poner en práctica los conocimientos adquiridos durante la realización del presente trabajo mediante el análisis de una denuncia real adjunta en este documento. Aportando posibles líneas de investigación que podrían ser tomadas por los Jueces de Instrucción o las Policías Judiciales.

En el desarrollo de la revisión bibliográfica se logró determinar la importancia de disponer de unos conocimientos actualizados en un mundo tan cambiante y volátil como es el de la ciberdelincuencia. Mundo en el que la legislación y las herramientas de control siempre van un paso por detrás de los delincuentes.

1.1.Justificación del tema elegido

La suplantación de identidad en la red y su relación con la ciberdelincuencia es un tema que desgraciadamente está de actualidad diariamente.

Ninguna persona que habitualmente interactúe con elementos en línea está libre de ser objeto de una de estas modalidades delincuenciales. Por lo que el sector poblacional que puede ser afectado es muy amplio.

Esta problemática es de suma importancia para la comunidad educativa y científica. Siendo la prevención y la formación una de las medidas más básicas y efectivas para combatir esta delincuencia transnacional.

Es por ello que se eligió este tema para la realización del Trabajo de Fin de Máster.

1.2. Problema y finalidad del trabajo

Durante la realización del presente documento se observó que no abundan los documentos actualizados relacionados con este tipo de ciberdelitos, estando la documentación relativa obsoleta o diseminada a lo largo de diferentes documentos en la red.

Con este trabajo se pretende unificar y homogeneizar toda esa información. Ilustrando de principio a fin todas las fases de este tipo de ciberdelitos.

1.3.Objetivos

El objetivo que se pretende con la redacción de este documento es informar a los lectores de las problemáticas existentes con la suplantación y usurpación de identidad, la ciberdelincuencia transnacional, el blanqueo de capitales derivado de estas actividades y cómo se combaten por parte de los Jueces, Fiscales y Fuerzas y Cuerpos de Seguridad que operan España.

2. Marco teórico y desarrollo

2.1. Aspectos generales de la usurpación y suplantación de identidad

2.1.1. Introducción a la ciberdelincuencia y estadísticas recientes

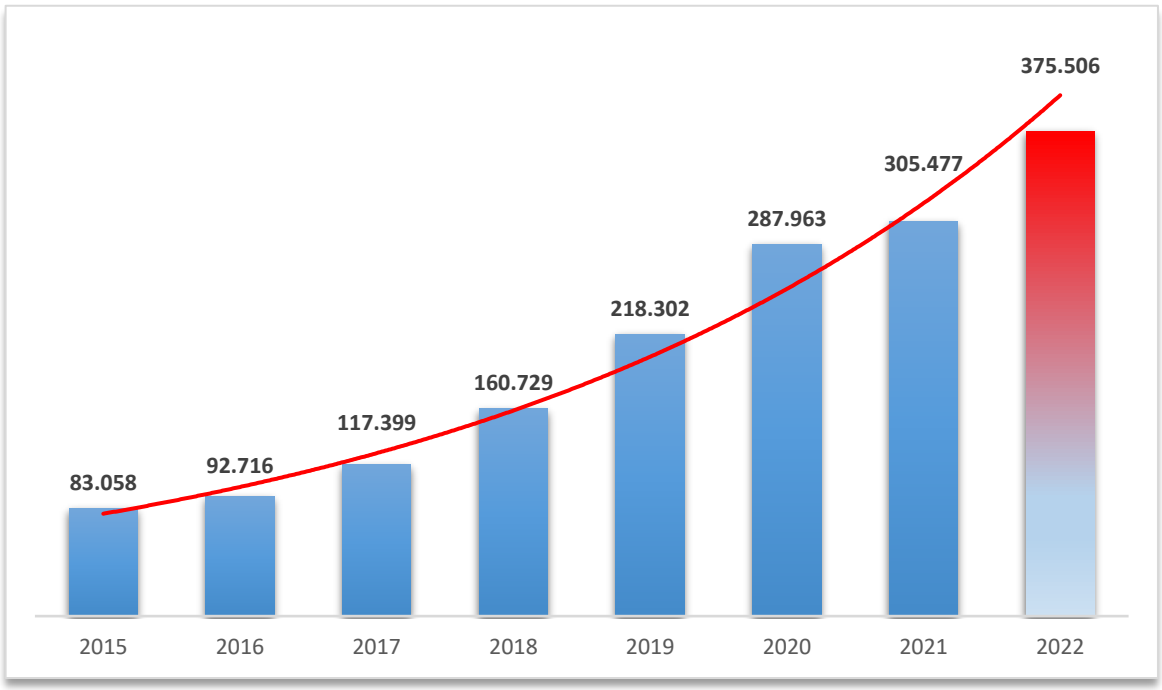
La ciberdelincuencia es un acto delictivo que se lleva a cabo usando las tecnologías de la información y la comunicación «TIC». Los delitos cibernéticos pueden incluir entre otros; acoso escolar, estafas, ciberterrorismo, ataques de malware, delitos de odio y un largo listado de acciones delictivas.

Los delitos informáticos se pueden calificar como las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin.

Se debe tener un aspecto más global del delito informático y tenerlo en consideración desde tres puntos de vista. Como fin en sí mismo, pues el computador puede ser objeto de la ofensa, al manipular o dañar la información que este pudiera contener; Como medio: Como herramienta del delito, cuando el sujeto activo usa el ordenador para facilitar la comisión de un delito tradicional; Como objeto de prueba: Los computadores guardan pruebas incidentales de la comisión de ciertos actos delictivos a través de ellos (DIAZ 2019, p.4).

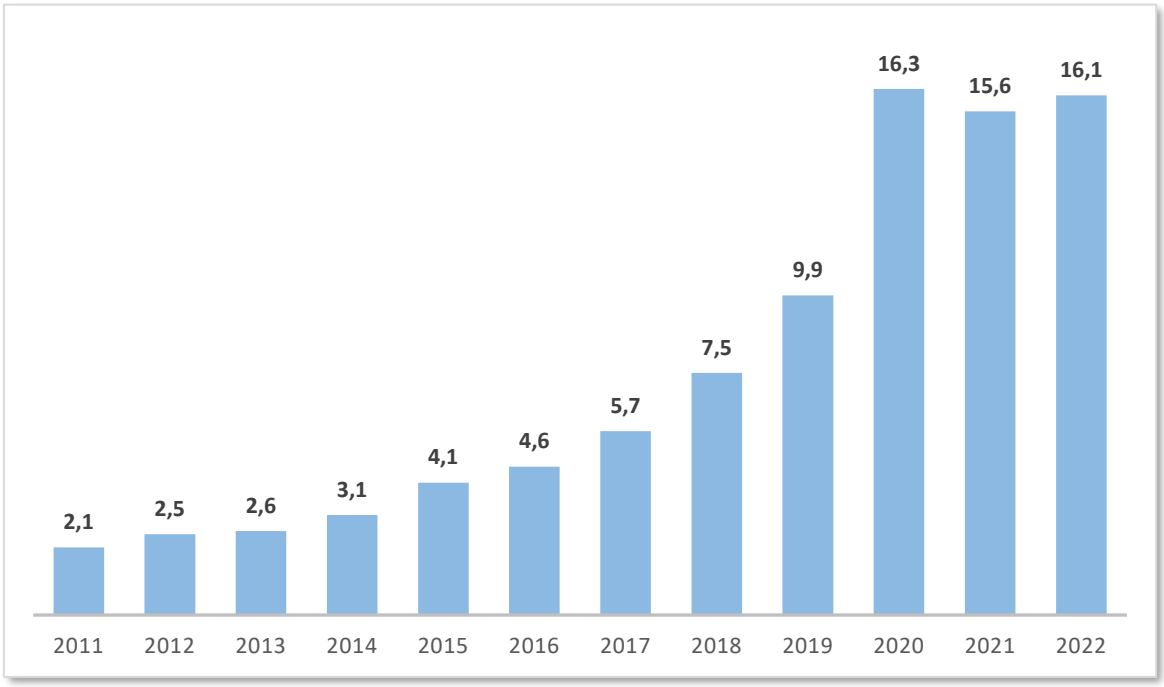
Los datos que muestra el Ministerio del Interior a través de la Secretaría de Estado de Seguridad muestran una clara evolución anual de la cibercriminalidad en España.

Tabla 1. Evolución anual de cibercriminalidad



Elaboración propia. Datos obtenidos del Ministerio del Interior. Estudio sobre la Cibercriminalidad en España 2022.

Tabla 2. Porcentaje de cibercriminalidad sobre el conjunto de la criminalidad



Elaboración propia. Datos obtenidos del Ministerio del Interior. Estudio sobre la Cibercriminalidad en España 2022.

Los datos mostrados anteriormente proceden de la recopilación de información proporcionada por el Cuerpo Nacional de Policía «CNP», la Guardia Civil «GC» y las diferentes Policías Autonómicas existentes en España.

Se aprecia una clara evolución ascendente del traslado de parte de la delincuencia física al mundo virtual. En gran medida producido por el aumento de la interacción social digital de la ciudadanía provocado por el confinamiento de la pandemia de la Covid-19.

2.1.2. Suplantación de identidad

Se trata de acciones donde inicialmente no se pretende propiamente una sustitución completa de la víctima, sino únicamente hacerse pasar por ella en determinados ambientes del ciberespacio, generalmente para realizar otras acciones delictivas. La apropiación indebida suele ser un medio y no un fin en sí mismo.

En principio, no suelen tener consideración delictiva, ya que la infracción penal depende de la acción posterior realizada, por ejemplo, la creación de un perfil falso con fines de cometer delitos como amenazas, revelación de secretos, estafas, injurias, calumnias, etc. Este tipo de hechos delictivos no tiene una vocación de persistencia.

Debido a la modificación del Código Penal Español «CP», artículo 172 ter apartado 5 por la disposición final 2.2 de la Ley Orgánica 1/2023, de 28 de febrero. Se ha tipificado como delito las coacciones en internet producidas por la creación de perfiles falsos.

El que, sin consentimiento de su titular, utilice la imagen de una persona para realizar anuncios o abrir perfiles falsos en redes sociales, páginas de contacto o cualquier medio de difusión pública, ocasionándole a la misma situación de acoso, hostigamiento o humillación.

2.1.3. Usurpación de estado civil

El delito de usurpación de estado civil se encuentra tipificado en el artículo 401 del CP de la siguiente manera: El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años.

Este tipo de conductas requiere una permanencia y la demostración de la afectación plena a la personalidad de la víctima, como la utilización del nombre, documentos o información personal sin el consentimiento del afectado.

El elemento central de esta acción delictiva gira en torno al verbo usurpar, el cual viene recogido por la Real Academia Española «RAE» de la siguiente manera:

1. Apoderarse de una propiedad o de un derecho que legítimamente pertenece a otro, por lo general con violencia.
2. Arrogarse la dignidad, empleo u oficio de otro, y usarlos como si fueran propios.

Existen diversas sentencias que aclaran este hecho delictivo, de acuerdo con la Sentencia del Tribunal Supremo «STS» 635/2009, no basta con usar un nombre y apellidos de otra persona, sino que es necesario hacer algo que solo puede hacer esa persona por las facultades, derechos u obligaciones que a ella solo corresponden, es decir debe arrogarse una cualidad de la que carece, tomándola como propia, y haciendo uso/ostentación pública.

En igual sentido lo afirman las SSTS 669/2009 y 331/2012, al considerar que la acción consiste en simular una identidad o una filiación distinta de la que corresponde al sujeto, ha de ser real y continuada, no una ficción esporádica o momentánea.

De acuerdo con las numerosas sentencias del Tribunal Supremo y acorde con la jurisprudencia que estas sientan, se exigen los siguientes requisitos para que un hecho sea tipificado acorde con el artículo 401 del CP:

- Carácter continuo y persistente de la suplantación de identidad.
- La persona suplantada tiene que ser real y viva.
- Ejercitar los derechos, deberes y acciones jurídicas de la persona usurpada.

2.1.4. Definición del bien jurídico protegido

En el ámbito de la ciberdelincuencia el bien jurídico a tutelar, más que el estado civil, será la apariencia o falacia que crea una persona atribuyéndose la personalidad de otra. Además de tratar de proporcionar la seguridad del tráfico jurídico que se proyecta del estado civil vulnerado.

