Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Suplantación de personalidad en Internet

Trabajo Fin de Máster

Máster Universitario en Gestión de la Información

Autor: Minerva Gámiz Mejias

Tutor: Juan Vicente Oltra Gutiérrez

Curso Académico: 2017 - 2018

Resumen

En este trabajo se presenta un estudio sobre la suplantación de identidad en Internet en el contexto de otros ciberdelitos. En el transcurso del mismo se muestra la legislación relacionada con los delitos y las nuevas normas que buscan proteger de una manera óptima nuestra información. También se señala el ciberacoso como consecuencia de la suplantación y la manera en que el mundo va mostrando los peligros que puede acechar ante un mal uso de nuestros datos.

En una parte más práctica se introduce un ejemplo de rastro digital, mostrando como se visualiza nuestra información en internet, y una recopilación de casos reales sobre la usurpación de identidad y otros delitos, así como guías de ayuda ante esta problemática creciente.

Palabras clave: suplantación de identidad, internet, usurpación del estado civil, ciberacoso, estudio legal, redes sociales.

Abstract

This paper presents a study on identity theft on the Internet in the context of other cybercrimes. During it is shown the legislation related to crimes and new rules that seek to optimally protect our information. It also points to cyberbullying because of the impersonation and the way in which the world is showing the dangers that can lie in the face of misuse of our data.

In a more practical part, an example of a digital trace is introduced, showing how our information is displayed on the Internet, and a compilation of real cases about identity theft and other crimes, as well as help guides to this growing problem.

Keywords: identity theft, internet, cyberbullying, legal study, social media.

Índice general

Índice de figuras

1. Objeto y objetivos

Objeto

El objeto del presente Proyecto de Fin de Carrera es la obtención del título de máster del Máster de Gestión de la Información expedido por la Universidad Politécnica de Valencia.

Objetivos

- El objetivo general del presente trabajo es realizar un estudio que ayude a comprender de mejor manera, qué es la suplantación de identidad en internet, lo que conlleva y la importancia que tiene proteger nuestros datos. Así como proporcionar una guía de prevención y actuación para no regalar nuestros datos a terceros.

Para ello se perseguirán los siguientes objetivos específicos:

- Diferenciar la suplantación de identidad de otros ciberdelitos, conociendo sus posibles motivaciones y usos para otras actividades delictivas.
- Identificar la legislación que afecta a este delito y otros posibles derivados, así como las consecuencias que pueda implicar.
- Aprender sobre los nuevos reglamentos y directivas que protegen los datos personales de los ciudadanos.
- Concienciar sobre la importancia de mantener nuestra información como algo privado y cómo controlar este hecho.

2. Estructura del documento

El presente trabajo se encuentra estructurado del siguiente modo:

- El capítulo 3 reúne la metodología utilizada al llevar a cabo este estudio.
- En el capítulo 4 se muestra una introducción a los delitos informáticos, así como varias estadísticas de los mismos.
- El capítulo 5 se centra en la suplantación de identidad como uno de los delitos informáticos existentes, diferenciando los nombres que se usan para referenciarla. También se exponen diversas metodologías utilizadas para llevarla a cabo y cuáles pueden ser sus principales motivaciones. El apartado finaliza con la legislación a la que afecta este delito presentada de manera estructurada.
- En el capítulo 6 se habla de las nuevas normas publicadas para la protección de datos, así como el método para implantar el nuevo reglamento publicado a las empresas.
- El capítulo 7 habla del ciberacoso, un delito que usualmente hace uso de la suplantación de identidad para llevarse a cabo. Se incluye también legislación a la que afecta y el uso de las netiquetas para mejorar la convivencia en Internet.
- En el capítulo 8 se presentan distintos modos en que la sociedad busca mostrar las amenazas de los ciberdelitos en un intento de paliar sus efectos.
- El capítulo 9 ofrece una muestra práctica del rastro digital que cada individuo puede estar dejando en la red sin tener consciencia.
- En el capítulo 10 se recogen diferentes casuísticas reales de delitos informáticos relacionados con este trabajo y que se han recopilado de fuentes de información veraces.
- El capítulo 11 ofrece una guía de prevención, para evitar en lo posible ser víctima de algún ciberdelito, así como una guía de actuación en caso de que ya se haya producido.
- En el capítulo 12 se presentan las distintas conclusiones obtenidas tras la realización de este estudio
- El capítulo 13 recopila la bibliografía utilizada a lo largo del trabajo de manera estructurada.

3. Metodología y herramientas

Para llevar a cabo este estudio se ha realizado un extenso uso de la base de datos Aranzadi. Con este recurso se han podido localizar las distintas legislaciones a las que se hace referencia a lo largo del trabajo. En esto se engloba tanto la legislación general contra diversos tipos de ciberdelitos, como la especifica hacia la usurpación de la identidad.

Respecto al nuevo reglamento de protección de datos, como a las directivas que lo acompañan, han sido localizadas en la web de la Agencia Española de Protección de Datos.

Para dar cabida a la distinta casuística recogida en los casos de ciberdelitos se ha recurrido a diferentes periódicos on-line y a la base de datos Aranzadi. Además, cada noticia se ha contrastado con las publicaciones de otros periódicos seleccionando aquella que aportaba una información más completa. Con el fin de aportar más variedad a los casos, se buscaron las noticias según tipologías de delitos, filtrando aquellas en que al menos se hubiese detenido a uno de los implicados.

Respecto a las herramientas utilizadas, se ha requerido un amplio uso del paquete Microsoft Office, habiéndose utilizado Microsoft Word para la maquetación de este trabajo, Microsoft Excel para los gráficos y Microsoft PowerPoint para la línea temporal de la legislación de protección de datos.

4. Introducción

El surgimiento de Internet, así como las nuevas tecnologías, supuso un gran avance para las personas. La comunicación interpersonal, la recolección de información o el impulso para nuevas investigaciones fueron solo algunas de las mejoras que permitieron una mayor rapidez tanto económica como social.

Pero este hecho también conllevó la creación de un nuevo canal para la delincuencia. Entre los factores que dieron paso a este hecho se encuentra el aumento de la dependencia de Internet, con el consecuente uso del mismo para el control de aquellos datos que antes solo estarían accesibles en papel, como la información bancaria.

Las mejoras de los sistemas y sus correspondientes actualizaciones, como la inexistencia de las mismas, abren las puertas a la creación de nuevos riesgos y vulnerabilidades, lo cual ha propiciado el aumento y proliferación de nuevas actividades delictivas (Interpol, 2017: 4).

El "cibercrimen" descrito como, "el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual (Casabona, 2006: 11)", ha aumentado de manera exponencial.

A continuación, se muestra un gráfico en el que se expone el aumento que ha sufrido la cantidad de ciberdelitos producidos en España, incrementándose hasta un 44% en cinco años.

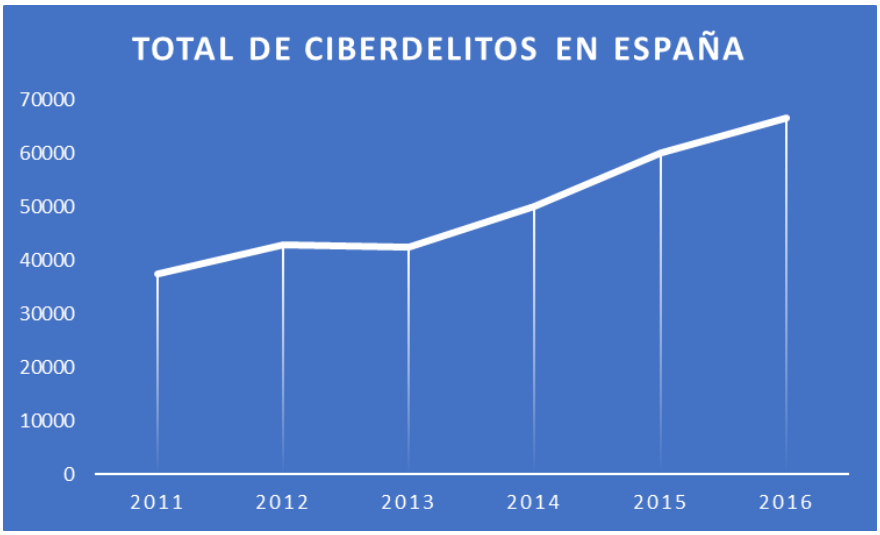

Figura 1: Total de ciberdelitos en España. Fuente: http://oedi.es/estadisticas/. Elaboración propia

El Ministerio del Interior (Ministerio del Interior, 2016: 29-44) clasifica los ciberdelitos en las siguientes temáticas: delitos contra el honor, acceso e interceptación ilícita,

falsificación informática, amenazas y coacciones, fraude informático, delitos contra la salud pública, delitos contra la propiedad industrial o intelectual, interferencia de datos y en el sistema; y delitos sexuales. A continuación, se muestran las estadísticas de dichas temáticas en referencia al número de delitos informáticos cometidos de 2011 a 2016. Cabe destacar que los gráficos aparecen diferenciados dado que el número de casos de la primera imagen son muy superiores a los de la segunda, siendo estos superados en más de 40.000 eventos.

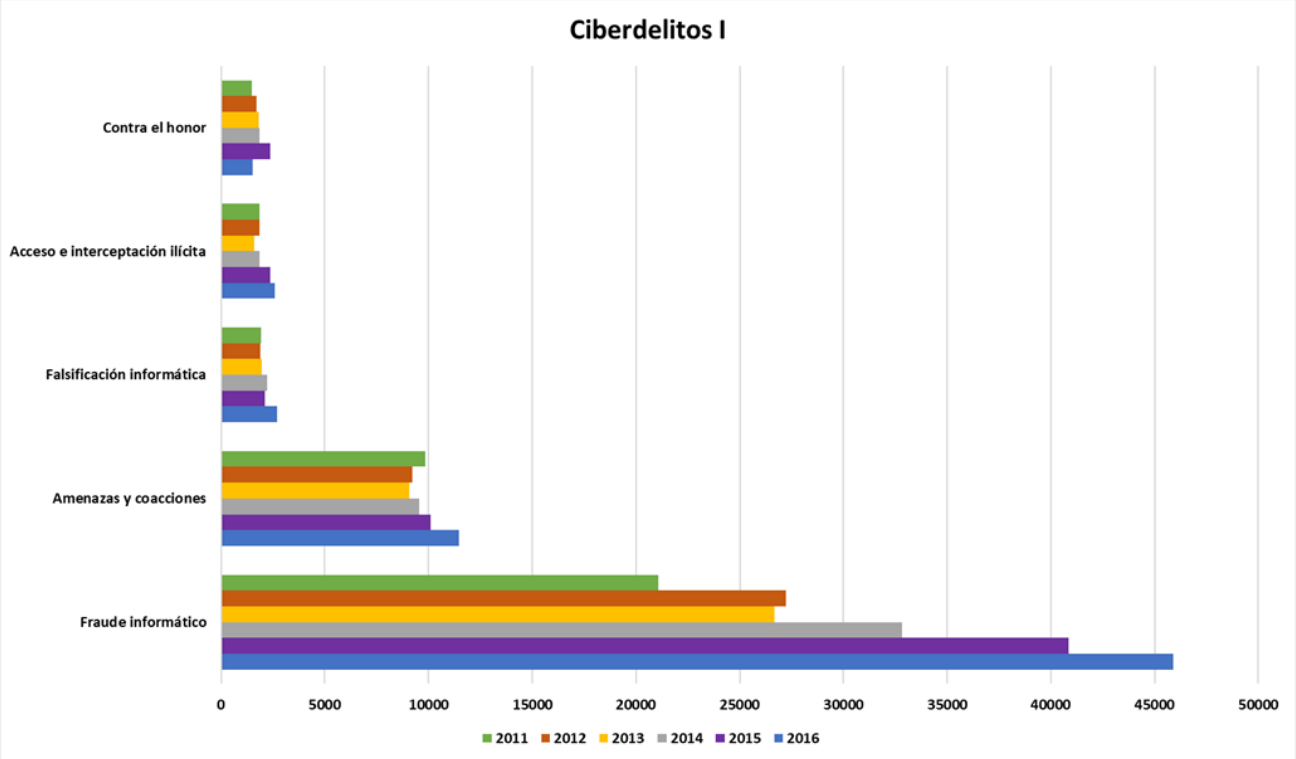

Figura 2: Ciberdelitos por tipologías (I). Fuente: http://oedi.es/estadisticas/. Elaboración propia