No obstante, el principal bien jurídico protegido en este tipo de delitos es la fe pública, la cual no es otra que la confianza que la sociedad deposita en determinados signos y formas exteriores que crea el Estado o por su valor probatorio, como por ejemplo un billete monetario o un título universitario.

Este tipo de hechos delictivos solo pueden ser cometidos mediante dolo directo por parte del sujeto activo. Requiriendo la voluntad y el conocimiento de la persona que lo está cometiendo. Quedando descartada la posibilidad de ejecución de manera imprudente.

2.1.5. Regulación internacional

En Europa existen distintas directivas que regulan los datos personales de las personas físicas y su libre circulación de datos «95/46/CE, de 24 de octubre» y la protección de la intimidad en las comunicaciones electrónicas «2002/58/CE, de 12 de julio». Pero a día de hoy se continúa sin regular de manera homogénea la suplantación de identidad digital en la zona euro.

Existen diversos países que han tipificado penalmente este tipo de comportamientos. Bien sea dentro del propio Código Penal como es el caso de Francia, mediante el artículo 226-4-1 o a través de una ley especial en Reino Unido con la norma *Malicious Communications Act.*

Es importante destacar el primer tratado internacional frente a los delitos informáticos es el Convenio de Cibercriminalidad de Budapest del año 2001. Mediante este tratado se ofrece un marco legislativo común a los países firmantes, gracias a la armonización de leyes y el aumento de la cooperación en la investigación de los ciberdelitos.

2.2. Formas de ejecución de la usurpación y suplantación de identidad

En la mayoría de las ocasiones la suplantación de identidad es un requisito previo a la hora de cometer posteriormente otro tipo de actividades delincuenciales. A continuación, se describen los principales métodos de suplantación llevados a cabo en el mundo cibernético.

2.2.1. Phishing

El phishing es un tipo de estafa basada en la ingeniería social gracias a la cual los ciberdelincuentes obtienen información personal y confidencial, generalmente datos bancarios de tarjetas de crédito, haciéndose pasar por una entidad confiable y legítima.

El objetivo de este tipo de delitos es el acceso no autorizado a la información personal de la víctima para cometer posteriormente fraudes, robos de identidad o la instalación de software malicioso.

Figura 1. Esquema ataque Phishing. «VALIMAIL».

Este tipo de ataques dispone de tres componentes, (BELCIC 2020, p. 1):

1- El ataque se realiza inicialmente mediante comunicaciones electrónicas.
2- El atacante se hace pasar por una persona u organización de confianza.
3- El objetivo es obtener información personal confidencial, como credenciales de inicio de sesión o números de tarjeta de crédito.

Estos ataques reciben este nombre debido a que los atacantes salen de pesca «*fishing*» por los océanos de internet. A mediados del siglo XX se realizaban ataques sobre las comunicaciones «*phone phreaking*» tratando de averiguar su funcionamiento. Con el paso del tiempo se fue perfeccionando y la suma de las palabras *Phreaking* + *Fishing* = *Phishing.*

Aunque el medio de comisión de estos delitos o vector de ataque es de lo más variado, generalmente se emplean el SMS, email, redes sociales «RRSS» o sitios web falsificados, el objetivo del atacante es siempre el mismo. Que la víctima haga clic en un enlace, se descargue algún archivo adjunto, introduzca sus datos personales debido a una actualización de seguridad o complete un pago.

2.2.2. Spoofing

El objetivo principal de los delitos de spoofing es hacerse pasar por una entidad de confianza como un banco, empresa o persona particular mediante técnicas de ocultación del remitente.

Como bien explica el autor TORRES (2022, p. 4), un error común es pensar que el *phishing* y el *spoofing* son sinónimos, dado que ambos delitos tienen un componente muy similar. Como ya se ha mencionado anteriormente el *phishing* trata de obtener información personal de la víctima mediante ingeniería social, mientras que el spoofing es una técnica de suplantación de identidad que busca engañar a la víctima para que crea que el mensaje es legítimo. Este tipo de delitos son cometidos mediante plataformas web o canales de comunicación falsos, pudiendo ser catalogados o no como *phishing*.

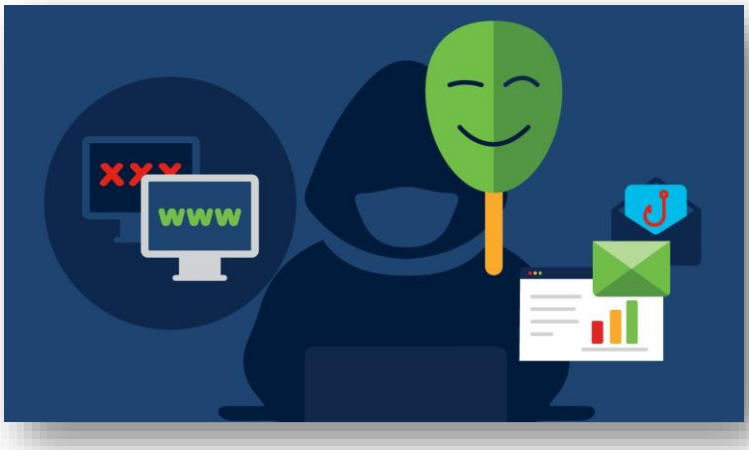


Figura 2. Spoofing. «CISCO».

2.2.3. Pharming

Una de las variantes del *phishing* más difíciles de detectar por la víctima es el *pharming*. El autor y Analista de Sistemas CALLEGARI (2007, p.2) define este tipo de delitos como una modificación del sistema de resoluciones de nombre de dominio del equipo de la víctima, con lo que cada vez que se introduce una URL válida de una página web legítima como por ejemplo una entidad bancaria o tienda on-line, puede que sea redirigida a un sitio fraudulento sin ni siquiera ser consciente de ello.

Al introducir la dirección de una página web www.mibanco.com esta se traduce en un código numérico IP «*Internet Protocol*» por ejemplo 192.168.1.1. La resolución de nombres de páginas web asociada a códigos numéricos es ejecutada por los DNS «*Domain Name Server*». Si se ha sufrido un ataque de *pharming*, el DNS habrá sido modificado por lo que cada vez que se trate de acceder a la página anteriormente mencionada, esta será redirigida a la página fraudulenta sin que la víctima sea consciente por ejemplo 192.168.0.1. De esta manera los atacantes tendrán acceso a las credenciales del sitio web legítimo.

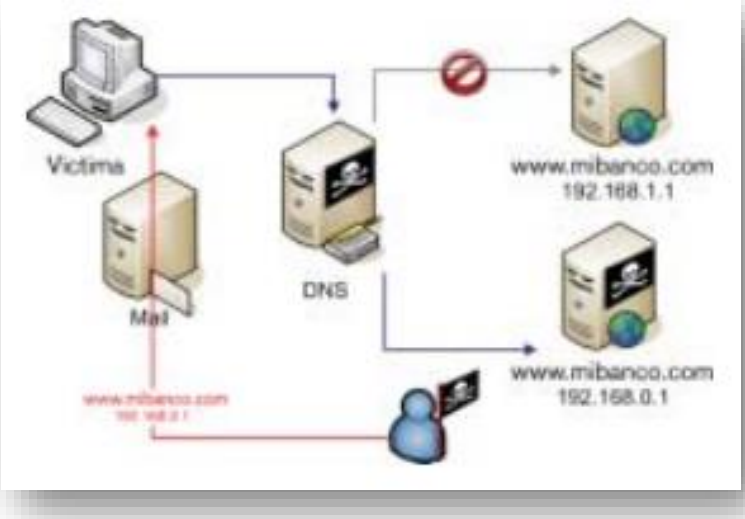


Figura 3. Esquema de Pharming. «.NET report».

2.2.4. Smishing

Un subtipo del delito de *phishing* es el denominado *smishing*, consistente en intentar obtener información privada del sujeto pasivo a través de mensajes de texto en el teléfono móvil. El empleo de esta definición viene determinado por la palabra SMS «*Short Message Service*» unido a la palabra *phishing*.

En este tipo de mensajes de texto fraudulentos se pretende derivar a la víctima a una página web o un número de teléfono malicioso con la intención de obtener sus datos personales.

Figura 4. Ejemplo de smishing. «Bankinter».

2.2.5. Vishing

De acuerdo con VENTURA (2020, p. 22) este tipo de estafas pretende suplantar la identidad afectando a través del VOIP «voz sobre protocolo de Internet IP» recreando una voz automatizada, semejante al de las entidades bancarias. La terminológica del vishing proviene de la unión de *voice -phishing*. Dicha modalidad se produce mediante llamadas tecnológicas suficiente para llamar la atención del usuario para que proporcione información confidencial.

2.2.6. SIM Swapping

Este tipo de delitos pretende secuestrar la línea telefónica de la persona afectada. Consiste en dejar sin cobertura el teléfono móvil y posteriormente clonar la tarjeta SIM de la víctima en otro dispositivo. Los sujetos activos del delito logran hacerse pasar por los titulares de la línea frente a las compañías telefónicas. Obteniendo así el acceso a las aplicaciones vinculadas a la misma, pudiendo realizar un uso fraudulento y beneficiarse de ellas.

Cabe recordar que esta técnica de estafa no está basada en un fallo de seguridad de los dispositivos electrónicos, sino en un procedimiento de verificación de identidad con dudosa rigurosidad en algunas ocasiones. Situación aprovechada por los delincuentes para cometer este tipo de delitos.

2.2.7. Perfiles falsos en redes sociales

En los últimos años las redes sociales se han llenado de estafadores que buscan suplantar la identidad de celebridades, entidades bancarias o marcas conocidas. Suplantando su identidad mediante la creación de perfiles falsos o el secuestro de las cuentas verificadas, con el objetivo de obtener los datos privados de usuarios que interactúen con el perfil suplantado.

Una de las técnicas más empleadas es el *scraping* consistente en monitorizar los comentarios que los usuarios hacen en perfiles de entidades bancarias, aerolíneas y demás cuentas legítimas. Posteriormente los delincuentes realizan la suplantación y contactan con el usuario con el objetivo de robarle la información privada.

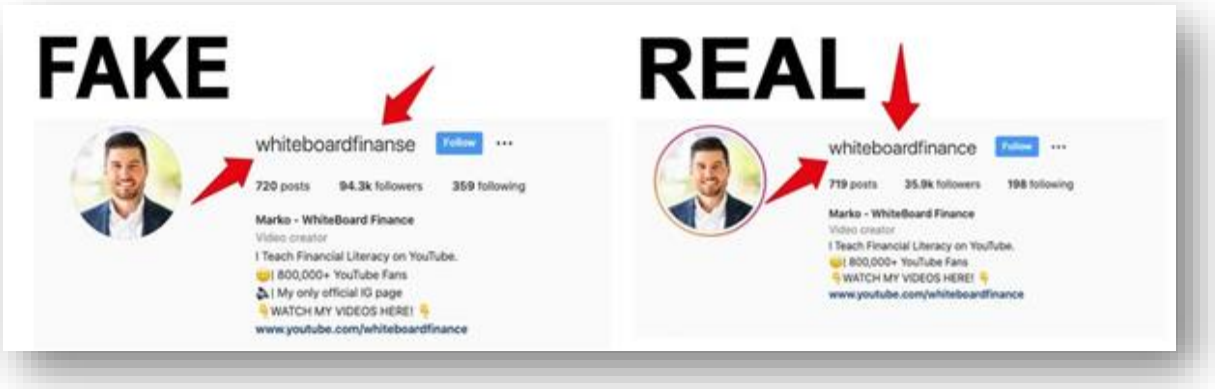


Figura 5. Ejemplo de perfil falso en la red. «Businessinsider».

2.2.8. Cuentas de WhatsApp robadas

La famosa aplicación de mensajería WhatsApp no escapa de los delitos de suplantación. A través de ella los delincuentes se hacen pasar por la víctima y contactan con los números de teléfono y tratan de hacerles creer que su familiar o amigo ha sufrido un percance o un problema en algún aeropuerto y necesitan un préstamo.

2.2.9. Fraude del CEO

No todas las estafas de suplantación se cometen en el ámbito particular de la víctima, una de las estafas empresariales más conocidas es la denominada fraude del CEO. Consistente en engañar a los empleados para que paguen una factura o realicen una transferencia desde la cuenta de la empresa a una cuenta del criminal. Este tipo de ataques tiene como perjudicado secundario a las entidades bancarias, es por ello que estas realizan grandes campañas de formación y sensibilización entre sus clientes. Como puede ser la realizada por Banco Santander en 2021, en la cual se detalla de una manera muy fácil de comprender cómo se pueden sufrir este tipo de ataques con un simple email:

1- Se recibe un email supuestamente de otro empleado o del jefe en el que pide ayuda con una operación confidencial y urgente.
2- El ciberdelincuente emplea una dirección de correo electrónico parecida a la legítima, o incluso suplantada.
3- El contenido transmite sensación de autoridad y de urgencia e incita a actuar rápidamente y en secreto, evitando así que la información pueda llegar a otros empleados.
4- El objetivo final es engañar a la víctima para que realice una o varias transferencias de altas cuantías a la cuenta del criminal, pensando éste que está llevando a cabo una operación lícita.

Para lograr el éxito de esta estratagema se emplea la ingeniería social mediante la recopilación de información de la empresa y sus trabajadores interceptando los mensajes o incluso teniendo acceso a los equipos de la empresa. Este tipo de estafas se suele cometerse por email, pero en los últimos años se están dando casos a través de llamadas telefónicas.

2.3. Medidas para mitigar su comisión

2.3.1. Medidas técnicas para el usuario

A- Concienciación

Uno de los primeros pasos para mitigar la probabilidad de ser víctima de cualquier tipo de ciberdelitos es la concienciación del usuario. El ciudadano debe ser consciente de los riesgos que existen en el mundo virtual y la magnitud de las estafas internacionales.

Estos conocimientos no son adquiridos de la misma manera por las personas denominadas nativas digitales frente a otras con una edad más avanzada por lo que deben realizarse charlas y campañas de información adaptadas a los públicos a las que van dirigidas las mismas. En esta línea de trabajo el Gobierno de España delega gran parte de esta tarea en el Instituto Nacional de Ciberseguridad «INCIBE», el cuál es una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.

Además del trabajo realizado por el INCIBE, una gran parte de la concienciación se logra difundir gracias a las charlas de las unidades especializadas de las Fuerzas y Cuerpos de Seguridad que operan en España, tales como Policía Nacional, Guardia Civil, Policías Autonómicas «*Mossos d'Esquadra*, *Ertzaintza*, Policía Foral de Navarra y Policía Canaria», sin olvidar a las Policías Locales de los ayuntamientos. Estas unidades realizan charlas preventivas orientadas a la concienciación de los ciberdelitos en la red a los alumnos de colegios e institutos, asociaciones de padres y madres, centros de ancianos, universidades y un largo etcétera. Cada charla se orienta al público al que va dirigido, logrando de esta manera tener un mayor calado en los diferentes rangos de edad de la sociedad.

B- Formación

En la actualidad los equipos informáticos, aplicaciones y terminales móviles son elementos de una gran complejidad técnica. Lo que provoca que en muchas ocasiones el usuario únicamente sepa cómo manejar un porcentaje muy reducido de las opciones que estos ofrecen.

Este tipo de equipos deberían llevar aparejada una formación básica relacionada con su correcto funcionamiento, de esta manera se lograría evitar en gran medida las estafas relacionadas con la ingeniería social.

Algunos de los aspectos a destacar en la formación básica a nivel de usuario serían los siguientes:

- Realice compras online en sitios web de confianza. De esta manera evitará la posibilidad de facilitar datos bancarios y personales de manera involuntaria.
- Revise regularmente el extracto bancario en busca de movimientos o cargos sospechosos.
- Almacene los documentos relacionados con las compras online, con el objetivo de disponer de ellos en caso de necesitarlos para demostrar o denunciar una irregularidad.
- No proporcione los datos bancarios salvo que se esté realizando una compra de un producto o servicio online.
- Evite enviar por email información bancaria como el número de la tarjeta o PIN.
- En las redes sociales mantenga su perfil privado.
- No facilite su número de teléfono a personas desconocidas o en webs de dudosa confianza. Incluidos anuncios en redes sociales que prometen una alta rentabilidad.
- Asista a los menores de edad del hogar en la navegación por internet. Se les deberá tutelar de la misma manera que se hace en el resto de ámbitos cotidianos.

C- Equipos actualizados

Algunos de los vectores de entrada de los ciberdelincuentes en los dispositivos electrónicos de las víctimas son a través de vulneraciones de fábrica de los equipos. Las denominadas vulneraciones *Zero Day* se describen por KARPESKY (2022, p.2), como el término "día cero" se refiere al hecho de que el proveedor o desarrollador acaba de conocer acerca de la falla, lo

que significa que ha tenido "cero días" para corregirla. Un ataque de día cero ocurre cuando los hackers aprovechan la falla antes de que los desarrolladores tengan la oportunidad de solucionarla.

A menudo el software dispone de vulnerabilidades, las cuales son aprovechadas por los delincuentes hasta que los desarrolladores son conocedores de ella y proceden a realizar un parche de seguridad que corrija dicha falla. Esto se denomina como código *exploit*.

Por este motivo es necesario disponer de equipos con sistemas operativos actualizados, así como mantener una versión actualizada de las aplicaciones móviles instaladas en los teléfonos.

D- Antivirus

Adquirir un correcto antivirus y mantenerlo actualizado con regularidad es un método muy útil de cara a evitar posibles filtraciones de información desde un terminal, ya sea un teléfono móvil o un ordenador personal.

E- Contraseñas seguras

Se deberán emplear robustas y seguras en los servicios online empleados por el usuario. Cumpliendo los siguientes requisitos se reduce ampliamente el riesgo de sufrir una suplantación de identidad en la red:

- Evitar usar la misma contraseña en más de un servicio o aplicación online.
- Emplear más de 10 caracteres de longitud.
- Incluir símbolos especiales como la «@», el «€», además de letras mayúsculas, minúsculas y números.
- No reflejar datos personales como el nombre o apellido.
- No emplear una palabra conocida del diccionario.
- No debe ser la misma palabra que el nombre de usuario.
- Cambiarlas periódicamente si se tienen sospechas de filtración.

@	[		]	^	_	!
"	#	$	%	&	'	(
)	*	+	,	-	.	/
:	;	{	}	<	>	=
|	~	?	A-Z	a-z	0-9	

Figura 6. Caracteres empleados en contraseñas seguras. «Strato».

F- Activar la verificación en dos pasos

Uno de los métodos más efectivos a la hora de complementar la seguridad de acceso a las diferentes aplicaciones informáticas es el uso de la verificación en dos pasos. Este método de seguridad es un complemento a las contraseñas mencionadas en el apartado anterior.

Una vez introducido el usuario y contraseña de un sistema, si estos son correctos, se solicitará al usuario que introduzca un código único adicional. Este código extra puede llegar al usuario a través de diferentes medios como el SMS, llamada telefónica, una tercera aplicación, códigos de seguridad… Todo ello puede variar dependiendo de la opción elegida por el usuario en la configuración de seguridad de su perfil o por imposiciones técnicas por parte del prestador de servicio.

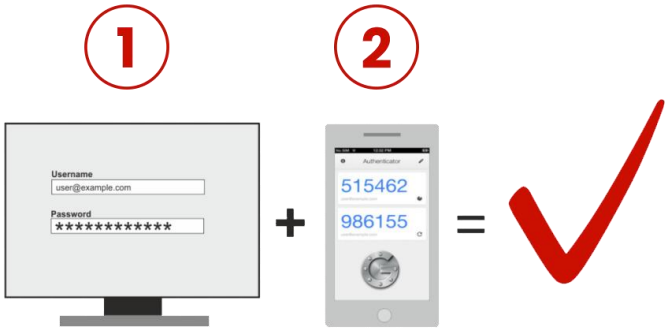


Figura 7. Verificación en 2 pasos. «Protección datos LOPD».

2.3.2. Soluciones a este tipo de problemas

Cabe destacar que este tipo de delitos tiene una problemática de compleja solución, puesto que dispone de varios factores a tratar para poder darle una solución al problema global de las estafas, suplantaciones y usurpaciones de identidad en el mundo virtual.

A continuación, trataremos algunos de los factores que se pueden corregir para mitigar la comisión de este tipo de delitos que se vienen cometiendo desde hace siglos, pero que ahora con la intercomunicación internacional provocada por internet se ha incrementado exponencialmente al interactuar los usuarios con el mundo digital.

A- Cooperación internacional

Con el objetivo de prevenir y combatir la ciberdelincuencia se firmó el Convenio de Budapest, el cual es un tratado internacional adoptado por el Consejo de Europa en noviembre de 2001.

Su objetivo no es otro que el de armonizar las leyes internacionales relacionadas con la ciberdelincuencia y propiciar una colaboración y cooperación real en este tipo de delitos entre los países firmantes del mismo. Este convenio actualmente está ratificado por 67 países.

La Unión Europea adoptó en 2013 la Directiva 2013/40/UE del Parlamento Europeo y del Consejo Europeo del 12 de agosto de 2013 relativa a los ataques contra los sistemas de información. Buscando soluciones a los problemas de cooperación, competencia y efectividad que existían entre los países miembros de la Unión Europea. Además de esta Directiva, posteriormente se fueron tomando diferentes medidas en la misma dirección:

- Directiva NIS/SRI o Directiva sobre ciberseguridad: Directiva «UE» 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
- Reglamento de Ejecución «UE» 2018/151, de la Comisión, de 30 de enero de 2018 que establece normas para la aplicación de la Directiva.
- Reglamento Europeo de Ciberseguridad 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019.
- Agencia Europea de Seguridad de las Redes y de la Información o Agencia de Ciberseguridad «ENISA».

En el año 1998 se creó Europol, es la agencia europea encargada de la lucha contra la delincuencia organizada y el terrorismo, uno de sus aspectos más destacado es la rama de la ciberdelincuencia. La agencia fue creada en 1992 y su sede se encuentra en La Haya, Países Bajos.

Dentro de la amplia gama de capacidades y herramientas de las que dispone Europol, existe la Plataforma Europea de Lucha contra la Delincuencia en Internet «EC3», encargada de la lucha contra la ciberdelincuencia, el fraude informático y la explotación infantil en la red.

Figura 8. EUROPOL y EC3 «EUROPOL».

Como media de respuesta rápida frente a las amenazas en la red, la UE creo un grupo especializado. La Red Europea de Equipos de Respuesta a Emergencias Informáticas «CERT-EU», es el órgano encargado de ayudar a los Estados miembros a prevenir y responder a las ciberamenazas. Dispone de un equipo de personas dedicado a prevenir, detectar y responder rápidamente frente a los problemas o incidentes de seguridad producidos en los sistemas informáticos. Con este equipo de personas se pretende contribuir a que la infraestructura de TIC las instituciones, los órganos y las agencias de la UE sea más segura.

Figura 9. CERT-EU «CERT-EU».

Este tipo de cooperación internacional es un comienzo en la buena dirección, pero es claramente insuficiente. Los ciberdelincuentes conocen la legislación y los acuerdos internacionales y realizan sus actividades delictivas desde países que no han suscrito los mencionados acuerdos o se establecen en auténticos paraísos delincuenciales. A lo largo de la investigación del presente documento se ha podido constatar fehacientemente que gran parte de las suplantaciones de identidad y sus posteriores delitos asociados proceden desde países como Costa de Marfil, Nigeria, Ucrania, Rusia, China entre otros.

Como se puede apreciar ninguno de los mencionados países pertenecen a la UE y tampoco son miembros firmantes del Convenio de Budapest, lo que dificulta enormemente la colaboración internacional en materia policial y judicial a la hora de perseguir los delitos cometidos a través de las redes.

B- Mejoras legislativas

A nivel legislativo existe un largo camino por recorrer hasta alcanzar una seguridad aceptable en el mundo digital.

En el ámbito preventivo de la ciberseguridad existen numerosas herramientas que el legislativo de cada país puede poner en práctica para disponer de soluciones pasivas a estos delitos. Como el endurecimiento de los estándares de seguridad que las empresas y organizaciones deben cumplir para poder operar legalmente en el país, estableciendo sanciones a las empresas que no cumplan estos requisitos impuestos.

La creación de leyes específicas que aborden la delincuencia en las redes. Numerosos países disponen de articulados diseminados a lo largo de diferentes leyes nacionales lo que en algunas ocasiones desdibuja o dificulta una correcta ejecución de las sanciones penales de este tipo de delitos.

Otra de las opciones legislativas disponibles existe la obligatoriedad real de colaboración público-privada, fomentando la relación bidireccional entre el sector público y el privado con el objetivo de compartir la ciberdelincuencia. A día de hoy las empresas privadas colaboran con el sector público de una manera escueta y forzada.