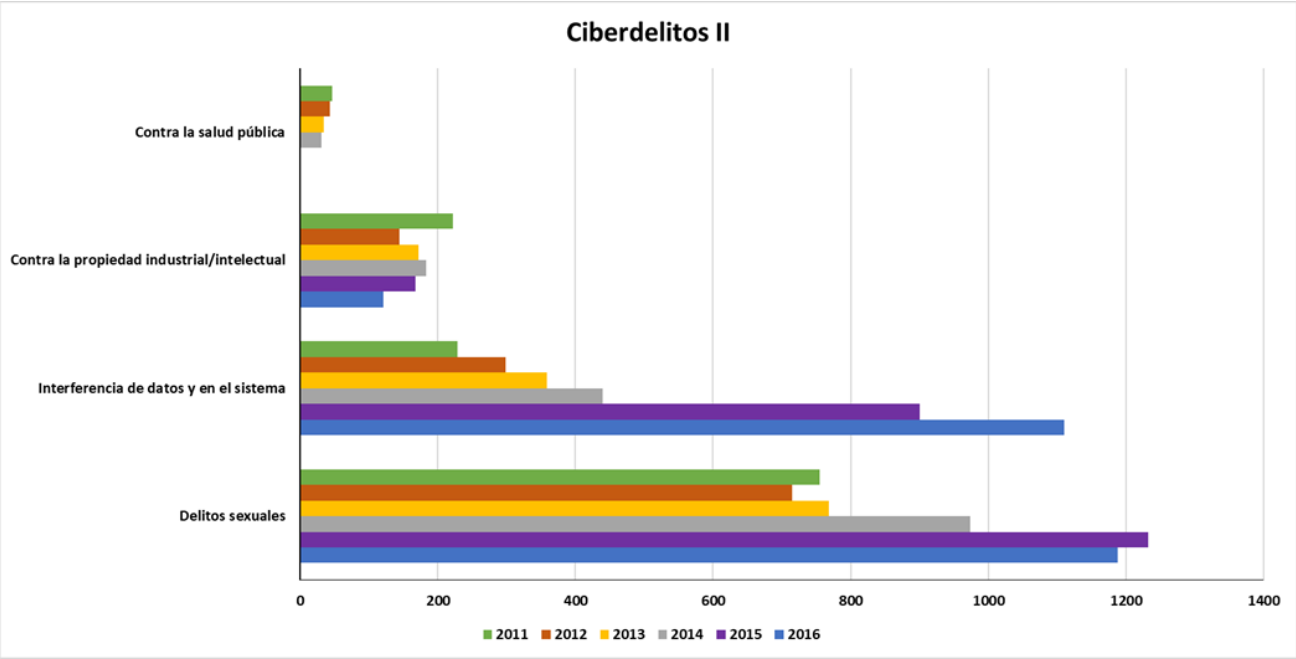

Figura 3: Ciberdelitos por tipologías (II). Fuente: http://oedi.es/estadisticas/. Elaboración propia

Para identificar mejor los ciberdelitos es necesario conocerlos, por lo que se muestran a continuación algunos de aquellos que se utilizan para llevar a cabo los crímenes mostrados anteriormente, y de los que se mostrarán ejemplos prácticos de algunos de ellos en apartados posteriores:

Phishing: es la técnica que aprovecha el gran uso que se les da a los correos electrónicos. Utilizando este mismo medio de contacto para perpetuar sus delitos los ciberdelincuentes se hacen pasar por entidades legítimas para sonsacar de este modo la información privada a las personas (Oficina de Seguridad del internauta, 2014).

El tipo de correos que emplean suelen tener asociados enlaces a páginas falsas donde suplantan la identidad de distintas empresas o servicios, aprovechándose en muchas ocasiones de la confianza que puedan tener los individuos en dichas páginas webs. Entre los casos más utilizados se encuentran los siguientes:

- Entidades bancarias: aprovechando excusas como, problemas en la seguridad de la cuenta, cambios de normativas en la compañía, bloqueos o desactivaciones de algunos servicios, etc. pretenden apropiarse de los números de tarjeta, PIN secretos o claves de seguridad, entre otras cosas. Un ejemplo de uso de esta técnica se puede encontrar en la noticia número 18 del apartado “Presentación de casos”.

- Redes sociales: empleando los pretextos de cambios de credenciales, conexiones irregulares desde otros dispositivos, notificaciones de la cuenta, etc. buscan hacerse con las identificaciones y contraseñas de los usuarios para, principalmente, robar sus cuentas (20 minutos, 2018A).

- Sistemas de pago online: suplantando pasarelas de pagos, tales como PayPal, Visa, etc. pretende hacer creer que han ocurrido intentos de intrusismo en las cuentas, cambios de normativas o inicios de sesión incorrectos. El objetivo de este método es conseguir los datos bancarios y privados del individuo, así como robar dinero.

- Páginas de compra/venta y subastas: al igual que en los casos anteriores el motivo que emplean para estafar en nombre de plataformas como EBay, Amazon u otras webs similares, es apropiarse de los datos personales del usuario para estafarlo económicamente. Secundando este fin alegan cambios de normativas de la web, intentos de intrusión de otros usuarios, problemas de inicio de sesión, etc.

- Soporte técnico de empresas y servicios: a través de falsas confirmaciones de cuentas como Outlook, Gmail, Apple, etc., informes de actividades sospechosas o avisos de que la capacidad de almacenamiento ha llegado al máximo, entre otras, intentan robar las cuentas e información personal de las personas. En el artículo 20 del décimo apartado hay un ejemplo de este caso.

Muchos de los casos anteriores se centran en atacar a la mayor cantidad posible de individuos, pero también existen otro tipo de ataques enfocados a empresas o personas específicas *(spear phishing)* con la finalidad de efectuar robos financieros, chantajes, obtenciones de datos sensibles o confidenciales, etc. Con este fin se usan ataques de denegación de servicios, ransomware, ataques a empleados de alto nivel con técnicas anteriores u herramientas varias que faciliten el ataque a las empresas elegidas. Un ejemplo a ataques a altos directivos es el caso 19 que aparece en un apartado posterior.

Pharming: esta amenaza recibe el nombre de la mezcla de "phishing" y "farming". Este método envenena la caché del DNS *(Domain Name System)*, el sistema que permite relacionar las direcciones IP de las máquinas donde están alojados los dominios a los que se desee acceder, con nombres más fáciles de recordar. Por ejemplo, www.google.es en lugar de 66.102.11.104.

Existen dos maneras de que este ataque se lleve a cabo. La primera, a través de un virus o troyano que infectando el ordenador cambie el archivo host del equipo, desviando el tráfico a un sitio web falso. El segundo, envenenando directamente un servidor DNS, de modo que varios usuarios accedan a la web infectada sin saberlo. Este hecho no se corrige escribiendo la dirección web manualmente en el navegador, ya que ocurre automáticamente cuando el equipo envía una solicitud de conexión, por lo que puede ser más complicado darse cuenta (Kaspersky Lab, 2018).

La finalidad habitual de este ciberdelito es el robo de información personal y financiera para la suplantación de identidad (Oficina de Seguridad del internauta, 2018A).

Sextorsión: se trata de la extorsión con fotos o videos de contenido altamente sensible y en muchos casos de índole sexual, obtenidas a menudo a través del sexting. Los fines pueden ser, obtener dinero, más contenido pornográfico o llevar a cabo coacciones para tener relaciones sexuales, dominando la voluntad de la víctima, entre otros. Pueden llevarse a cabo con personas conocidas o no, abarcando como víctimas de este hecho tanto a mayores de edad como a menores (Pantallas amigas, 2018).

Este delito puede darse acompañado por el grooming o acoso sexual en internet o el ciberbulling, entre otros. En futuros apartados se presentan distintas casuísticas de esto.

Malware: es el término abreviado de *"malicious software"*, se considera como tal todo tipo de software o código informático malicioso que pretenda acceder a un dispositivo sin el permiso ni conocimiento de otro usuario (Avast, 2018).

Algunos ejemplos de malware son los siguientes:

- Virus: son programas que se incrustan en archivos de un equipo con la principal finalidad de propagarse a otros haciendo copias de sí mismo.
- Backdoors: permiten crear brechas en los sistemas para que el ciberdelincuente pueda tener acceso a los equipos.

- Botnet: es una red de ordenadores infectados que son controlados por una persona u organización. Las botnet son utilizadas usualmente para conseguir contraseñas y datos personales, realizar denegaciones de servicio, manipular encuestas u otro tipo de fraudes. Entre los indicios para reconocer si el sistema está infectado se encuentran: un funcionamiento lento del equipo, mensajes de error inesperados, ventiladores que se ejecutan aun cuando el equipo permanece inactivo, etc.

- Gusanos: son programas muy parecidos a los virus con la singularidad de que pueden replicarse a sí mismos para propagarse, por lo que pueden continuar funcionando, aunque se elimine el archivo del que nacieron.

- Troyanos: son programas que permiten al ciberdelincuente obtener acceso total al ordenador de la víctima, de modo que le permita robar datos o dañar el ordenador. Según la tipología del troyano el ataque puede estar más centrado en un tipo de ataque u otro. Esto permite al atacante que pueda realizar acciones como: encender la webcam, realizar cambios en el sistema, copiar archivos, etc.

- Keylogger: es un software que registra todo aquello que se escribe en el teclado. De este modo, quedan almacenadas todas las conversaciones, documentos, registros, contraseñas, datos bancarios y personales, etc. que se escriban. En el caso 31 del apartado "Presentación de casos" puede consultarse un ejemplo de esta técnica.

- Rootkit: es un conjunto de herramientas que los intrusos informáticos suelen utilizar para ocultar sus huellas. Por ejemplo, mostrando información falsa al intentar encontrar los procesos que se estén ejecutando, escondiendo archivos de la vista del usuario o engañando al antivirus para evitar que desinfecte el equipo (CERT-PY, 2018).

- Spyware: este malware se encarga de reunir información sobre los hábitos de navegación, búsquedas y sitios visitados, así como la información solicitada en estas webs. Puede atacar tanto a personas como a organizaciones y habitualmente se usa la información recogida como moneda de venta.

- Ransomware: se encarga de cifrar el contenido del sistema para evitar su acceso a él. A cambio de devolverlo y recuperar los datos, se deben seguir las instrucciones que muestre. Normalmente estas directrices incluyen el pago de una cantidad específica de dinero como rescate. Esto es lo que ocurre con el ramsonware SamSam mencionado en el capítulo 42 de este estudio.

5. Estudio legal de la suplantación de identidad

Antes de presentar la legislación que afecta a este delito, es necesario diferenciar las distintas designaciones empleadas a la hora de hablar de suplantación de identidad que pueden encontrarse en internet.

Falsa identidad: es resultado de la creación de un perfil falso, o la utilización del nombre y apellidos de otra persona, sin hacer uso de información personal como fotografías. Esta acción en sí misma no es ilegal, ya que el hecho en sí no perjudica al individuo.

Robo de identidad: se produce al sustraer las claves y contraseñas de acceso a internet o redes sociales de otro individuo. Puede implicar o no suplantación de identidad, pero el acto en sí es delictivo.

Suplantación de identidad: se lleva a cabo cuando una persona se hace pasar por otra ante terceros, sea de manera privada o pública. Generalmente, la finalidad por la que este hecho se produce es con un carácter ilegal o con el propósito de cometer algún perjurio.