C- Creación de un ID digital general

Una solución al problema de la suplantación de identidad sería la implantación de un identificador digital en todos los ámbitos de interacción que realizamos en la red, desde redes sociales, servicios de mensajería, trámites con la administración o plataformas de entretenimiento entre otras. Este tipo de identificación única ayudaría a prevenir la ciberdelincuencia aportando una mayor seguridad en el mundo online. De esta manera se evitaría ir diseminando información personal por diversos sitios web o servicios en línea que el ciudadano emplee en su día a día. En un ámbito más orientado al sector empresarial, evitaría la suplantación de identidad en la relación cliente-empresa reduciendo así la posibilidad de sufrir una ciberestafa y aportando una mayor seguridad a las comunicaciones.

No obstante, la creación de este ID digital general no está exento de polémica puesto que podría llegar a vulnerar aspectos relacionados con temas tan delicados como la privacidad y la seguridad de los datos personales. Debiendo tener un sistema de seguridad de gran nivel puesto que una filtración de seguridad en sus sistemas provocaría una exposición total de los usuarios adheridos a este sistema.

Analizados los aspectos positivos y negativos de esta medida se puede concluir que es una herramienta con un gran potencial en materia de seguridad informática, pero se debe abordar con cautela y con las medidas técnicas apropiadas a los datos que gestiona.

D- Autenticación en dos pasos 2FA

De acuerdo con el autor SEPULVEDA (2022, p. 7), en las últimas décadas se ha observado una nueva tendencia de evolución en sistemas de autenticación «unifactor o multifactor», su meta es asegurar la información del usuario utilizando métodos de seguridad que respalden su identidad al momento de usar un sistema; sin embargo, esto ha ocasionado que varios perpetradores averigüen la manera de vulnerar dichas seguridades, aprovechando falencias aún no corregidas en los procesos de autentificación.

Es por ello que se ha popularizado el proceso de autenticación de dos factores, conocido también como la autenticación de dos fases o 2FA, por sus siglas en inglés y es definido como el empleo de dos sistemas de autenticación en el ingreso a un sistema para comprobar y validar la identificación del usuario.

En relación a estas técnicas de gestión de accesos, cabe destacar que, al utilizar usuarios y contraseñas como único sistema de verificación y acceso a una plataforma digital, se fuerza a las personas a guardarlas o apuntarlas en algún lugar asequible para disminuir el riesgo de olvidarlas y tener que inventar constantemente contraseñas nuevas y diferentes. Este hecho llega a representar un peligro ya que la contraseña queda al acceso de terceros y como consecuencia queda anulado su alto nivel de seguridad.

Por dicha razón, se recomienda un segundo y tercer factor de autenticación, en el segundo caso se recomienda utilizar elementos de carácter biométrico, entendido como algo que es propio del usuario, como por ejemplo las huellas dactilares, la composición de la retina, la voz o el patrón en los intervalos de pulsación de teclas, mensaje de texto o correo de verificación, preguntas de seguridad.

No obstante, el tener que introducir tres factores de autenticación para acceder a una red social o al correo electrónico es un proceso un tanto incómodo que algunos usuarios no están dispuestos a sacrificar en pos de un incremento de la seguridad en el uso de la misma.

A este posible rechazo de algunos usuarios a la hora de implementar un segundo o tercer factor de autenticación se le debe sumar el incremento en las costas de los servicios que estos sistemas repercuten en las empresas prestadoras de servicios online. Algunas de las cuales son reticentes a este tipo de sistemas de seguridad por su elevado coste económico y la necesidad de soporte técnico de cara al usuario si alguno de estos sistemas falla.

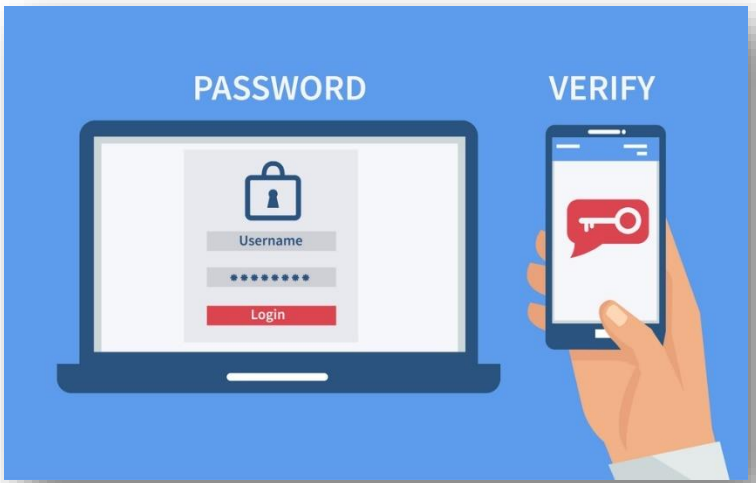


Figura 10. Esquema sistema 2FA «DEISOLTEC».

E- Especialización y refuerzo de las fuerzas policiales

Las personas encargadas de perseguir y combatir en primera línea la ciberdelincuencia son las unidades de la policía judicial de los diferentes cuerpos policiales que operan en cada país.

En el caso de España se disponen de unidades especializadas en función del cuerpo policial en el que operen.

- Policía Nacional: Brigada Central de Investigación Tecnológica «BCIT».
- Guardia Civil: Grupo de delitos telemáticos «GDT».
- Policía Foral de Navarra: Grupo de Delitos Informáticos «GDI».
- Mossos d'esquadra: Unidad de Ciberseguridad «UCIBER».
- Ertzaintza: Sección Central de Delitos en Tecnologías de la Información «SCDTI».

Debido a la alta tecnificación y constante evolución de este tipo de delitos, los cuerpos policiales anteriormente mencionados deben no solo disponer de un número de agentes acorde a la elevada tasa de delincuencia online, sino que debe ir acompañado de una formación técnica de gran calidad y la adquisición de herramientas de trabajo para poder lograr llevar a cabo las investigaciones pertinentes y resolver los delitos cibernéticos.

Un aspecto a mencionar sería la contratación o colaboración con expertos en ciberseguridad de manera más ágil mediante convenios de colaboración con diferentes empresas o intuiciones privadas.

2.4. Persecución de estos delitos en Internet

2.4.1. Respuesta por parte de los cuerpos policiales españoles

Los diferentes cuerpos policiales que operan en España disponen de un gran número de herramientas informáticas que permiten combatir y perseguir los delitos informáticos.

- Software de análisis forense encargado de recuperar y analizar los datos en discos de almacenamiento masivo, equipos informáticos y dispositivos móviles. Pudiendo obtener pruebas digitales dentro de los mismos, permitiendo ser utilizadas en los procesos penales como evidencias digitales.
- Herramientas de análisis de redes capaces de identificar y rastrear actividades delincuenciales en la red.

- La monitorización de redes sociales es una herramienta muy útil de cara a la investigación de delitos cometidos en las mismas, permitiendo obtener cuantiosa información útil en las investigaciones policiales.
- La investigación en fuentes abiertas «OSINT» se trata de una técnica de búsqueda enfocada a la recopilación de información publicada en fuentes públicas y accesibles. Estas fuentes pueden ir desde sitios web, redes sociales abiertas, bases de datos públicas, información de metadatos, entre otras.

Además de todas estas herramientas digitales y modernas, las Fuerzas y Cuerpos de Seguridad «FCS» que trabajan en España, disponen de otras más tradicionales como pueden ser los oficios policiales, los oficios judiciales, los convenios de colaboración europea mencionados anteriormente o las Comisiones Rogatorias Internacionales.

Una herramienta muy útil para los cuerpos policiales y juzgados no es otra que los oficios. Bien sean oficios policiales u oficios judiciales respectivamente.

De acuerdo con la Real Academia Española «RAE», una de las definiciones de oficio hace referencia a toda comunicación dirigida por las autoridades policiales al órgano judicial interesando su autorización para la práctica de determinadas diligencias de investigación que exijan la misma.

La Ley de Enjuiciamiento Criminal Española «LECRIM», en su artículo 588 ter e, establece el Deber de Colaboración de las empresas prestadoras de servicios que operen en España de la siguiente manera:

“1. Todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, están obligados a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones.

2. Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades.

3. Los sujetos obligados que incumplieren los anteriores deberes podrán incurrir en delito de desobediencia".

Este articulado habilita a los jueces, Ministerio Fiscal y agentes de Policía Judicial a solicitar información relacionada con usuarios, compras o interacciones producidas en el seno de las empresas prestadoras de servicios en territorio nacional. De manera que, si se precisan los datos asociados a una cuenta de usuario de una plataforma web o red social, una dirección de correo electrónico o el historial de pedidos de una empresa de compras online. Mediante un mandamiento policial o judicial enmarcado dentro de una investigación penal se solicitará dicha información con el objetivo de esclarecer un hecho delictivo o proseguir con la investigación.

Gracias a los Acuerdos de Colaboración Europeos, estos oficios también se pueden enviar a empresas prestadoras de servicios que se encuentren en un país miembro de la Unión Europea. Como suele suceder habitualmente con Irlanda, sede de las grandes tecnológicas internacionales en suelo europeo.

No obstante, si se precisan obtener datos en poder de empresas afincadas en otros países fuera de la Unión Europea, sería necesario recurrir a las Comisiones Rogatorias Internacionales «CRI». Una comisión rogatoria se basa en la notificación y solicitud de práctica de pruebas en el extranjero, aludiendo a la colaboración internacional existente entre países a nivel judicial debido a la limitación territorial de los juzgados en el ámbito competencial y su incapacidad de realizar pruebas fuera de su territorio.

Por comisión rogatoria se entiende el instrumento por el cual la autoridad judicial de un Estado «Estado requirente» solicita de la autoridad competente de otro Estado «Estado requerido» la ejecución, dentro del territorio de su jurisdicción, de un acto de instrucción o de otros actos judiciales, especialmente la práctica de una diligencia probatoria. (ARCHONTAKI 2016, p.100).

Este tipo de solicitudes internacionales se realizan en casos relacionados con narcotráfico, corrupción, lavado de dinero, terrorismo y otros delitos graves o de gran repercusión social.

La solicitud de una comisión rogatoria internacional puede incluir aspectos como la recolección de pruebas, obtención de declaraciones de testigos o realización de investigaciones.

2.4.2. Agente Encubierto Informático

Las investigaciones encubiertas en el ciberespacio merecen un capítulo aparte dentro de las medidas de las que disponen los cuerpos policiales, es por ello que se le dedica el presente apartado. Al precisar de una gran preparación previa y poner en riesgo algunos derechos fundamentales de las personas investigadas.

Tanto en el caso del agente encubierto tradicional, como en el informático, estas investigaciones se requieren en operaciones contra el narcotráfico, el terrorismo y otros delitos que por su singularidad o dificultad para ser investigados con métodos tradicionales necesitan de esta medida.

Los especialistas en inteligencia definen la infiltración policial como una técnica de investigación aplicable a la delincuencia organizada en que el instrumento que se utiliza es un funcionario de Policía, el agente encubierto, que se introduce en una organización criminal, cambiando de identidad, llevando a cabo tareas principalmente de represión y de prevención del delito, con el fin de ganarse la confianza del grupo, identificar a sus integrantes, obtener información en cuanto a su funcionamiento, financiación, etc., recaudar pruebas y, excepcionalmente, presentar testimonio de cargo ante la justicia (RIQUELME 2016, p.8).

En la Sentencia del Tribunal Supremo 1140/2010, 29 de diciembre se señala que:

"El término *under cover* o agente encubierto, se utiliza para designar a los funcionarios de policía que actúan en la clandestinidad, con identidad supuesta y con la finalidad de reprimir o prevenir el delito.

Agente encubierto, en nuestro ordenamiento será el policía judicial, especialmente seleccionado, que bajo identidad supuesta, actúa pasivamente con sujeción a la Ley y bajo el control del Juez, para investigar delitos propios de la delincuencia organizada y de difícil averiguación, cuando han fracasado otros métodos de la investigación o estos sean manifiestamente insuficientes, para su descubrimiento y permite recabar información sobre su estructura y modus operandi, así como obtener pruebas sobre la ejecución de hechos delictivos".