En el estudio que nos ocupa nos centraremos en el último aspecto, la suplantación de la identidad. Para ello se hablará de algunos métodos empleados para llevarla a cabo, tales como la ingeniería social, la falsedad documental y la firma digital, así como las principales motivaciones, y la legislación afectada.

Uno de los métodos más utilizados, además de los anteriormente vistos en el apartado de delitos informáticos, es el uso de la ingeniería social. Esta técnica permite disminuir en gran medida el uso técnico de la informática, sustituyéndolo por la psicología, aunque no por ello es algo de menor dificultad. El principio que proclama esta práctica es que los usuarios son el eslabón débil.

La ingeniería social puede definirse como el conjunto de técnicas de tipo social que pueden usar ciertos individuos, grupos u organizaciones de cualquier tipo para manipular o persuadir a objetivos humanos con la intención de que realicen acciones, tomen decisiones o revelen información valiosa para el atacante de manera voluntaria (Ramos, 2015: 17).

Además de esta, la falsedad documental es otra de las técnicas utilizadas para los ciberdelitos. Esta se produce cuando los delincuentes alteran un documento en alguno de sus elementos o requisitos de carácter esencial; simulan un documento en todo o en parte, de manera que induzca a error sobre su autenticidad; suponen en un acto la intervención de personas que no la han tenido; atribuyen a las que han intervenido en él

declaraciones o manifestaciones diferentes de las que hubieran hecho; o faltan a la verdad en la narración de los hechos.

El acceso a la firma digital es otro de los métodos que puede usar el criminal para hacerse con el poder de nuestra información. La firma digital es un conjunto de datos asociados a un mensaje digital que garantizan la identidad del firmante y la integridad del mensaje, es decir, que el contenido del mismo no haya sido alterado en el trascurso del envío. Debido a la naturaleza de este sistema, la falsificación de una firma digital da lugar a un delito de falsedad documental ya que el firmante resulta ser un individuo distinto del que dice ser.

En el funcionamiento de la firma digital se hace uso de dos claves, la pública y la privada. La clave pública puede ser mostrada libremente y no tiene importancia si otra persona accede a ella. Es utilizada para poder leer el contenido del mensaje. En cambio, la clave privada debe mantenerse en secreto hacia terceros ya que es la que se utiliza para cifrar los mensajes que se envían y permitirá, junto a la clave pública, descifrar el mensaje, ya que es lo que prueba que el documento no se ha visto comprometido y que es el mismo que se mandó en un primer momento (Martínez y Alcover, 1998: 47-49).

Por tanto, el peligro de este método reside en la clave privada, ya que si alguien se adueña de ella podrá hacerse pasar por dicha persona y firmar cualquier documento. Tal como se ha visto anteriormente, el factor humano es el eslabón más débil en la cadena de la seguridad, por lo que el ciberdelincuente puede intentar hacerse dueño de la clave privada accediendo a nuestros ordenadores si esta no se encuentra debidamente protegida. Es importante que la clave no se guarde a simple vista de los demás y se ponga el esfuerzo necesario para mantenerla a salvo.

También hay que asegurarse de que la clave ha sido generada por un prestador de servicios de certificación confiable, usando un software criptográfico reconocido internacionalmente y aprobado por un laboratorio especializado en el tema. De no ser así, el peligro comienza desde su creación y la clave privada podría no ser segura.

Los fines para los que se lleva a cabo la suplantación de identidad suelen estar relacionados con la venganza personal. Para llevar a cabo esto suelen subirse imágenes de la persona suplantada acompañadas de textos vejatorios, o añadiendo datos personales tales como direcciones o números telefónicos para aumentar el daño a la víctima.

Tampoco es necesario que el delincuente posea el deseo de herir a la otra persona. En algunas ocasiones, el perpetuador de este hecho puede hacerlo sin la consciencia necesaria. La motivación perseguida podría ser la simple búsqueda de diversión, usando internet de ese modo para reírse de terceros. Esta conducta no es menos peligrosa que las demás ya que puede desembocar también en graves daños psicológicos para la víctima.

Otro de los motivos por los que se puede llevar a cabo esta mala práctica es el monetario. Conseguir recaudar dinero a través de estafas, robos de cuentas bancarias o la extorsión son algunos de los medios utilizados para lograrlo.

En referencia a la legislación que se aplica contra la usurpación de identidad en internet, cabe destacar que no existen leyes de aplicación exacta a esta situación. Esto es debido a una desactualización de las leyes que todavía están adaptándose a este nuevo entorno informático y a los problemas que acarrea. A pesar de esto, existen normas que aun siendo algo antiguas pueden amoldarse a las situaciones pertinentes. Por esto, se muestran a continuación una serie de leyes recogidas en diversos documentos y que tratan el tema desde la visión de la protección de datos, el derecho a la intimidad, la propia usurpación del estado civil o las consecuencias del daño acarreado a elementos informáticos, también llamado *cracking*.

Para facilitar la visualización de las mismas se han clasificado jerárquicamente en función del ámbito al que afectan. Así pues, en primer lugar, aparece la legislación supranacional, la cual afecta a todos los Estados. En segundo lugar, legislación nacional se divide en la Constitución Española, la Ley Orgánica de Protección Jurídica del Menor y, por último, el código civil. Debido a la cantidad de artículos referenciados del Código Civil, se han agrupado de manera ordenada según los títulos a los que corresponden, tal y como aparecen en la siguiente imagen.

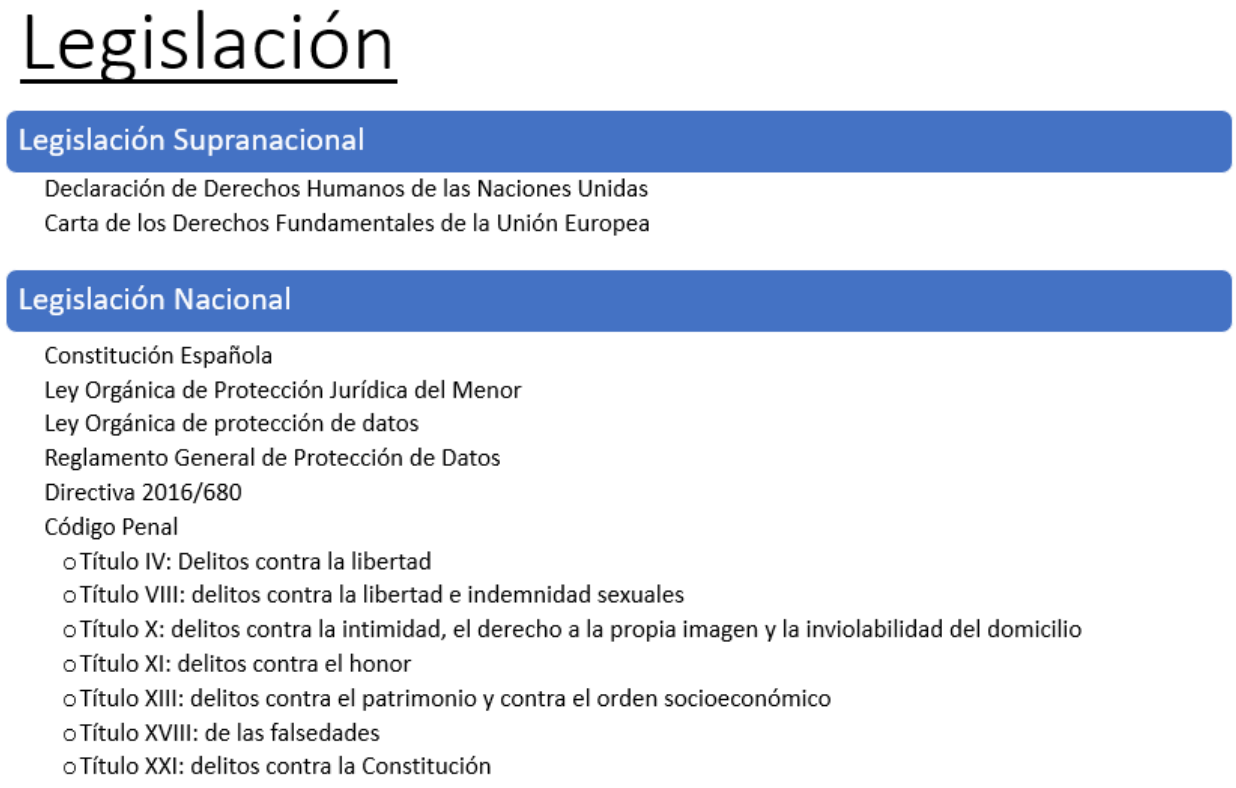

Figura 4: Esquema de la legislación utilizada. Elaboración propia.

Legislación Supranacional

Artículo 12 de la Declaración de Derechos Humanos de las Naciones Unidas

"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" (Naciones Unidas, 2018).

Artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea

"Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones" (Diario Oficial de la Unión Europea, 2000).

Legislación Nacional

Constitución Española

Artículo 10 de la Constitución Española

"La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social".

Artículo 18 de la Constitución Española

1: *"Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen"*

4: *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".*

Artículo 39 de la Constitución Española

4: *"Los niños gozarán de la protección prevista en los acuerdos internacionales que velan por sus derechos"* (Agencia Estatal Boletín del Estado, 1978).

Ley Orgánica de Protección Jurídica del Menor

Artículo 4 de la Ley Orgánica de Protección Jurídica del Menor

"Se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales" (Agencia Estatal Boletín del Estado, 1996).

Código Penal

Título IV: Delitos contra la libertad

Artículo 169 del Código Penal:

"El que amenazare a otro con causarle a él, a su familia o a otras personas con las que esté íntimamente vinculado un mal que constituya delitos de homicidio, lesiones, aborto, contra la libertad, torturas y contra la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio y el orden socioeconómico, será castigado:

> ***1.º** Con la pena de prisión de uno a cinco años, si se hubiere hecho la amenaza exigiendo una cantidad o imponiendo cualquier otra condición, aunque no sea ilícita, y el culpable hubiere conseguido su propósito. De no conseguirlo, se impondrá la pena de prisión de seis meses a tres años.*

Las penas señaladas en el párrafo anterior se impondrán en su mitad superior si las amenazas se hicieren por escrito, por teléfono o por cualquier medio de comunicación o de reproducción, o en nombre de entidades o grupos reales o supuestos.

> ***2.º** Con la pena de prisión de seis meses a dos años, cuando la amenaza no haya sido condicional"* (Agencia Estatal Boletín del Estado, 1995).

Artículo 171 del Código Penal:

***1.** "Las amenazas de un mal que no constituya delito serán castigadas con pena de prisión de tres meses a un año o multa de seis a 24 meses, atendidas la gravedad y circunstancia del hecho, cuando la amenaza fuere condicional y la condición no consistiere en una conducta debida. Si el culpable hubiere conseguido su propósito se le impondrá la pena en su mitad superior".*

***2.** "Si alguien exigiere de otro una cantidad o recompensa bajo la amenaza de revelar o difundir hechos referentes a su vida privada o relaciones familiares que no sean públicamente conocidos y puedan afectar a su fama, crédito o interés, será castigado con la pena de prisión de dos a cuatro años, si ha conseguido la entrega de todo o parte de lo exigido, y con la de cuatro meses a dos años, si no lo consiguiere".*

Artículo 172 ter. del Código Penal:

1. *"Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:*

> ***1.ª*** *La vigile, la persiga o busque su cercanía física.*
>
> ***2.ª*** *Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.*
>
> ***3.ª*** *Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.*
>
> ***4.ª*** *Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.*

Si se trata de una persona especialmente vulnerable por razón de su edad, enfermedad o situación, se impondrá la pena de prisión de seis meses a dos años".

2. *"Cuando el ofendido fuere alguna de las personas a las que se refiere el apartado 2 del artículo 173, se impondrá una pena de prisión de uno a dos años, o trabajos en beneficio de la comunidad de sesenta a ciento veinte días. En este caso no será necesaria la denuncia a que se refiere el apartado 4 de este artículo".*

Título VIII: delitos contra la libertad e indemnidad sexuales

Artículo 183 bis. del Código Penal

"El que, con fines sexuales, determine a un menor de dieciséis años a participar en un comportamiento de naturaleza sexual, o le haga presenciar actos de carácter sexual, aunque el autor no participe en ellos, será castigado con una pena de prisión de seis meses a dos años.

Si le hubiera hecho presenciar abusos sexuales, aunque el autor no hubiera participado en ellos, se impondrá una pena de prisión de uno a tres años".

Artículo 183 ter. del Código Penal

1. *"El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años*

de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño".

2. *"El que, a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años".*

Artículo 189 del Código Penal

1. *"Será castigado con la pena de prisión de uno a cinco años:*

> ***a)*** *El que captare o utilizare a menores de edad o a personas con discapacidad necesitadas de especial protección con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas.*
>
> ***b)*** *El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido".*

2. *"Serán castigados con la pena de prisión de cinco a nueve años los que realicen los actos previstos en el apartado 1 de este artículo cuando concurra alguna de las circunstancias siguientes:*

> ***a)*** *Cuando se utilice a menores de dieciséis años.*
>
> ***b)*** *Cuando los hechos revistan un carácter particularmente degradante o vejatorio.*
>
> ***c)*** *Cuando el material pornográfico represente a menores o a personas con discapacidad necesitadas de especial protección que sean víctimas de violencia física o sexual.*
>
> ***d)*** *Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, la vida o salud de la víctima.*
>
> ***e)*** *Cuando el material pornográfico fuera de notoria importancia.*
>
> ***f)*** *Cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.*

g) *Cuando el responsable sea ascendiente, tutor, curador, guardador, maestro o cualquier otra persona encargada, de hecho, aunque fuera provisionalmente, o de derecho, del menor o persona con discapacidad necesitada de especial protección, o se trate de cualquier otro miembro de su familia que conviva con él o de otra persona que haya actuado abusando de su posición reconocida de confianza o autoridad.*

h) *Cuando concurra la agravante de reincidencia".*

Título X: delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio

Artículo 197 del Código Penal:

1: "*El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses".*

2: "*Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero".*

7: "*Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona".*

bis.1*: "El que, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años".*

bis.2: *"El que, mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las*

emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses".

Artículo 201 del Código Penal

1. *"Para proceder por los delitos previstos en este Capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, persona con discapacidad necesitada de especial protección o una persona desvalida, también podrá denunciar el Ministerio Fiscal".*

Título XI: delitos contra el honor

Artículo 205 del Código Penal

"Es calumnia la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad".

Artículo 206 del Código Penal

"Las calumnias serán castigadas con las penas de prisión de seis meses a dos años o multa de doce a 24 meses, si se propagaran con publicidad y, en otro caso, con multa de seis a 12 meses".

Artículo 208 del Código Penal

"Es injuria la acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

Solamente serán constitutivas de delito las injurias que, por su naturaleza, efectos y circunstancias, sean tenidas en el concepto público por graves, sin perjuicio de lo dispuesto en el apartado 4 del artículo 173.

Las injurias que consistan en la imputación de hechos no se considerarán graves, salvo cuando se hayan llevado a cabo con conocimiento de su falsedad o temerario desprecio hacia la verdad".

Artículo 209 del Código Penal

"Las injurias graves hechas con publicidad se castigarán con la pena de multa de seis a catorce meses y, en otro caso, con la de tres a siete meses".

Título XIII: delitos contra el patrimonio y contra el orden socioeconómico

Artículo 248 del Código Penal

1. *"Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno".*

2. *"También se consideran reos de estafa:*

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

Artículo 250 del Código Penal

1. "*El delito de estafa será castigado con las penas de prisión de uno a seis años y multa de seis a doce meses, cuando:*

> ***1.º*** *Recaiga sobre cosas de primera necesidad, viviendas u otros bienes de reconocida utilidad social.*
>
> ***2.º*** *Se perpetre abusando de firma de otro, o sustrayendo, ocultando o inutilizando, en todo o en parte, algún proceso, expediente, protocolo o documento público u oficial de cualquier clase.*
>
> ***3.º*** *Recaiga sobre bienes que integren el patrimonio artístico, histórico, cultural o científico.*
>
> ***4.º*** *Revista especial gravedad, atendiendo a la entidad del perjuicio y a la situación económica en que deje a la víctima o a su familia.*
>
> ***5.º*** *El valor de la defraudación supere los 50.000 euros, o afecte a un elevado número de personas.*
>
> ***6.º*** *Se cometa con abuso de las relaciones personales existentes entre víctima y defraudador, o aproveche éste su credibilidad empresarial o profesional.*

7.º *Se cometa estafa procesal. Incurren en la misma los que, en un procedimiento judicial de cualquier clase, manipularen las pruebas en que pretendieran fundar sus alegaciones o emplearen otro fraude procesal análogo, provocando error en el juez o tribunal y llevándole a dictar una resolución que perjudique los intereses económicos de la otra parte o de un tercero.*

8.º *Al delinquir el culpable hubiera sido condenado ejecutoriamente al menos por tres delitos comprendidos en este Capítulo. No se tendrán en cuenta antecedentes cancelados o que debieran serlo".*

2. "*Si concurrieran las circunstancias incluidas en los numerales 4.º, 5.º, 6.º o 7.º con la del numeral 1.º del apartado anterior, se impondrán las penas de prisión de cuatro a ocho años y multa de doce a veinticuatro meses. La misma pena se impondrá cuando el valor de la defraudación supere los 250.000 euros".*

Artículo 264 del Código Penal

1. *"El que, por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años".*

2. *"Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:*

1.ª *Se hubiese cometido en el marco de una organización criminal.*

2.ª *Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.*

3.ª *El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.*

4.ª *Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.*

5.ª *El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter.*

Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado".

3. *"Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero".*

Artículo 264 bis. del Código Penal

1. *"Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno:*

> ***a)*** *realizando alguna de las conductas a que se refiere el artículo anterior;*
>
> ***b)*** *introduciendo o transmitiendo datos; o*
>
> ***c)*** *destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.*

Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado".

2. *"Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior".*

3. *"Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero".*

Artículo 264 ter. del Código Penal

"Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores:

> ***a)*** *un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o*

b) *una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información".*

Título XVIII: de las falsedades

Artículo 392 del Código Penal

1. *"El particular que cometiere en documento público, oficial o mercantil, alguna de las falsedades descritas en los tres primeros números del apartado 1 del artículo 390*[1]*, será castigado con las penas de prisión de seis meses a tres años y multa de seis a doce meses".*

2. *"Las mismas penas se impondrán al que, sin haber intervenido en la falsificación, traficare de cualquier modo con un documento de identidad falso. Se impondrá la pena de prisión de seis meses a un año y multa de tres a seis meses al que hiciere uso, a sabiendas, de un documento de identidad falso".*

Artículo 401 del Código Penal

"El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años".

Artículo 402 del Código Penal

"El que ilegítimamente ejerciere actos propios de una autoridad o funcionario público atribuyéndose carácter oficial, será castigado con la pena de prisión de uno a tres años".

Título XXI: delitos contra la Constitución

Artículo 510 del Código Penal

1. "*Serán castigados con una pena de prisión de uno a cuatro años y multa de seis a doce meses:*

a) *Quienes públicamente fomenten, promuevan o inciten directa o indirectamente al odio, hostilidad, discriminación o violencia contra un grupo,*

[1] El delito de falsedad documental se produce al: alterar un documento en alguno de sus elementos o requisitos de carácter esencial, simular un documento en todo o en parte, de manera que induzca a error sobre su autenticidad, suponiendo en un acto la intervención de personas que no la han tenido, o al atribuir a las que han intervenido en él declaraciones o manifestaciones diferentes de las que hubieran hecho o faltando a la verdad en la narración de los hechos (Agencia Estatal Boletín del Estado, 1995).

una parte del mismo o contra una persona determinada por razón de su pertenencia a aquél, por motivos racistas, antisemitas u otros referentes a la ideología, religión o creencias, situación familiar, la pertenencia de sus miembros a una etnia, raza o nación, su origen nacional, su sexo, orientación o identidad sexual, por razones de género, enfermedad o discapacidad".

6. Actualización de la ley de protección de datos

A lo largo del tiempo, tal y como se puede observar en la figura que aparece a continuación, la legislación referente a la protección de datos ha ido modificándose y expandiéndose según las necesidades del momento.

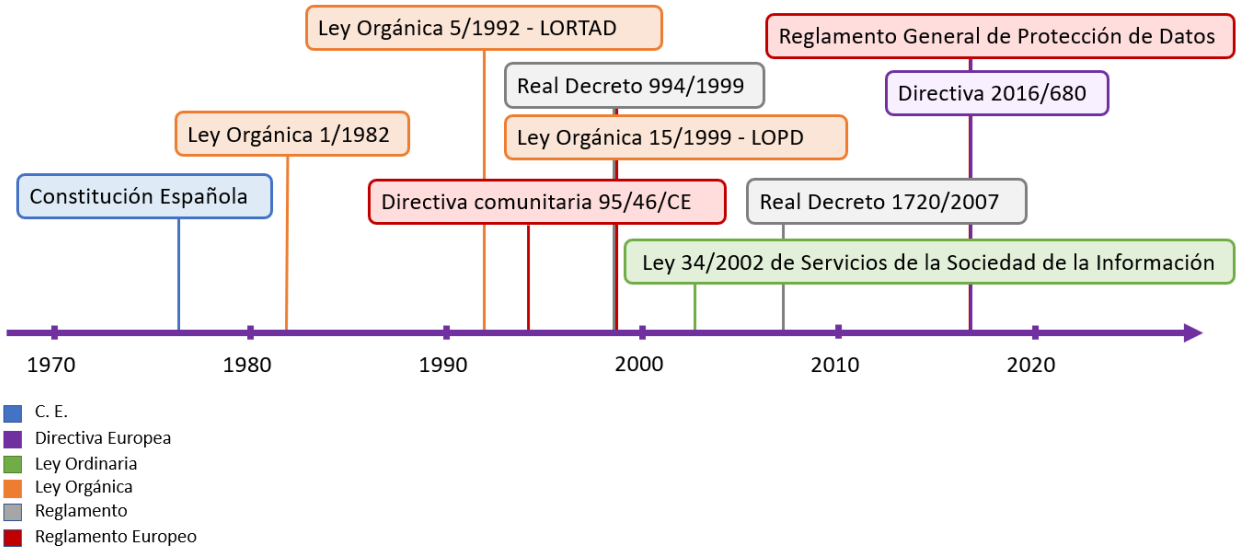

Figura 5: Línea temporal de la legislación sobre protección de datos. Elaboración propia.

En relación a esto, el 14 de abril de 2016 se aprobó el Reglamento General de Protección de Datos (RGPD), que entró en vigor el 25 de mayo de 2018. Este reglamento reemplaza a la Directiva 95/46/EC relativa a la protección de datos en su función de unificar las leyes de privacidad de datos en toda Europa (EU General Data Protection Regulation, 2018).

El objetivo del reglamento es proteger a todos los ciudadanos europeos de las infracciones en los datos y en la privacidad de las personas, dado que la directiva anterior, al datar de 1995, quedaba desfasada ante la nueva realidad de un mundo que cada día se basa más en la información.

El propósito es que los usuarios puedan comprender de manera directa y sencilla qué tipo de datos tratan las empresas, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo (Agencia Española de Protección de Datos, 2018A).

Los principios de privacidad no han variado mucho de la directiva anterior, pero se han propuesto muchos cambios a las políticas regulatorias. A continuación, se muestran los puntos clave del nuevo reglamento, así como el impacto que tendrá en las empresas.