A- Regulación:

Este tipo de actuaciones policiales viene regulado en el artículo 282 bis de la LECRIM de la siguiente forma:

"A los fines previstos en el artículo anterior y cuando se trate de investigaciones que afecten a actividades propias de la delincuencia organizada, el juez de Instrucción competente o el Ministerio Fiscal dando cuenta inmediata al juez, podrán autorizar a funcionarios de la Policía Judicial, mediante resolución fundada y teniendo en cuenta su necesidad a los fines de la investigación, a actuar bajo identidad supuesta y a adquirir y transportar los objetos, efectos e instrumentos del delito y diferir la incautación de los mismos. La identidad supuesta será otorgada por el Ministerio del Interior por el plazo de seis meses prorrogables por períodos de igual duración, quedando legítimamente habilitados para actuar en todo lo relacionado con la investigación concreta y a participar en el tráfico jurídico y social bajo tal identidad.

(…)

Ningún funcionario de la Policía Judicial podrá ser obligado a actuar como agente encubierto.

Cuando las actuaciones de investigación puedan afectar a los derechos fundamentales, el agente encubierto deberá solicitar del órgano judicial competente las autorizaciones que, al respecto, establezca la Constitución y la Ley, así como cumplir las demás previsiones legales aplicables."

B- Responsabilidad:

El agente encubierto estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de la misma y no constituyan una provocación al delito.

A diferencia del agente encubierto tradicional el agente encubierto informático dispone de un mayor número de supuestos en los que poder actuar. Al poder ejercer sobre los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

Esta habilitación se convierte una herramienta muy útil para investigar todos aquellos delitos que puedan ser cometidos a través de medios informáticos o redes sociales como pueden ser

los ataques de malwares, estafas informáticas, espionajes informáticos, suplantación de identidad digital, los ciberacosos y delitos similares.

Esta modificación fue introducida en la reforma de la Ley de Enjuiciamiento Criminal operada por la LO 13/2015 de 5 de octubre en el apartado 6 del artículo 282 bis relativa a las medidas de investigación tecnológica. Con el objetivo de adaptar a los nuevos tiempos las investigaciones policiales.

Pese a la exención de responsabilidad penal por parte del agente encubierto en la realización de sus funciones de investigación, el juez competente que sea conocedor de la causa requerirá un informe de actuación al agente de la policía judicial al que haya autorizado la medida judicial de agente encubierto, tras conocer el informe el juez resolverá si existe algún tipo de responsabilidad criminal durante la investigación.

C- Expedición de nueva identidad:

En las investigaciones que requieran de la utilización de un agente encubierto informático, se solicitará al Ministerio del Interior la autorización y creación de una identidad supuesta por un plazo de 6 meses para uno de los miembros de la Policía Judicial del cuerpo policial al que pertenezca el investigador. Durante este tiempo se pretende lograr la infiltración y obtención de información de los delitos investigados gracias a la utilización de un Documento Nacional de Identidad temporal creado ex proceso para la ocasión.

Esta identidad de Agente Encubierto Informático «AEI» será asumida de manera voluntaria por uno de los agentes de la unidad de Policía Judicial del cuerpo policial encargado de la investigación.

D- Provocación o incitación al delito:

Cabe destacar que el AEI no está habilitado para provocar o incitar a otros sujetos a cometer delitos en la red, debiendo respetar en todo momento el ordenamiento jurídico.

No obstante, la provocación al delito está incorporada por el artículo 282 bis de la LECrim en su apartado 5º que «el agente encubierto estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación,

siempre que guarden la debida proporcionalidad con la finalidad de esta y no constituyan una provocación al delito». Este concepto se ha ido adaptando y modificando en base a la diferente jurisprudencia.

E- Requisitos necesarios:

Antes de la autorización de este tipo de medidas debe asegurarse si la medida judicial cumple el juicio de proporcionalidad, verificando las tres siguientes condiciones marcadas por el Tribunal Constitucional en su sentencia STC 186/200039:

> "1.- Si la medida acordada puede conseguir el objetivo propuesto (juicio de idoneidad).
>
> 2.- Si es necesaria en el sentido de que no exista otro medio más moderado para conseguir el fin propuesto con igual eficacia (juicio de necesidad); y
>
> 3.- Si la medida es equilibrada, es decir, que el beneficio que vaya a obtenerse debe ser superior al perjuicio causado por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto".

F- Modalidades de actuación

Con el objetivo de no vulnerar ningún derecho fundamental, el agente encubierto informático debe actuar bajo el amparo de una autorización judicial.

Una vez emitida la autorización judicial, el agente recibirá una identidad falsa con la que podrá acceder a foros, páginas webs y diferentes círculos de comunicación en la red. Con el objetivo de establecer contacto con los sujetos a investigar, tratando de ganarse su confianza. Pudiendo enviar documentos, imágenes o archivos de carácter ilícito con la finalidad de pasar desapercibido en dichos entornos. Este material enviado será supervisado y facilitado por el Ministerio del Interior, con el objetivo de llevar un control del mismo.

Con el objetivo de evitar la difusión por la red de este tipo de material, este será modificado o camuflado de manera que aparente ser material ilícito, pero en realidad se trata de contenido plenamente lícito y sin dañar a ningún sujeto pasivo.

El agente encubierto informático está habilitado para realizar las siguientes operaciones:

a) Envío de archivos ilícitos, siempre y cuando rija el principio de proporcionalidad y legitimidad constitucional. Respetando el principio de provocación al delito.
b) Grabación de imagen y sonido de las conversaciones mantenidas con el sujeto de la investigación policial.
c) Analizar los archivos mediante algoritmos matemáticos con el objetivo de averiguar su procedencia, así como su rastro de información.

El AEI actuará de manera diferente en función del entorno en el que se esté infiltrando, algunos de los medios en los que se puede introducir son los siguientes:

- **CANALES DE COMUNICACIÓN CERRADOS**

La Ley Orgánica 13/2015 del 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, recoge que únicamente es necesaria autorización judicial en las investigaciones en canales de comunicación cerrados. Definiendo como canal de comunicación cerrado todo aquél que requiera de una identificación previa para acceder. Siendo necesaria una autorización especial y separada con relación al intercambio de documentación de archivos ilícitos.

No obstante, los agentes podrán iniciar un contacto inicial a fin de recabar indicios y elementos suficientes que sustenten la necesidad de solicitar una posterior autorización judicial.

- **CIBERPATRULLAJE**

Debido a que numerosas plataformas en la red requieren de un "*nickname*" o alias para interactuar con el resto de usuarios y a su vez estos rara vez suelen corresponder con la identidad real del usuario de dicho canal de comunicación. En estos canales abiertos no es preceptiva una autorización judicial para ejecutar un ciberpatrullaje preventivo de delitos en la red.

- **ANÁLISIS DE ALGORITMOS ASOCIADOS A ARCHIVOS ILÍCITOS**

El artículo 282 bis 6 de la Ley de Enjuiciamiento Criminal ahonda en la posibilidad de analizar los ficheros obtenidos mediante algoritmos de análisis. Este apartado es de gran importancia dado que permite el examen de archivos y su identificación posterior.

Los algoritmos matemáticos a los que hace referencia el mencionado artículo de la LECrim son llamados *HASH.*

De acuerdo con la definición proporcionada por el sitio web CRIPTOTARIO, "una función *hash* es una función matemática que transforma una entrada de cualquier tamaño en una salida encriptada de un tamaño fijo.

Sin importar la cantidad de información que tenga lo que ingresamos en la función hash, puede ser una cadena de palabras o un archivo, siempre nos devolverá un hash del mismo tamaño."

Dicha identificación alfanumérica que proporciona el hash, permite a las unidades de policía judicial identificar imágenes, mantener un seguimiento de la modificación y recorrido de las mismas.

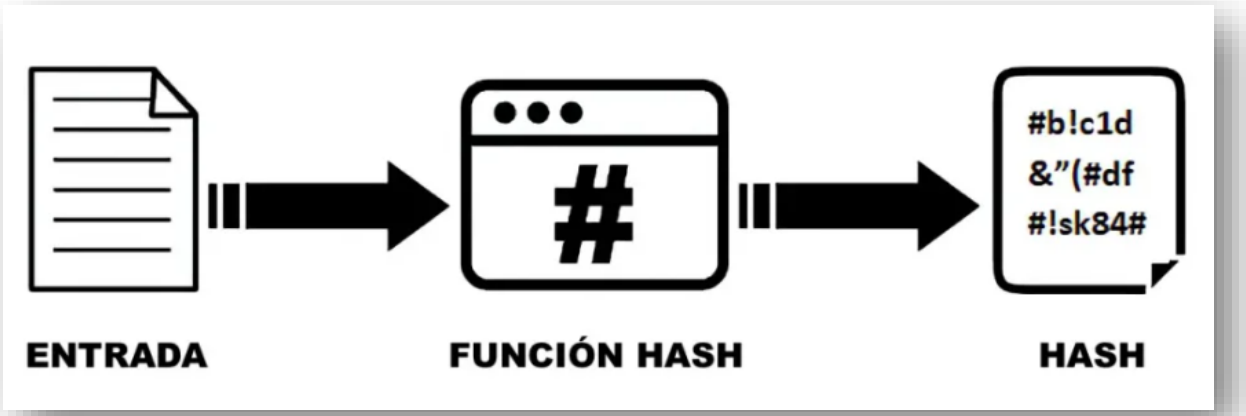


Figura 11. Esquema función hash «CRIPTOTARIO».

G- Justificación

Una vez expuesta toda la información relativa al AEI en la legislación española, cabe destacar que España es el uno de los países que más ciberataques sufren en la red. Gracias a las herramientas de análisis del INCIBE, se puede obtener una fotografía en tiempo real de este tipo de amenazas. En la mayoría de las ocasiones estas solo pueden combatirse con la figura del AEI, destacando por ello su gran importancia en la lucha contra el cibercrimen.

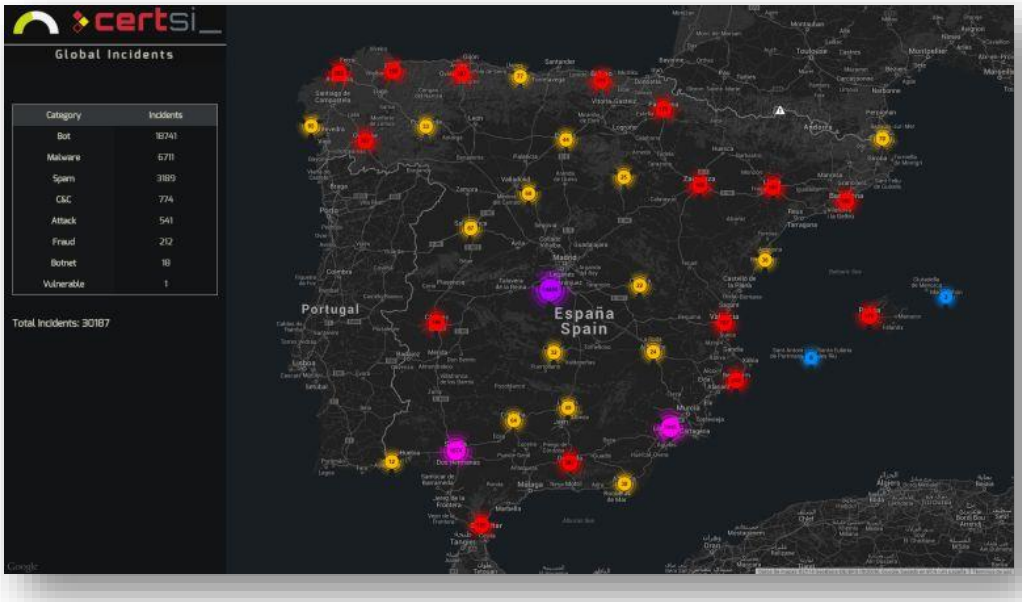


Figura 12. Ciberataques en España «INCIBE».

2.4.3. Rastro del dinero en la red

Una vez analizados los diferentes ciberdelitos relacionados con la suplantación o usurpación de identidad y las medidas de investigación llevadas a cabo por policías, fiscales y jueces. Llega el momento de hablar de la relación entre estos delitos y su monetización generalmente a través de las criptomonedas.

Las criptomonedas proporcionan un medio de intercambio digital que puede ser utilizado para cometer todo tipo ciberdelitos, como el ransomware «secuestro de datos», la extorsión en la red, el fraude informático o la suplantación de identidad. Al mismo tiempo, la tecnología *blockchain* que subyace en las criptomonedas también puede ser utilizada para rastrear y prevenir estos ciberdelitos.