Jurisdicción ampliada: anteriormente la aplicación territorial de la directiva podía no ser precisa, en cambio en la actual queda descrito que todas aquellas empresas que procesen datos personales de individuos que residan en la Unión Europea deben cumplir con el reglamento, independientemente de la localización de la compañía. Esta medida engloba también a aquellas empresas dedicadas al almacenamiento de datos, sea en la nube o no, o a las que ofrezcan servicios a los ciudadanos, sean o no de pago.

Sanciones: las empresas que infrinjan el reglamento pueden ser sancionadas con una multa de hasta 20 millones de euros o un 4% de la facturación anual de la compañía, optando por la opción mayor. Esta es la multa máxima que se puede imponer por las infracciones más graves, por ejemplo, no tener el consentimiento del cliente para procesar sus datos. Existe un sistema escalonado de las multas, por ejemplo, una empresa puede recibir una multa del 2% por no tener sus registros en orden, o por no notificar a la autoridad supervisora y al titular de los datos sobre una infracción o evaluación del sistema.

Consentimiento: las condiciones para obtener el consentimiento por parte de los usuarios han sido fortalecidas, de modo que en la actualidad es necesario que se soliciten utilizando fórmulas fácilmente comprensibles para el usuario, con un lenguaje sencillo y claro. Este consentimiento debe aparecer de manera diferenciada de otras materias, facilitando así su visualización y asegurando que el usuario autorice todos los distintos tratamientos. Por tanto, el consentimiento, debe ser inequívoco y explícito. Además, debe ofrecerse una manera sencilla de revocar dicho consentimiento en cualquier momento.

Notificación de brecha de seguridad: el aviso de cualquier riesgo de filtración o violación de datos, que pueda generar un riesgo para los derechos y libertades de las personas, deberá ser emitido inmediatamente por todas las empresas. Esto debe hacerse dentro de las 72 horas de haberse dado cuenta de la violación por primera vez.

Derecho de acceso: los interesados pueden obtener información del Delegado de Protección de Datos sobre si sus datos personales están siendo procesados, dónde y con qué propósito. Además, se podrá solicitar una copia de sus datos, sin cargo, en formato electrónico.

Derecho al olvido: cualquier persona podrá solicitar al responsable del tratamiento de datos que elimine sus datos personales, cese la divulgación de estos y, potencialmente, detenga el uso de dicha información por terceros (Agencia Española de Protección de Datos, 2018B). Las condiciones para llevar a cabo esta solicitud de borrado, tal como aparecen descritas en el artículo 17 (Diario Oficial de la Unión Europea, 2016B), incluyen que los datos ya no sean relevantes para los propósitos originales de su procesamiento, o que los usuarios retiren el consentimiento. También se debe tener en cuenta que este derecho requiere que los controladores de datos comparen los derechos de los usuarios al "interés público de la disponibilidad de los datos" al considerar tales solicitudes, por lo que es posible que no siempre se acepten todas las solicitudes.

Portabilidad de datos: el usuario deberá recibir los datos que le conciernen tras solicitarlos al personal correspondiente, en un formato legible y de uso común. La información que contenga deberá ser concisa, transparente, comprensible y de fácil acceso, con un lenguaje claro y sencillo. Además, tiene derecho a mandar está información a otro controlador de datos.

Protección de datos desde el diseño: se propone la inclusión de la privacidad desde el principio del diseño de los sistemas, en lugar de ser una adición posterior. De este modo los que controlan la información solo poseerán aquella que sea absolutamente necesaria para el cumplimiento de las funciones de la compañía, minimizando los datos almacenados y limitando su acceso a únicamente las personas indispensables para su tratamiento.

Delegado protector de datos: esta persona es la encargada de asegurar el correcto uso de los datos almacenador por las compañías. En el caso de los organismos públicos será obligatorio que cuenten con este responsable, pero en aquellas empresas privadas solo será necesario cuando los datos sean tratados a gran escala o se trate de información muy sensible, que pueda incluso estar relacionada con condenas y delitos penales. Si, además, la empresa tiene menos de 250 trabajadores, no tendrá que llevar un registro.

Entre las características del delegado se encuentran:

- Poseer conocimientos especializados sobre legislación y prácticas de protección de datos.
- Ser un miembro del personal o un proveedor de servicios externo.
- Proporcionar los datos de contacto a la autoridad pertinente, en este caso, la Agencia Española de Protección de Datos.
- Contar con los recursos adecuados para llevar a cabo sus tareas y mantener su conocimiento.
- Informar directamente al más alto cargo.
- No realizar ninguna otra tarea que pueda generar un conflicto de intereses.

Las funciones del delegado son:

- Informar y asesorar al responsable del tratamiento de datos, así como al resto de empleados, de las obligaciones del RPGD y cualquier otra normativa aplicable en protección de datos.
- Supervisar el cumplimiento del RGPD y demás normativa aplicable en protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.

- Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

- Cooperar con la autoridad de control. actuando como punto de contacto para cuestiones relativas al tratamiento de datos o cualquier otra consulta (Agencia Española de Protección de Datos, 2018C).

Complementariamente al RGPD, la Directiva 2016/680 asegura la protección de los datos personales "en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario", como es el caso de las actividades en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial.

En esta directiva se establecen las normas específicas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública (Diario Oficial de la Unión Europea, 2016A).

Implantación del Reglamento en empresas

La Agencia Española de Protección de Datos proporciona la herramienta "Facilita_RGPD" (Agencia Española de Protección de Datos, 2018D) para ayudar a los responsables del tratamiento de datos cuyas empresas trabajan con información de escaso nivel de riesgo. Así como una hoja de ruta para ayudar a cumplir el Reglamento en todas sus fases a aquellas organizaciones que trabajen con datos de alto riesgo (Agencia Española de Protección de Datos, 2018E).

En ese aspecto, para aquellas entidades cuyas actividades impliquen un alto riesgo, deberán analizar cada una de ellas para decidir si se necesita una evaluación de impacto relativa a la protección de datos (EIPD) (Agencia Española de Protección de Datos, 2018F: 11).

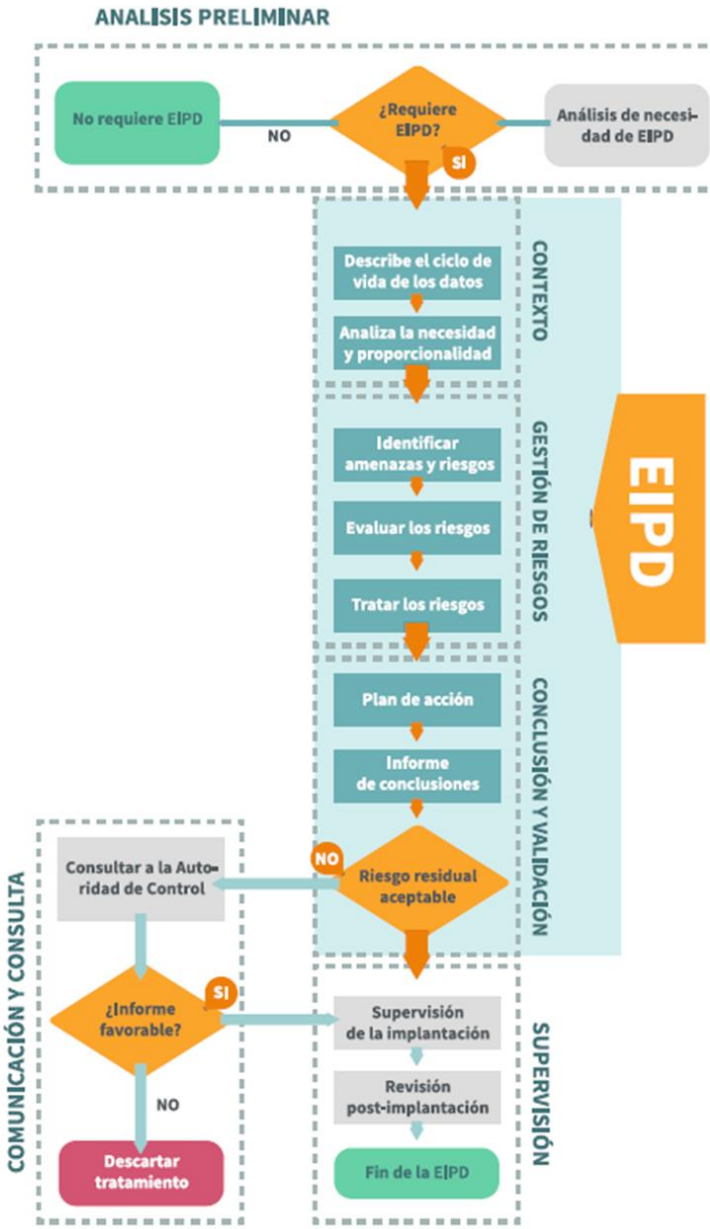

Figura 2: Guía para implantar una EIPD. Fuente: Agencia Española de Protección de Datos.

La manera de analizar cada casuística es contrastándola con las listas de supuestos que requieren de una EIPD, las cuales se enumeran en el RGPD. De este modo, si el tratamiento coincide con alguno de los casos, se deberá documentar en un informe de análisis la necesidad de realizar la EIPD y llevarla a cabo. En caso contrario, deberá documentarse que no aparece en ninguna de las listas de supuestos, asegurándose bien de este hecho.

También debe evaluarse las características de las actividades de tratamiento de datos según su naturaleza, alcance, contexto y finalidad para decidir si conllevan un grave riesgo.

En el caso de que las actividades de tratamiento no supongan un alto riesgo y, por tanto, no se requiera de un EIPD, se deberá realizar un análisis básico de riesgos. Las

actividades deben agruparse según los procesos que tienen en común que posean riesgos parecidos, generando medidas de seguridad y control estándar para todos ellos (Agencia Española de Protección de Datos, 2018G).

Además de esto, cada responsable de datos debe llevar un registro de las actividades de tratamiento realizadas bajo su responsabilidad. Dicho registro, de acuerdo con el artículo 30 del RGPD debe contener la siguiente información:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;

b) los fines del tratamiento;

c) una descripción de las categorías de interesados y de las categorías de datos personales;

d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;

g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

El representante del responsable de datos debe, a su vez, presentar el registro de todas las categorías de actividades de tratamiento que haya llevado a cabo el responsable. El registro debe contener:

a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;

b) las categorías de tratamientos efectuados por cuenta de cada responsable;

c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.

7. Una nueva forma de acoso

El acoso, en sus múltiples formas, existe desde hace mucho tiempo, pero con la llegada de las tecnologías de información y comunicación, como las redes sociales, internet o la telefonía móvil, el acoso ha encontrado un nuevo entorno donde materializarse. De este modo, internet provee de un lugar disponible las 24 horas diarias y sin barreras geográficas, en el que se puede humillar, difamar o chantajear a una persona de manera anónima.

Respecto a la procedencia, el ciberacoso puede darse entre personas que tienen o han tenido alguna relación, como puedan ser parejas estables o esporádicas; amistades; o familiares. Se producen por motivos directa o indirectamente vinculados a la esfera afectiva. En estos casos, en alguna medida, el ciberacoso tiene un importante componente emotivo como los celos, la envidia, el odio, la venganza, o la incapacidad de aceptar un rechazo.

En otras ocasiones no hay ni tan siquiera relación afectiva de ningún tipo, y se acosa por la existencia de una relación puramente profesional. Los desencadenantes pueden ser envidias en el trabajo, debido a ascensos o a un sentimiento de infravaloración frente a dicho compañero, o debido a la preexistencia de un ambiente laboral tóxico en el que no se han tomado ningún tipo de medidas para refrenarlo.

Y, en otras ocasiones, se realiza por el mero placer de aterrorizar a la víctima, de atacar, humillar, difamar, amenazar… por la única satisfacción del proceso de elaboración del acto violento y porque quien acosa está en el convencimiento o creencia que tiene una justa causa para acosar (Pachés, Fernando, 2017).