Las criptomonedas también son utilizadas en esquemas de fraude en línea, como la estafa de inversión en criptomonedas, donde los delincuentes prometen altos rendimientos a cambio de inversiones en criptomonedas falsas o inexistentes. Llegando a suplantar la identidad de operadores acreditados de criptodivisas para generar una apariencia creíble en la víctima.

Gracias a la naturaleza inmutable y transparente de la tecnología *blockchain* puede ser utilizada para rastrear las transacciones de criptomonedas y descubrir a los delincuentes detrás de los ciberdelitos.

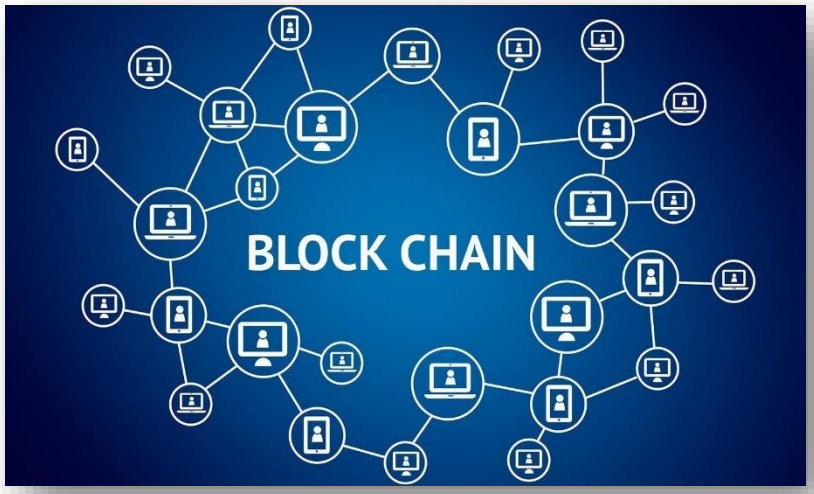


Figura 13. Esquema tecnología Blockchain «LENOVO».

De acuerdo con el autor CANTILLO (2023, p.1), un *Blockchain* es, textualmente, una cadena de bloques o cadena articulada. En realidad, es una base de datos formada en estas cadenas de bloques que están diseñadas para evitar que se puedan modificar una vez publicadas, lo que garantiza su seguridad y fiabilidad. Dichos bloques contienen una información codificada de las transacciones en la red al estar entrelazados entre si los bloques de datos.

Aunque las criptomonedas proporcionan un medio conveniente para cometer ciberdelitos, la tecnología *blockchain* subyacente también puede ser utilizada para prevenir y rastrear dichos delitos. Es importante tener en cuenta que las criptomonedas no son inherentemente maliciosas, sino que su uso puede ser desviado por delincuentes para fines ilegales.

Con el objetivo de rastrear las criptodivisas surgen varias empresas encargadas de esta tarea, las cuales son muy útiles de cara a las investigaciones policiales relacionadas con criptodivisas.

Una de estas es *Chainalysis*, siendo una empresa de análisis de datos de *blockchain* y criptomonedas que proporciona soluciones para gobiernos, empresas y organizaciones encargadas de hacer cumplir la ley en todo el mundo. La empresa fue fundada en 2014 y tiene su sede en Nueva York.

Figura 14. Logo de Chainalysis «Chainalysis».

Chainalysis utiliza herramientas de análisis de datos y algoritmos de inteligencia artificial para rastrear y analizar las transacciones en la cadena de bloques de las criptomonedas. Estas herramientas permiten visualizar el flujo de transacciones de criptomonedas en tiempo real y detectar patrones sospechosos, como transacciones que implican actividades ilegales, lavado de dinero, financiamiento del terrorismo, fraude y otros delitos financieros.

Por todo ello, esta herramienta es muy beneficiosa para las FCS que operan en España y permite esclarecer delitos que sin dicha herramienta sería muy complicado o imposible.

2.4.4. Responsabilidad civil subsidiaria de los bancos

La responsabilidad civil subsidiaria de los bancos se refiere a su obligación de hacerse cargo de los daños y perjuicios que terceros puedan sufrir como resultado de actividades financieras fraudulentas, generalmente estafas informáticas, realizadas por clientes a través de sus servicios. En otras palabras, los bancos tienen la responsabilidad de tomar medidas adecuadas para prevenir y evitar el fraude financiero y otras actividades ilegales en el uso de sus servicios bancarios.

Este tipo de regulación de la mencionada responsabilidad civil viene referida en el artículo 120.3 del Código Penal español, el cual establece lo siguiente:

«Las personas naturales o jurídicas, en los casos de delitos cometidos en los establecimientos de los que sean titulares, cuando por parte de los que los dirijan o administren, o de sus dependientes o empleados, se hayan infringido los reglamentos de policía o las disposiciones de la autoridad que estén relacionados con el hecho punible cometido, de modo que éste no se hubiera producido sin dicha infracción».

Existen diversas sentencias judiciales que avalan este articulado del CP.

La Sentencia del Tribunal Supremo, número 963/2010 de 21 de octubre de la Sala de lo Social dictaminó que "Ante la inexistencia o insuficiencia de las medidas de prevención adoptadas entre ellas, básicamente el despliegue de los deberes de vigilancia y de control exigibles, podrán acordarse las resoluciones oportunas para llegar a la efectivación de la responsabilidad civil subsidiaria. Aquella inhibición o descuido genera un riesgo que es base y sustento de la responsabilidad."

Según se recoge en la Sentencia del Tribunal Supremo 413/2015, de 30 de junio, "Los requisitos legales que son necesarios para el nacimiento de dicha responsabilidad civil, son los siguientes:

a) Que se haya cometido un delito o falta;
b) Que tal delito o falta haya ocurrido en un determinado lugar, un establecimiento dirigido por persona o empresa contra la cual se va a declarar esta responsabilidad, esto es, el sujeto pasivo de dicha pretensión;
c) Que tal persona o empresa o alguno de sus dependientes, haya realizado alguna "infracción de los reglamentos de policía o alguna disposición de la autoridad";
d) Que dicha infracción sea imputable no solamente a quienes dirijan o administren el establecimiento, sino a sus dependientes o empleados."

«SSTS. 413/2015 de 30.06, 10829/2014».

Este tipo de responsabilidad civil viene producido al poner a disposición de los clientes determinadas operaciones virtuales, lo que produce una exposición de sus activos financieros a determinados ciberdelitos.

Es importante destacar que esta responsabilidad subsidiaria no implica que el banco sea directamente responsable del delito financiero en sí, sino que se le responsabiliza por no haber tomado medidas adecuadas para prevenir o detectar el delito financiero en cuestión.

2.5. Análisis de un caso real

2.5.1. Explicación del caso

Una vez estudiados todos los elementos que rodean los casos de suplantación de identidad en la red, se procede en el presente capítulo a una breve aplicación práctica de dichos conocimientos a través del análisis de un caso real.

En este caso la víctima ha sufrido el robo de su teléfono móvil durante la estancia de sus vacaciones en Colombia. Motivo que el sujeto activo del delito aprovecha para cometer todas las actividades delincuenciales durante el periodo de tiempo que la víctima está incomunicada en un país extranjero y sin percatarse de dichas actividades.

Una vez el delincuente tiene en su haber el terminal móvil, solicita una portabilidad de la tarjeta SIM a otra compañía telefónica. De esta manera logra tener acceso a los SMS de verificación bancarios enviados a la víctima.

A día de hoy los teléfonos móviles o *Smart Phones* están vinculados a diversas plataformas de servicios online como redes sociales, empresas de comercio online, sistemas de almacenamiento de información masiva en la nube y un largo etcétera de aplicaciones.

Teniendo en su poder el teléfono de la víctima, con pleno acceso a su contenido y una vez efectuada la portabilidad de compañía telefónica. El sujeto activo del delito comenzó a realizar varios cargos fraudulentos a costa de las cuentas bancarias de la víctima.

Varios cargos fraudulentos que suman en total *3197,15€* desglosados de la siguiente manera:

- Gastos en Bizum con concepto "Fiesta de anoche y Cena" 454,95€.
- Gastos en Amazon 1242,2€.
- Gastos en Transferencia Bancaria 1500€.
- Solicitud de un préstamo de 4520€ con el número 2004623025, aparejado un cargo de 20€ de seguro de vida. Día 13 agosto, formalizado el 16 agosto.

- Amortización del préstamo anterior de 3500€, haciéndose efectivo el 16 de agosto. Penalización de 17,50€.

En este caso las entidades bancarias de las cuales es cliente la víctima no se hacen cargo del importe estafado, ya que todas las operaciones fueron confirmadas mediante códigos de seguridad remitidos al teléfono móvil del denunciante. Por lo que las medidas de seguridad implantadas por la entidad bancaria han funcionado correctamente y desde el punto de vista de la entidad bancaria, no se cumplen los requisitos de la responsabilidad civil subsidiaria necesaria para que tengan que asumir los costos producidos por la suplantación de identidad producida en este caso.

2.5.2. Aporte de las denuncias reales

Gracias a la cesión de las denuncias por parte de un colaborador en el presente Trabajo de Fin de Máster, se ha logrado incorporar los Anexos A y B. Donde se pueden leer detenidamente dos denuncias interpuestas por la víctima en relación a varias ciberestafas y una suplantación de identidad respectivamente. Plasmando de una manera real varios de los aspectos tratados a lo largo del presente documento.

Una de las denuncias ha sido interpuesta ante la Policía Nacional y la otra ante la Guardia Civil.

Figura 15. Emblema de Policía Nacional y Guardia Civil «CNP y GC».

2.5.3. Líneas de investigación

A continuación, se mencionarán algunas de las líneas de investigación que se podrían realizar en relación con el caso real que se está tratando. Cabe destacar que se deberá tener en cuenta cada evidencia recibida y reevaluar la línea de investigación con cada una de ellas. Adaptando la investigación conforme se reciban los resultados de las pruebas solicitadas.

- Emitir un mandamiento judicial oficiado a la compañía telefónica que ha recibido la portabilidad de la SIM del denunciante. Solicitando todos los datos disponibles por la operadora:
    - Información del titular de la línea, nombres, apellidos, documentación aportada durante la portabilidad.
    - Fecha y hora de la de portabilidad.
    - Información del canal utilizado para la solicitud de la portabilidad.
    - En caso de tratarse de una SIM física, identificar la tienda física en la que ha sido adquirida o la dirección de envío postal. En caso de envió postal informen agencia de trasportes y numero de seguimiento.
    - Información de la tarjeta/cuenta bancaria relacionada con el pago de la portabilidad y/o facturación de la línea de telefónica.
    - Otros datos que puedan ayudar a la investigación policial por el fraude denunciado.

- Emitir un mandato judicial oficiando a la entidad bancaria en relación a la cuenta bancaria destino de las trasferencias por importe total de 1.500 euros. Solicitando todos los datos disponibles por la entidad bancaria:
    - Identidad completa del titular o personas autorizadas en la misma, comprendiendo los mismos números de teléfono aportados o direcciones de correo electrónico.
    - Oficina, fecha y lugar de apertura de la mencionada cuenta bancaria, así como copia de los documentos de identidad aportados para abrir la misma o grabaciones de las cámaras de seguridad de la oficina. Reseñando si la cuenta bancaria ha sido abierta de manera presencial o telemática.

- Faciliten numeración completa de las tarjetas asociadas a la cuenta bancaria, si se trata de una tarjeta virtual o física, reseñando el titular de cada una de ellas. Indicar la fecha de entrega, si se han entregado a su titular de manera presencial o mediante envió postal, reseñando hora, fecha y lugar y/o dirección postal.
- Relación de movimientos «ingresos, reintegros, trasferencias recibidas y enviadas» así como números de cuenta de los que proviene o a los que se dirige desde enero de 2022 hasta la actualidad.
- Ultimas diez «10» direcciones IP que posean al respecto a las operaciones online, realizadas mediante banca electrónica, en relación a la citada cuenta bancaria, con clara expresión de su fecha y hora, reflejando así mismo el tipo de uso horario por el que se rigen.
- Se proceda de manera provisional al bloqueo de la cantidad de 1.500 euros de la cuenta bancaria antes reseñada, destino de las trasferencias denunciada en las presentes por importe de 1.500 euros, evitando la fuga de capital a manos no deseadas, asegurando de esta forma pueda ser posteriormente devuelto al perjudicado si Su Señoría así lo ordenase.
- Estado actual de la cuenta «bloqueada, cancelada, …» y motivo del mismo. Saldo actual de la cuenta.
- Otros datos que puedan ayudar a la investigación policial por el fraude denunciado.

- Emitir un mandato judicial oficiando a la compañía de pagos Bizum en relación con los movimientos cuyo concepto fue "Fiesta de anoche y Cena" por un importe de 454,95€. Solicitando todos los datos disponibles a la plataforma:
  - Información del titular de la línea telefónica receptora del pago, nombres, apellidos, número de teléfono, cuenta bancaria y documentación aportada.
  - Información del histórico de movimientos recibidos por parte del número de teléfono receptor del movimiento no autorizado.
  - Información del histórico de datos bancarios asociados al del número de teléfono receptor del movimiento no autorizado.

  - Otros datos que puedan ayudar a la investigación policial por el fraude denunciado.

- Emitir un mandato judicial oficiando a la empresa de comercio electrónico Amazon en relación con las compras realizadas a través de la cuenta de la persona denunciante. Solicitando todos los datos disponibles a la empresa de comercio electrónico:
  - Información del titular receptor del producto adquirido sin autorización, nombres, apellidos, número de teléfono, cuenta bancaria y documentación aportada.
  - En caso de disponer de información de algún cliente de la compañía que pudiera coincidir con los datos del remitente arriba mencionado. Se solicita toda la información disponible; nombre, apellidos, documento de identidad, histórico de las direcciones de entrega, histórico de números de tarjetas bancarias asociadas, histórico de pedidos adquiridos en la plataforma.
  - Ultimas diez «10» direcciones IP que posean al respecto a las operaciones online, realizadas mediante su plataforma de comercio electrónico, en relación a la citada cuenta de usuario, con clara expresión de su fecha y hora, reflejando así mismo el tipo de uso horario por el que se rigen.
  - Otros datos que puedan ayudar a la investigación policial por el fraude denunciado.

- Emitir un mandato judicial oficiando a la empresa aseguradora prestadora del seguro contratado fraudulentamente por los ciberdelincuentes. Solicitando todos los datos disponibles por la empresa aseguradora:
  - Identidad completa del titular o titulares asociados a la póliza de seguros mencionada, comprendiendo los mismos números de teléfono aportados o direcciones de correo electrónico.
  - Información referente al tipo de póliza de seguros contratada y las coberturas que contratadas.

- Oficina, fecha y lugar de apertura de la contratación de la póliza, así como copia de los documentos de identidad aportados para abrir la misma o grabaciones de las cámaras de seguridad de la oficina. Reseñando si la póliza ha sido contratada de manera presencial o telemática.
- Otros datos que puedan ayudar a la investigación policial por el fraude denunciado.

3. Conclusiones

1. Se observa un crecimiento exponencial de los delitos informáticos en España, siendo estos un reflejo de lo que sucede en el resto del mundo. Derivado del crecimiento en el uso de las TICs por parte de la población y el traslado de parte de su interacción social del mundo físico al mundo virtual.

2. Existe una falta de acuerdos internacionales que permitan perseguir de una manera real este tipo de actividades delictivas. Al margen de la Unión Europea y del Convenio de Budapest, no existen grandes herramientas que permitan a los jueces nacionales perseguir estos delitos en países que no son propensos a la colaboración internacional. Siendo estos de facto un refugio de ciberdelincuentes.

3. El órgano legislativo de cualquier país siempre se encontrará la zaga de los ciberdelincuentes en lo relativo a la regulación de estas actividades. Debido a su gran versatilidad de comisión y la rigidez de los países en adaptar estas conductas a su ordenamiento jurídico.

4. El breve pero complejo listado de ciberdelitos relacionados con la suplantación de información en la red no hace más que poner de manifiesto la gran inventiva de los delincuentes para obtener datos personales de las víctimas y acabar monetizando dichas acciones.

5. Una gran parte de la población no es consciente de los expuesta que está a los ciberdelincuentes en el mundo virtual a los ciberdelincuentes. Claro ejemplo de ello es la falta de concienciación de estos peligros, llegando a alegar que si no eres una persona famosa o rica no serás víctima de estos delitos. Una vez más la concienciación es una herramienta básica para combatir estas actividades delincuenciales.

6. La creación de una identidad digital general aportaría más seguridad a las interacciones de los ciudadanos con las empresas y gobiernos. Siendo este aspecto un tema muy

delicado y complejo a tratar, pero necesario de abordar si se quiere combatir la suplantación de identidad en la red.

7. Los juzgados y agentes de policía están sobrepasados por la gran cantidad de casos relacionados con estos delitos, por lo que sería necesario no solamente reforzar con más personal en sus respectivos puestos de trabajo. Sino también darles una formación técnica de calidad que les permita realizar su trabajo con mayor eficiencia.

8. Dada la gran cantidad de ciberdelitos que acaban relacionados con las criptomonedas, sería aconsejable establecer una mayor regulación de su actividad en los países sobre las que operan.

Referencias bibliográficas

Bibliografía básica

- ARCHONTAKI, C*. El tratado de Lisboa y la armonización del derecho penal material: realidad y propuestas*. Programa de Doctorado en Derecho. Universidad de Alcalá, Alcalá de Henares 2016.
- Banco Santander. «Fraude del CEO: una de las estafas más peligrosas que afecta a empresas de todo el mundo». *Banco Santander*, 9 de enero de 2021. Disponible en: https://www.bancosantander.es/blog/ciberseguridad/fraude-del-ceo
- BELCIC, I. «¿Qué es el phishing?». *Avast*, 5 febrero 2020, Disponible en: https://www.avast.com/es-es/c-phishing#topic-1
- CALLEGARI, O. «Delitos informáticos: Pharming» .*Net Report*, 31 de mayo de 2007. Disponible en: http://www.rnds.com.ar/notas_detalle.asp?id_categ=37&rowsperpage=10&ittlnumitems=25&idbloc=20
- CANTILLO, F. «¿Qué es un "Blockchain"?». *Blog Lenovo*, 15 de abril de 2023. Disponible en: https://www.bloglenovo.es/que-es-un-blockchain/
- CRIPTOTARIO. «¿QUÉ ES UNA FUNCIÓN HASH?». Disponible en: https://criptotario.com/funcion-hash
- DIAZ, A. *El bien jurídico tutelado de la información y los nuevos verbos rectores en los delitos informáticos*. Universidad Santiago de Cali, Facultad de Derecho, Cali 2019.
- INCIBE. «Guía de ciberseguridad: La ciberseguridad al alcance de todos». *INCIBE*, 11 de julio de 2022. Disponible en: https://www.incibe.es/sites/default/files/docs/senior/guia_ciberseguridad_para_todos.pdf
- KARPESKY. «¿Qué es un ataque de día cero?: definición y explicación». *Karpesky*, 14 de abril de 2023. Disponible en: https://latam.kaspersky.com/resource-center/definitions/zero-day-exploit
- RIQUELME, E. *El agente encubierto en la ley de drogas. La lucha contra la droga en la sociedad del riesgo*. Derecho penal, Universidad Pompeu Fabra. Barcelona, 2016.
- SEPULVEDA, J.C. *Análisis de la efectividad de los modelos de autenticación 2FA y MFA de acuerdo a los algoritmos y protocolos aplicados en la seguridad de cuentas de*

servicios y plataformas online en Colombia. Universidad Nacional Abierta y a Distancia (UNAD), Escuela de ciencias básicas, tecnología e ingeniería. Medellín 2022.

- TORRES, I. *Estudio comparativo de tecnologías de la seguridad informática phishing y spoofing para la detección de un ataque informático*. Universidad Técnica de Babahoyo. Facultad de administración, finanzas e informática, Babahoyo 2022.
- VENTURA, M.A. *La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en lima*. Universidad Privada del Norte. Facultad de derecho y ciencias políticas, Lima 2020.
- ZARATE, P y BECERRA M.C. *Robo de Identidad y su Incidencia en el Cibercrimen*. XXI Simposio Argentino de Informática y Derecho, virtual 2021

Legislación citada

- España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Boletín Oficial del Estado, 24 de noviembre de 1995, núm. 281, p. 33987. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444
- España. Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. Boletín Oficial del Estado, de 3 de enero de 1883, núm. 260. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036
- España. Constitución española. Boletín Oficial del Estado, 29 de diciembre de 1978, núm. 31. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229
- España. Boletín Oficial del Estado. Instrumento de Ratificación del Convenio sobre Ciberdelincuencia, hecho en Budapest, el 23 de noviembre de 2001. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221
- Ley 29/2022, de 21 de diciembre, por la que se adapta el ordenamiento nacional al Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre Eurojust, y se regulan los conflictos de jurisdicción, las redes de cooperación jurídica internacional y el personal dependiente del Ministerio de Justicia en el exterior.
- Diario Oficial de la Unión Europea. Directiva 2014/41/CE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal. Disponible en: https://www.boe.es/doue/2014/130/L00001-00036.pdf.

- Ley Orgánica 13/2015 del 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725

Jurisprudencia referenciada

- Sentencia del Tribunal Supremo, núm. 963/2010 de 21 de octubre, Sala de lo Social.
- Sentencia del Tribunal Supremo, núm. 413/2015 de 30 de junio, Sala de lo Penal, Sección 2ª.
- Sentencia del Tribunal Constitucional, núm. 186/200039 de 10 de julio, Sala Primera.
- Sentencia del Tribunal Supremo, núm. 1140/2010 de 29 de diciembre, Sala de lo Penal, Sección 1ª.

Listado de abreviaturas y siglas

2FA: Autenticación de dos pasos que combina dos factores o métodos.

AEI: Agente Encubierto Informático.

BCIT: Brigada Central de Investigación Tecnológica.

CERT: Red Europea de Equipos de Respuesta a Emergencias Informáticas.

CNP: Cuerpo Nacional de Policía.

CP: Código Penal.

CRI: Comisión Rogatoria Internacional.

DNS: Domain Name Server.

EC3: Plataforma Europea de Lucha contra la Delincuencia en Internet.

ENISA: Agencia Europea de Seguridad de las Redes y de la Información.

GC: Guardia Civil.

GDI: Grupo de Delitos Informáticos.

GDT: Grupo de delitos telemáticos.

INCIBE: Instituto Nacional de Ciberseguridad.

IP: Internet Protocol.

LECRIM: Ley de Enjuiciamiento Criminal Española.

RAE: Real Academia Española.

RRSS: Redes Sociales.

SCDTI: Sección Central de Delitos en Tecnologías de la Información.