La facilidad de crear un perfil en las redes sociales facilita mucho su uso y proliferación. Pero también es uno de los factores que hace tan sencillo realizar en ellos la usurpación de identidad o ciberacoso.

Para llevar a cabo este hecho es necesario, entre otras cosas, conocer algunos detalles de la persona a la que se va a suplantar, los cuales también se pueden saber por medio de estas mismas redes sociales. Por ejemplo, se puede conseguir información básica como nombre, apellidos, edad o localización a través de alguna de las diferentes redes. Así mismo, también es posible conseguir imágenes en las que aparezca dicha persona.

Con todos estos datos el siguiente paso sería crear una cuenta de e-mail falso, lo cual tampoco es difícil de conseguir, ya que muchas veces una misma persona puede tener varias cuentas de correo electrónico de diversas compañías. O incluso se pueden hacer usos de e-mails temporales.

Una vez hecho todo lo anterior solo se necesitaría unir toda la información en la red social elegida con la finalidad deseada. Las opciones podrían ser las siguientes: crear el

perfil a nombre de la persona suplantada para crear una falsa imagen de ella; crear perfiles ficticios de personas de su alrededor para hablar mal de dicha persona y crear un ambiente de desconfianza además de las subyacentes injurias; o inventar varias personas ficticias para arremeter contra la víctima y propiciar la suma de más perfiles al ataque. Las posibilidades que ofrecen estos perfiles son numerosas y variadas, lamentablemente las consecuencias en que desembocan tienden a generar daños irreparables para la persona perjudicada.

Algunas de las características principales del ciberbullyng son las siguientes:

- Se trata de un ataque habitualmente anónimo, facilitado por el uso de las tecnologías. La víctima puede desconocer quién es el atacante, incluso en el caso ser varios, estos pueden no saber quiénes son sus cómplices.

- El ciberbullyng puede darse en el ámbito privado, donde solamente atañe al agresor y a la víctima, o en el ámbito público, donde terceras personas son testigos de estos hechos.

- El acoso debe ser reiterado o de duración prolongada en el tiempo. Esto también incluye aquellas acciones que el agresor realiza una única vez, pero por su proliferación la víctima recibe el ataque de manera repetida. Por ejemplo, si se publica una imagen para ridiculizar a una persona, cada vez que esta se divulgue o comente por otros reiterará el daño a la víctima.

Si se tiene consciencia del acto de acoso se debe remitir a las entidades pertinentes para tomar medidas en el menor tiempo posible. También es necesario recabar la mayor cantidad de pruebas posibles, esto incluye obtener información de las personas involucradas como los agresores y sus familiares, así como posibles testigos del ámbito escolar o profesorado. Cualquier comentario vejatorio o coacción debe ser recogido del mismo modo, sin importar si se dan por medio de redes sociales o servicios de mensajería. Se pueden utilizar capturas de pantalla para obtener dichos datos. Asimismo, se le puede hacer ver al agresor que su comportamiento no es adecuado, de una manera pacífica pero clara, de modo que posea conocimiento de causa.

La responsabilidad legal afecta a los agresores, sean o no menores de edad, a los padres o tutores legales en caso de ser menor de edad el autor de los hechos, y al centro donde tuviesen acto esas acciones, como pueda ser el colegio, las clases extraescolares, excursiones, etc. Tanto los adultos como las instituciones se deben hacer cargo del pago de las sanciones económicas y de las administrativas disciplinarias.

Respecto a los menores, si son mayores de 14 años, les afecta la LORPM. Por lo que según el art. 7 de la misma (Agencia Estatal Boletín del Estado, 2000), las medidas que podrían serles impuestas son las siguientes:

- Internamiento en régimen cerrado, semiabierto o abierto.

- Internamiento terapéutico en régimen cerrado, semiabierto o abierto.

- Tratamiento ambulatorio.
- Asistencia a un centro de día.
- Permanencia de fin de semana.
- Libertad vigilada.
- Prohibición de acercarse o comunicarse con la víctima o sus familiares según determine el juez.
- Convivencia con otra persona, familia o grupo educativo.
- Prestaciones en beneficio de la comunidad.
- Realización de tareas socioeducativas.
- Amonestación.
- Privación del permiso de conducir ciclomotores y vehículos a motor, o del derecho a obtenerlo, o de las licencias administrativas para caza o para uso de cualquier tipo de armas.
- Inhabilitación absoluta, incluyendo la incapacidad para obtener otros honores, cargos o empleos públicos, o de ser elegido para cargo público.

Por otra parte, a los menores de 14 años se les aplica las siguientes normas sobre protección del Código Civil:

Artículo 9 quáter de la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia.

2. "Los menores tienen que respetar a los profesores y otros empleados de los centros escolares, así como al resto de sus compañeros, evitando situaciones de conflicto y acoso escolar en cualquiera de sus formas, incluyendo el ciberacoso" (Agencia Estatal Boletín del Estado, 2015).

Art. 1903 del código civil

"Los padres son responsables de los daños causados por los hijos que se encuentren bajo su guarda.

Los tutores lo son de los perjuicios causados por los menores o incapacitados que están bajo su autoridad y habitan en su compañía.

Lo son igualmente los dueños o directores de un establecimiento o empresa respecto de los perjuicios causados por sus dependientes en el servicio de los ramos en que los tuvieran empleados, o con ocasión de sus funciones.

Las personas o entidades que sean titulares de un Centro docente de enseñanza no superior responderán por los daños y perjuicios que causen sus alumnos menores de edad durante los períodos de tiempo en que los mismos se hallen bajo el control o vigilancia del profesorado del Centro, desarrollando actividades escolares o extraescolares y complementarias.

La responsabilidad de que trata este artículo cesará cuando las personas en él mencionadas prueben que emplearon toda la diligencia de un buen padre de familia para prevenir el daño". (Agencia Estatal Boletín del Estado, 1889).

Con el propósito de mejorar la convivencia en Internet y evitar conflictos, se puede hacer uso de las netiquetas, las cuales son una serie de normas de comportamiento para la red. Algunas de las que se podrían adoptar en el intento de evitar este tipo de situaciones son las siguientes (Netiqueta, 2012):

- Pide permiso antes de publicar fotografías o vídeos de otras personas.
- Dirígete a los demás con respeto.
- Si alguien comete un error comunícaselo de manera privada.
- No etiquetes a otras personas sin su permiso o lo hagas con fines negativos.
- No insultes, humilles o dañes a otras personas.
- No aceptes a personas que no conoces en redes sociales.
- Denuncia aquellos contenidos inapropiados, pero sin caer en la denuncia injusta.
- No reenvíes información sin pedir permiso anteriormente.
- Comunica a tus contactos como quieres que se trate tu información.
- Lee las normas de uso de las páginas que utilizas.
- Recuerda que el uso de las mayúsculas puede ser interpretado como un grito.
- Asegúrate de que al reenviar un mensaje ocultas los destinatarios a los que va dirigido.
- No abras archivos adjuntos de personas desconocidas.

8. Visualización de la suplantación de identidad

La suplantación de identidad, así como otros ciberdelitos, son un problema grave que puede afectar a cualquier persona, por este motivo es importante una buena concienciación. Con el paso del tiempo esta temática ha ido cobrando fuerza e imponiéndose en la sociedad, no solo a través de películas o talleres si no en campañas de publicidad, usualmente digitales, o en nuevas herramientas virtuales. A continuación, se mostrarán algunas de las medidas que se han utilizado para hacer más visible esta problemática.

Contenido multimedia

Ingrid Goes West: la película trata la adicción a las redes sociales, concretamente Instagram, y del acoso que puede producirse a través de las mismas, obteniendo incluso datos suficientes para convertir el acoso virtual en físico. Esto es lo que se dedica a hacer la protagonista de la película que, tras su primera orden de alejamiento con una *influencer*, se embarca a conocer a otra y ser parte de su mundo. Aparece plasmado también el contraste de aquella persona que busca la privacidad en su vida y aquella otra que no teme hacer público todo lo que hace, sufriendo así las consecuencias (Ingrid Goes West, 2017).

Identity thief: esta película de comedia muestra de una manera desenfadada como una mujer le roba la identidad a un hombre, dejando sus cuentas bancarias en números rojos. Ante la dificultad de detenerla sin pruebas, va él mismo a por ella para llevarla a la justicia (Identity thief, 2013).

Cazadores de trolls: este programa de La Sexta, emitido en 2017, presenta a varias víctimas de ciberacoso o ciberbullyng, con el propósito de desenmascarar a aquellos que están detrás de los ataques. Cada capítulo cuenta la historia de una persona diferente y, una vez encontrados los perpetuadores, no se emiten sus rostros para evitar problemas legales. El programa solo cuenta con una temporada de cuatro capítulos debido a que los productores temían seguir con ella por posibles consecuencias peligrosas para las víctimas y los trabajadores (Cazadores de trolls, 2018).

Catfish: Mentiras en la Red: es una serie estadounidense de siete temporadas y actualmente en emisión. Trata de visibilizar el *catfish*, es decir, personas que crean perfiles falsos en las redes sociales para tratar de enamorar a otras. Cada capítulo presenta a una persona diferente que sospecha estar siendo víctima de *catfish*, por lo que los presentadores tratan de investigar los casos y, finalmente reunirlos, con el propósito de descubrir si es así o no. En estos casos no se tratan de intentos de estafas como podría suceder en otras situaciones, aun así, muestra otra cara de internet que puede

servir para que otros desconfíen más de quienes puedan estar tras la pantalla del ordenador (Catfish, 2017).

Campañas de publicidad

No seas estrella: campaña de publicidad lanzada por Unicef donde se escogen a 9 niños y adolescentes. Los participantes son llevados a un aula montada a modo de rueda de prensa, allí se les efectúan una serie de preguntas basadas en aquellas cosas que suben a las redes sociales. Las preguntas se van volviendo cada vez más específicas y detalladas de manera que muchos de los jóvenes piden el cese de la entrevista o muestran su incomodidad ante la misma (UNICEF, 2017).

Love Story: Movistar junto a la Policía Nacional y la Guardia Civil, lanza un vídeo de concienciación contra el acoso sexual de menores por internet. La historia se basa en dos jóvenes que se conocen por internet y deciden quedar para verse, descubriéndose que en realidad ambos son adultos (Movistar Espala, 2018).

#OjitoconlaRed: es la tercera campaña presentada por la Agencia Canaria de Investigación, Innovación y Sociedad de la Información, tras la emisión de #TICconcabeza (ViveInternet, 2016) y #noseasanimal (ViveInternet, 2015). En esta serie de diez vídeos donde colaboran personajes famosos de la televisión, deporte y ciencia se busca concienciar de problemas como la suplantación de identidad, ciberacoso y adicción tecnológica, entre otros (ViveInternet, 2017).

Sé un héroe contra el ciberbullying: las fundaciones ONCE, Legálitas, Rudy Fernández y Deporte Joven del Consejo Superior de Deporte colaboran en la creación de un vídeo, distribuido por las redes sociales, con el fin de concienciar a los jóvenes en contra del ciberbullyng e impedir que estos sean cómplices del mismo (Legálitas Abogados, 2016).

Conferencias y talleres

La Rioja: durante cuatro días y con motivo del Día de Internet Seguro, se celebraron dos talleres educativos y una jornada sobre el *blockchain* en La Rioja. El público al que va dirigido son estudiantes de 10 a 14 años. Entre los temas a tratar se encuentran, el ciberacoso, la identidad digital y la ciberseguridad. Hacen uso de ejercicios prácticos sobre hechos cotidianos para evaluar sus acciones y aconsejarles. También accedieron a un mapa especial creado en Minecraft para que solucionasen distintos retos de seguridad (La Rioja, 2018).