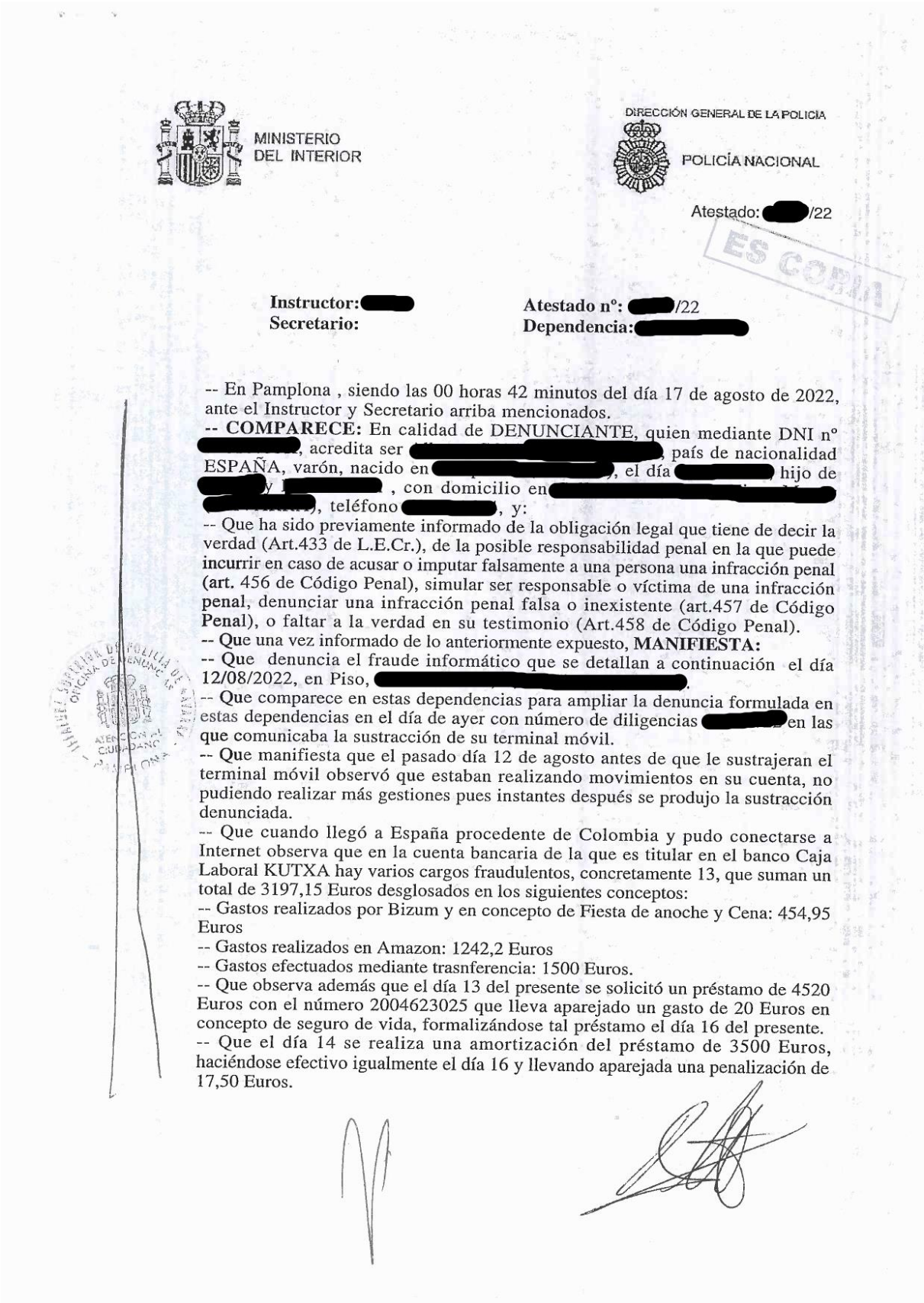
STS: Sentencia del Tribunal Supremo.

TIC: Tecnologías de la Información y la Comunicación.

UCIBER: Unidad de Ciberseguridad.

UE: Unión Europea.

Anexo A. Primera denuncia real: Ciberestafa



MINISTERIO DEL INTERIOR

DIRECCIÓN GENERAL DE LA POLICÍA

POLICÍA NACIONAL

Atestado: [redacted]/22

ES COPIA

Instructor: [redacted]
Secretario:

Atestado nº: [redacted]/22
Dependencia: [redacted]

-- En Pamplona , siendo las 00 horas 42 minutos del día 17 de agosto de 2022, ante el Instructor y Secretario arriba mencionados.
-- **COMPARECE:** En calidad de DENUNCIANTE, quien mediante DNI nº [redacted], acredita ser [redacted], país de nacionalidad ESPAÑA, varón, nacido en [redacted], el día [redacted], hijo de [redacted], con domicilio en [redacted], teléfono [redacted], y:
-- Que ha sido previamente informado de la obligación legal que tiene de decir la verdad (Art.433 de L.E.Cr.), de la posible responsabilidad penal en la que puede incurrir en caso de acusar o imputar falsamente a una persona una infracción penal (art. 456 de Código Penal), simular ser responsable o víctima de una infracción penal, denunciar una infracción penal falsa o inexistente (art.457 de Código Penal), o faltar a la verdad en su testimonio (Art.458 de Código Penal).
-- Que una vez informado de lo anteriormente expuesto, **MANIFIESTA:**
-- Que denuncia el fraude informático que se detallan a continuación el día 12/08/2022, en Piso, [redacted].
-- Que comparece en estas dependencias para ampliar la denuncia formulada en estas dependencias en el día de ayer con número de diligencias [redacted] en las que comunicaba la sustracción de su terminal móvil.
-- Que manifiesta que el pasado día 12 de agosto antes de que le sustrajeran el terminal móvil observó que estaban realizando movimientos en su cuenta, no pudiendo realizar más gestiones pues instantes después se produjo la sustracción denunciada.
-- Que cuando llegó a España procedente de Colombia y pudo conectarse a Internet observa que en la cuenta bancaria de la que es titular en el banco Caja Laboral KUTXA hay varios cargos fraudulentos, concretamente 13, que suman un total de 3197,15 Euros desglosados en los siguientes conceptos:
-- Gastos realizados por Bizum y en concepto de Fiesta de anoche y Cena: 454,95 Euros
-- Gastos realizados en Amazon: 1242,2 Euros
-- Gastos efectuados mediante trasnferencia: 1500 Euros.
-- Que observa además que el día 13 del presente se solicitó un préstamo de 4520 Euros con el número 2004623025 que lleva aparejado un gasto de 20 Euros en concepto de seguro de vida, formalizándose tal préstamo el día 16 del presente.
-- Que el día 14 se realiza una amortización del préstamo de 3500 Euros, haciéndose efectivo igualmente el día 16 y llevando aparejada una penalización de 17,50 Euros.

MINISTERIO DEL INTERIOR

DIRECCIÓN GENERAL DE LA POLICÍA

POLICÍA NACIONAL

Atestado: [redacted]

-- Que puesto que estando en Colombia le sustrajeron el terminal móvil cree que ambos sucesos pueden estar relacionados.
-- Que en este acto aporta extracto bancario expedido por la entidad observando los movimientos referidos copia del cual se adjunta a las presentes.
-- Que es informado de los derechos que le asisten como víctima de delito lo que se realiza en Acta aparte que se adjunta igualmente al presente.
-- Fraude Informático
-- Tarjeta de Crédito: [redacted]
-- Comercio de uso de Tarjeta: BIZUM AMAZON Y PRSTAMO BANCARIO.
-- Entidad Bancaria CAJA LABORAL KUTXA.
-- Número de Cuenta Bancaria: [redacted].

DATOS AUTOR:

-- Nacionalidad: ESPAÑA.

ADVERTENCIAS LEGALES:

-- Finalmente en este mismo acto, por parte de esta Instrucción también se le informa y advierte de lo siguiente:
-- Que **la copia de este documento,** sólo tiene valor de resguardo de haber formulado denuncia (art.268 LECrim.) y por lo tanto, no certifica como ciertos o verdaderos los hechos denunciados, así como tampoco acredita la identidad de la persona que la porte.
-- En cumplimiento de lo estipulado en la L.O. 15/99 de 13 de diciembre de Protección de Datos de Carácter Personal(disposición transitoria cuarta. L.O. 3/2018 de Protección de Datos Personales y garantía de los derechos digitales), se le informa que sus datos personales serán incorporados al fichero Sidenpol (regulado por la Orden INT/1202/2011 de 4 de mayo), cuyo responsable es la Dirección Adjunta Operativa, calle Rafael Calvo, 33, Madrid. Órgano mediante el cual podrá dirigirse para ejercer los derechos de acceso, rectificación y cancelación.
-- Que al amparo del Estatuto de la Víctima y del R.D. que lo desarrolla es informado que, como víctima de infracción penal, tiene derecho a recibir la asistencia que presta las Oficinas de Asistencia a las Víctimas y que consiste en información general y particular, apoyo emocional, asesoramiento y coordinación.
-- Que no tiene/n más que decir, firmando su declaración en prueba de conformidad, en unión del Instructor. CONSTE Y CERTIFICO.

Anexo B. Segunda denuncia real: Suplantación Identidad

ATESTADO Nº: [redacted]

FOLIO Nº:

Diligencia de inicio por denuncia de infracción penal mediante comparecencia

En [redacted], siendo las 18:55, del dia 18 de octubre de 2022, actuando como Instructor de las presentes diligencias el agente de la Guardia Civil con Tarjeta de Identidad Profesional (TIP) [redacted] por medio de la presente se hace constar que:

COMPARECE ante el instructor, D/Dña. [redacted] (NIF (DNI): [redacted], nacido en [redacted], España, el [redacted] hijo de [redacted] con domicilio en Calle [redacted] Num/Km: [redacted], Teléfono móvil [redacted].

La persona compareciente lo hace en calidad de Denunciante-Víctima.

La persona compareciente DENUNCIA la comisión de la siguiente infracción penal: Delito de falsificación de documentos públicos, oficiales, mercantiles y de despachos transmitidos por servicios de telecomunicaciones, ocurrida entre el 12-08-2022 00:00 y el 19-10-2022 00:00, en Calle [redacted] Num/Km: [redacted] España.

La persona compareciente DECLARA que los siguientes objetos están relacionados con los hechos delictivos indicados anteriormente:

DOCUMENTOS

- Clase de documento: Otros documentos. Tipo de documento: Otro documento. N: [redacted]

Vinculación: Relacionado.

PREGUNTADA la persona compareciente DECLARA:

Que ha sido informado de la obligación legal que tiene de decir la verdad (Art. 433 de la LECrim) y de la posible responsabilidad penal en la que puede incurrir en caso de acusar o imputar falsamente a una persona una infracción penal o con temerario desprecio hacia la verdad (Art. 456 del Código Penal), simulando ser responsable o víctima de una infracción penal (Art. 457 del Código Penal), o faltar a la verdad en su testimonio (Art. 458 del Código Penal).

De conformidad con lo establecido en la Ley Orgánica 03/2018 de 05 de diciembre de Protección de Datos de Carácter Personal y garantía de los derechos digitales, se informa al interesado que sus datos personales serán incorporados al fichero INTPOL, cuyo responsable es el Director General de la Guardia Civil y tiene por finalidad el mantenimiento de la seguridad ciudadana mediante el control de hechos y personas de interés policial. Podrá ejercer los derechos de acceso, oposición, rectificación y cancelación por escrito ante el Exmo. Sr. General Jefe de Policía Judicial (C/Guzmán el Bueno, número 1 10, 28003 Madrid).

La persona manifiesta que llegando de viaje en Colombia el día 16 de Agosto, el día 18 de Agosto observa que no tiene conexión telefónica con la compañía Finetwork con la tarjeta con código ICC [redacted] Desde dicha compañía le informan de que se hizo efectiva la portabilidad a otra compañía el día 12 de Agosto, realizándose la solicitud sobre el día 08 de Agosto a la compañía Pepe phone. Realizando llamada a Pepe phone le informan que tendría que personarse en una oficina presencialmente, verificando su DNI y realizar un duplicado de tarjeta SIM, anulando la anterior tarjeta, siendo la nueva con cada ICC [redacted].

PREGUNTADA para que diga si anteriormente le ha ocurrido algo parecido, RESPONDE que desde su usurpación de identidad ha interpuesto varias denuncias, 2 por estafa, una por cada compañía bancaria, que la verificación de transferencias se realizaría usurpando

GUARDIA CIVIL

Página 1 de 2

ATESTADO Nº: | FOLIO Nº:

su identidad, ya que la confirmación se haría mediante SMS de la compañía Pepe phone de la que no era conocedor, ni poseedor de la tarjeta SIM.

La persona denunciante ha instado a la compañía Pepe phone a que aporte todos los datos referentes a la portabilidad fraudulenta, con el fin de demostrar que no sería la persona que habría verificado las transacciones denunciadas en las dos denuncias anteriores. Aun habiendo aportado toda la documentación solicitada por la compañía en referencia a las transacciones fraudulentas, en el día de hoy aún no tendría respuesta de dicha compañía.

PREGUNTADA para que diga si conoce el posible autor del ilícito RESPONDE manifiesta que lo desconoce, que anteriormente habría aportado datos por las estafas.

PREGUNTADA para que diga si esto le habría sucedido con anterioridad, RESPONDE manifiesta que no.

PREGUNTADA si desea aportar algún dato más de interés a las presentes, RESPONDE que no.

Se dan por tanto inicio a las presentes diligencias, en atención a cuanto disponen los artículos 282 y 284 de la LECrim, con sujeción a las formalidades y principios que fija la referida norma legal.

Y para que conste, se extiende la presente que firma la persona declarante, tras haberla leído por sí, en unión de la Fuerza Instructora y demás intervinientes.

Firma Agentes actuantes

TIP [redacted]

Firma otros intervinientes

ZONA DE LA GUARDIA CIVIL * OFICINA DE ATENCIÓN AL CIUDADANO * PUESTO PRINCIPAL PAMPLONA

Firma Declarante

NIF (DNI):

GUARDIA CIVIL

Página 2 de 2