Es.pabila: durante tres jueves a lo largo del mes de mayo, la Concejalía de Juventud y el Instituto Nacional de Ciberseguridad, programó tres conferencias sobre ciberseguridad en León. Las dos primeras, sobre ciberbullying y seguridad en redes

sociales, están enfocadas a los jóvenes, mientras que la tercera pretende guiar y enfocar a los padres en cómo deben tratar el uso que hacen sus hijos de la tecnología (Noticiascyl, 2018).

Hackron: la sexta edición de este congreso se producirá entre febrero y marzo de 2019 en Tenerife, donde muchos expertos en la materia de ciberseguridad se reunirán para formar y compartir conocimientos con los asistentes (Hackron, 2018).

I Jornada de Seguridad en Hospitales 4.0: el 10 de julio de 2018 en Madrid se celebra una jornada de concienciación sobre la importancia de la ciberseguridad en los hospitales. Las charlas hablarán sobre los posibles riesgos a los que se expone la información que almacenan y cómo protegerla, así como la introducción de distintas herramientas tecnológicas para ello (Centro de Ciberseguridad Industrial, 2018).

Herramientas

Vulnerómetro: el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ha desarrollado una herramienta on-line para medir el nivel de riesgo de suplantación de identidad que poseas. Este recurso se presenta en forma de semáforo y marca de poco vulnerable a muy vulnerable. Las preguntas que trata abarcan los hábitos de seguridad que posees en el uso del móvil, ordenador y redes sociales (Instituto Nacional de Transparencia, 2018).

Servicio Antibotnet: la Oficina de Seguridad del Internauta ofrece la opción de comprobar que tu ordenador no forme parte de una botnet. Para ello compara tu dirección IP con su base de datos de incidentes de botnets. Aparte de este método se muestra la posibilidad de instalar plugins para que puedan avisarte instantáneamente si la situación cambia (Oficina de Seguridad del internauta, 2018B).

Kit de autodiagnóstico: el Instituto Nacional de Ciberseguridad ofrece a las empresas una evaluación del estado de ciberseguridad a través de un formulario on-line. Al final la realización del mismo se muestra un porcentaje del riesgo al que está sometida la institución. También se muestran los riesgos según respectan a personas, procesos o tecnologías (Instituto Nacional de Ciberseguridad, 2018A).

CONAN mobile: esta app para móviles comprueba que las aplicaciones instalas en tu dispositivo no sean maliciosas, que cuentes con la última actualización en tu software y que tu configuración sea la adecuada (Oficina de Seguridad del internauta, 2018C).

Otros

Hackend: el juego contiene nueve misiones diferentes que poseen distintas fases. En la primera, se deben buscar las posibles amenazas y riesgos de los escenarios que puedan propiciar el robo de información. En la segunda, se realiza un informe de riesgos con lo

encontrado en el paso anterior, ofreciendo los consejos pertinentes para evitar situaciones de riesgo. En la última fase, se debe capturar al culpable viajando por todo el mundo para conseguir pistas sobre su aspecto (Instituto Nacional de Ciberseguridad, 2016A).

Hackers vs Cybercrook: en este juego tomamos el papel de un niño que debe proteger su casa inteligente de un ciberdelincuente. Al mismo tiempo que propone distintos minijuegos para mantener su hogar a salvo, va dando lecciones y consejos sobre ciberseguridad (Instituto Nacional de Ciberseguridad, 2016B).

Juego de rol: el Instituto Nacional de Seguridad presenta cinco casos diferentes para realizar juegos de rol sobre temáticas de ciberseguridad. Está enfocado a pymes y autónomos, para que aprendan a reaccionar adecuadamente ante este tipo de situaciones (Instituto Nacional de Ciberseguridad, 2018B).

Proofup: la aseguradora Das ha creado una app exclusiva para sus clientes, la cual está enfocada a ser usada por aquellos menores que están sufriendo algún tipo de acoso. Su objetivo es poder recabar pruebas para poder denunciar la situación ante las autoridades, de este modo, entre algunas de sus funcionalidades se encuentra el poder guardar capturas de pantalla, grabaciones o ubicaciones en tiempo real (Jané, Carmen, 2017).

9. Rastro digital

El rastro digital se conforma de aquella información que el propio usuario crea sobre sí mismo. La mayoría de información de una persona, perteneciente al universo digital, forma parte de la sombra digital, esta es generada por sistemas que no puede controlar. Se trata de información sobre una persona, almacenada en ficheros financieros o listas de correos, en los historiales de navegación web o en las imágenes obtenidas por las cámaras de seguridad en aeropuertos y centros urbanos (Estudio del universo, 2014).

El resto de la información se crea por las acciones de las propias personas, por ejemplo, a través de publicaciones y comentarios, fotografías, o el envío de correos electrónicos. Esto es lo llamado rastro digital.

A continuación, se analizarán estos rastros a través del buscador Google, consiguiendo de ese modo obtener una pequeña muestra de toda la información que permanece almacenada a ojos de aquellos que sepan encontrarla.

Debido a la naturaleza del tipo de datos que intentan encontrarse, yo misma tomaré el papel de "sujeto de pruebas" y analizaré mi presencia en la red.

Se comenzará por búsquedas simples de nombre completo, comprobando si se puede acceder a información más personal como teléfonos o correos electrónicos. Después se comprobará la información almacenada sobre dichos datos, así como si aparecen imágenes personales. También se realizará búsquedas desde diversas redes sociales. Y, por último, se hará uso de herramientas online para la localización de personas.

Búsquedas sencillas

La primera búsqueda simple en Google radicó en buscar mi nombre completo sin comillas. Sin embargo, dado que en la búsqueda aparecían enlaces en la primera página de Google que conducían a resultados donde, las personas que aparecían compartían alguno de mis apellidos o nombre, pero mis datos no se encontraban en el sitio web, se ha preferido utilizar estrategias de búsqueda que obvien ese tipo de resultados.

Para ello se han realizado las búsquedas haciendo uso del sistema de comillas, de este modo indicamos que lo que intentamos localizar forma parte de una frase exacta. Por consiguiente, los resultados a devolver solo incluirán aquellos donde aparezca literalmente lo que se ha buscado, incluyendo el orden en que aparecen las palabras sin que haya ninguna más por medio.

Así pues, utilizando la búsqueda "Minerva Gamiz Mejias", ya que es como normalmente aparecería si fuese yo la que alimentase de contenido la web, se pueden encontrar los siguientes resultados, enumerados a continuación:

El primero de los enlaces da acceso a mi perfil público de Linkdln, dado que una de las finalidades de este sitio web es darse a conocer y ser encontrado por las empresas, con

el propósito de encontrar empleo, no supone ningún problema que aparezca en primer lugar. Además, se trata de un perfil creado por propia voluntad en el que no aparecen datos sensibles.

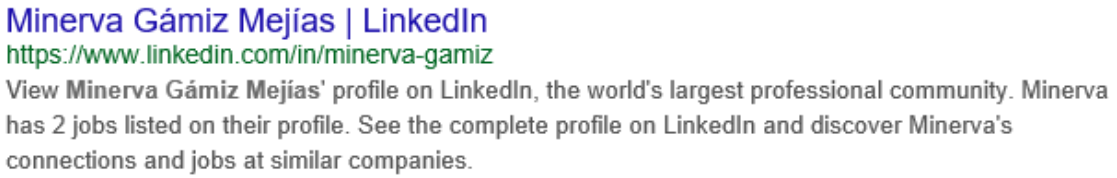

Figura 6: Rastro digital (I). Fuente: Google. Elaboración propia.

Tanto el segundo y tercer enlace se basan en distintos filtros de la página Linkdln anteriormente nombrada. En estos se agrupan personas que compartan conmigo alguno de mis apellidos o nombre.

Figura 7: Rastro digital (II). Fuente: Google. Elaboración propia.

Por último, el cuarto enlace, redirige a la página de Slideshare, donde debido a un trabajo práctico de la universidad subíamos a la red una presentación gráfica haciendo uso de la indización de contenido. Las diapositivas hacen referencia a un lugar donde trabajé, lo cual junto a mi nombre y primer apellido es la única información personal que aparece. Estos datos, además, también son localizables en mi perfil de Linkdln.

Figura 8: Rastro digital (III). Fuente: Google. Elaboración propia.

Respecto a la lista de fotografías que Google Imágenes tiene asociadas a ese nombre, en mi caso, la única foto que aparecería sería la de Linkdln, pero dado que todavía no incluí ninguna, tampoco puede verse. También aparecen varias imágenes del trabajo académico anteriormente explicado, además de un conjunto de imágenes de perfil de aquellas personas que aparecían en los filtros de Linkdln que compartían algún apellido o nombre.

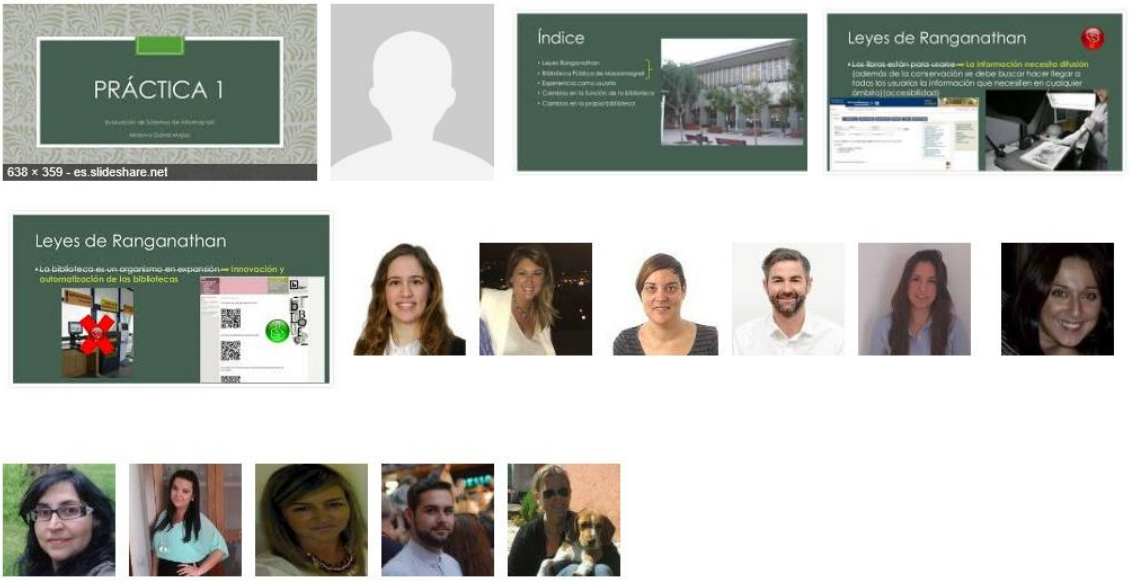

Figura 9: Rastro digital (IV). Fuente: Google. Elaboración propia.

La siguiente búsqueda realizada en Google imita el modo en que las instituciones almacenan habitualmente nuestros datos. Esto es, primero los apellidos y después el nombre.

Respecto a los resultados obtenidos de la búsqueda "Gamiz Mejias Minerva", se observa lo siguiente:

Los primeros dos enlaces listan los nombres y DNI de mis compañeros del grado en Información y Documentación, cursado en la Universitat de Valencia, con los títulos de los trabajos de final de grado correspondientes que han sido aceptados. También los nombres del tribunal que van a examinarlos y los horarios. En este aspecto, la propia universidad cuenta con un apartado sobre protección de datos en el que habla de como llevar correctamente la LPD (Universitat de Valencia, 2018).

El tercer enlace es un listado, con los nombres completos, de aquellas personas aceptadas en una beca de la diputación que oferta trabajos durante el verano.

El cuarto enlace conduce a una lista de nombres completos y los correspondientes DNIs de aquellas personas a las que se les ha rechazado la beca, así como el motivo de ello. El quinto y sexto, por el contrario, muestra aquellas personas a las que sí se les concedió la beca, el nombre completo, DNIs y cuantía de esta.

El séptimo enlace es un listado de todos los admitidos en cualquier universidad, por lo que cada nombre completo viene acompañado del código que identifica a cada institución.

El octavo, noveno y décimo enlace muestran otro listado de nombres completos junto a DNIs con motivo de varias oposiciones en las que me registré.

Los otros cuatro resultados son repeticiones de lo anteriormente dicho: dos convocatorias a oposiciones, un listado de alumnos según universidad y la cantidad de dinero concedida a cada alumno en una beca.

Redes sociales

Para asegurar la búsqueda en las redes sociales, se han realizado búsquedas especificas por cada una de las más utilizadas actualmente y que podrían arrojar más información útil para una suplantación de identidad: Facebook, Twitter e Instagram.

Se han utilizado las siguientes estrategias de búsqueda:

- minerva gamiz mejias site: facebook.com
- “minerva gamiz mejias” site: facebook.com
- minerva gamiz site: facebook.com
- “minerva gamiz” site: facebook.com
- minerva site: facebook.com

- minerva gamiz mejias site: twitter.com
- “minerva gamiz mejias” site: twitter.com
- minerva gamiz site: twitter.com
- “minerva gamiz” site: twitter.com
- minerva site: twitter.com

- minerva gamiz mejias site: instagram.com
- “minerva gamiz mejias” instagram.com
- minerva gamiz site: instagram.com
- “minerva gamiz” site: instagram.com
- minerva site: instagram.com

Ninguna de las búsquedas arroja información útil dado que utilizo pseudónimos en todas mis redes sociales. Esto puede ser una mecánica utilizada por muchas otras personas en diversas redes, sobre todo aquellas destinadas únicamente a la visualización de imágenes o fotografías como Instagram.

A pesar de ello, si se dispusiera de información sobre familia o amigos de la persona que se quisiese encontrar, se podría efectuar una búsqueda entre sus contactos usando nombres o seudónimos conocidos para intentar localizarla.

Según si dichos familiares y conocidos tuviesen los perfiles públicos o privados podría dificultar más o menos el encontrar algún tipo de información útil.

Además de esto, es necesario tener en cuenta que aun con la seudonimización de los nombres en las redes sociales, podemos ser encontrados por la dirección IP de los dispositivos que utilicemos al conectarnos a internet. Del mismo modo ocurre con el artículo 25 del RGPD[2] y la seudonimización de nuestros datos que poseen las empresas. Es necesaria una estrecha vigilancia sobre el tipo de datos que se almacenan, pues, aunque puedan estar anonimizados, si en algún fichero aparece por error el nombre real de la persona a la que pertenecen, se conocerá la identidad a la que corresponden el resto de los datos que aparezcan relacionados con esta.

Teléfono y correo electrónico

Tras buscar en Google los tres números telefónicos con los que cuento, dos móviles y un teléfono fijo, no se ha encontrado información de interés. Únicamente aparecen páginas para conocer si son números utilizados para efectuar spam.

Respecto a los correos electrónicos, se ha intentado localizar cuatro e-mails diferentes, dos de Gmail, uno de Hotmail y el correo personal de la universidad. De nuevo, ninguna de estas búsquedas ha dado resultados útiles.

Imágenes

Para profundizar más en el uso de Google Imágenes, y dado que los resultados por imágenes obtenidos en las búsquedas sencillas anteriores no dieron buenos frutos, se ha utilizado la herramienta de "Buscar por imagen" que ofrece la plataforma

Para ello se han efectuado dos pruebas, la primera de ellas consistió en subir una fotografía clara del rostro de modo que pueda ser más fácilmente identificada por otras imágenes visibles en Google. A pesar de esto, ninguno de los resultados correspondía con la persona utilizada.

[2] *"Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados"* (Diario Oficial de la Unión Europea, 2016A).

Figura 10: Rastro digital (V). Fuente: Google. Elaboración propia.

En la segunda prueba se utilizó una fotografía publicada en Facebook desde un perfil público hace un par de años, en esta aparecen también otras personas para ampliar la posibilidad de que el reconocimiento pudiese ser efectivo. A pesar de todo esto ninguno de los resultados se corresponden, de hecho, ni siquiera aparece algún enlace a Facebook.

Figura 11: Rastro digital (VI). Fuente: Google. Elaboración propia.

Sitios webs especializados

Finalmente, existen páginas webs que ofrecen sus servicios para encontrar personas, por lo que introduciendo su nombre completo y opcionalmente su mote o localización podría devolver resultados de ciertos datos interesantes para quien los busca. Por ejemplo, aparición en redes sociales, edad, números de teléfono, ubicación, correos o personas relacionadas, entre otros.

Pero debido a la naturaleza volátil de Internet, y de la naturaleza de los datos que proveen estos sitios webs, muchos de aquellos que todavía funcionaban en 2017 ahora han cerrado.

Entre aquellas páginas que aún subsisten se encuentran:

Pipl.com, una web que muestra nombre completo, edad, lugar de trabajo, educación, asociaciones con otras personas, lugares de residencia, idiomas, así como un listado de las redes sociales en las que se puede encontrar a dicha persona.

Webmii.com, donde encontrar el nombre completo, empleo, fotografías o vídeos en que aparece la persona o que la haya publicado, palabras clave, personas relacionadas y resultados en búsquedas específicas de redes sociales.

Snitch.name, una web que permite buscar al mismo tiempo en una gran cantidad de sitios distintas webs. La realidad de ello es que la mayoría de estas webs están caídas, y el resto son búsquedas sencillas en cada sitio, que además deben ser abiertas en páginas nuevas para su visualización, ya que el anunciante no permite que la información se muestre en marcos. Pese a todo, puede ser un punto de partida para ver las distintas webs que utiliza al buscar la información y probar en ellas.

Yasni.es aparece citado en muchos resultados sobre buscadores de personas, ofrece fotografías de las personas buscadas, localidad y redes sociales, entre otros. A pesar de esto, se han realizado múltiples consultas de diversas maneras y normalmente no daba ningún tipo de información, ni siquiera de LinkedIn.

Por tanto, en el caso estudiado no se ha encontrado una gran cantidad de información útil dado el recelo con el que se proporcionaron los datos a Internet desde un primer momento. El uso de pseudónimos, múltiples cuentas de correo electrónico según el sitio web, la privacidad en las redes sociales o el bajo número de fotos publicadas son factores que propician pasar de manera más desapercibida en las redes.

A pesar de esto, hay personas que no dudan en publicar su fecha de nacimiento, nombre completo, lugar de residencia, correos electrónicos y/o números de móvil. Estos hechos pueden facilitar el hallazgo de nuevos datos como el DNI o derivar en un mal uso de los mismos como, por ejemplo, su uso en servicios de SMS Premium, suplantación de identidad en sitios web de redes de contactos o servicios de índole sexual, mentir a compañías para cambiar de servicios o, en definitiva, ser víctimas de estafas o bromas.

La geografía puede afectar también a la facilidad de encontrar datos de personas en Internet. Respecto a los sitios webs se han encontrado un mayor número y variedad de páginas que operan en Estados Unidos y brindan la ocasión de encontrar personas por nombre completo. También pueden localizarse reos, o personas con cargos de delitos sexuales o acoso por localidad.

10. Casos

A lo largo de este apartado se presentan una serie de casos recogidos de diversas fuentes de información, relacionados con los ciberdelitos. La mayoría de estos, tienen como nexo común la usurpación de identidad como elemento clave. Para favorecer su lectura se han clasificado atendiendo a los objetivos perseguidos, pero cabe destacar que a pesar de esto no se tratan de categorías mutuamente excluyentes. Por ejemplo, una suplantación a una organización puede ser parte también de una estafa.

Finalmente, la estructura planteada es la siguiente:

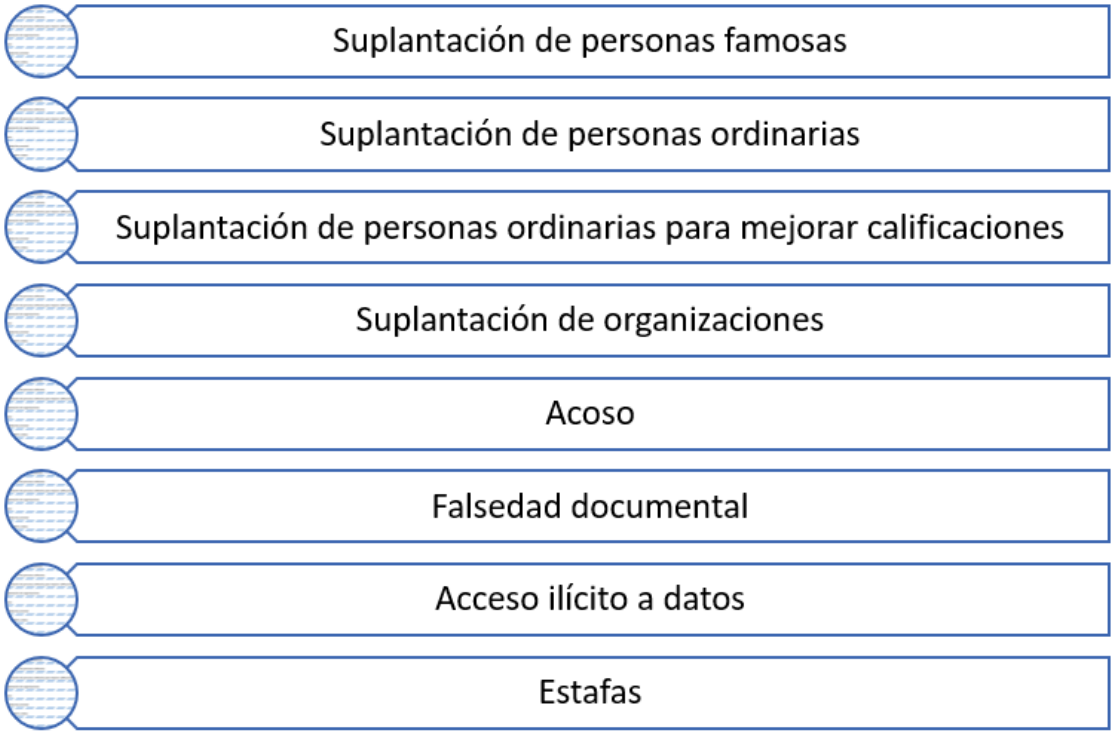

Figura 12:Estructura de la presentación de los casos. Elaboración propia.

Suplantación de personas famosas

ID	01
Fuente	Periódico El Norte de Castilla[3].
Fecha	1 enero 2018.
Inicio de la investigación	Desconocido.
Lugar	On-line.
Titulo	Suplantan la identidad de Silvia Abascal.
Ámbito	Redes sociales.

[3] http://www.elnortedecastilla.es/gente-estilo/suplantan-identidad-facebook-20171229183143-nt.html (16 junio 2018)

Descripción	La actriz Silvia Abascal descubre que un fan ha suplantado su identidad en Facebook y lo comunica por Instagram.
Delitos	Usurpación de estado civil.
Relación con la victima	Fan.
Finalidad	Obtener la atención de otros fans.
Medidas técnicas	Generar un aviso cuando varias personas utilicen los mismos nombres y apellidos, o implantar cuentas verificadas.
Edad del acusado	Desconocida.
Sexo del acusado	Desconocido.

ID	**02**
Fuente	Periódico La República[4].
Fecha	28 noviembre 2017.
Inicio de la investigación	Desconocido.
Lugar	On-line.
Titulo	Suplantan la identidad de Neymar.
Ámbito	Redes sociales.
Descripción	El jugador de fútbol Neymar Jr. denuncia a través de Instagram Stories que dos personas diferentes han suplantado su identidad por móvil para mensajearse con los medios de comunicación en su nombre. Como solución ha pedido a sus fans que denuncien a los culpables, compartiendo fotos con sus números de teléfono.
Delitos	Usurpación de estado civil.
Relación con la victima	Desconocida.
Finalidad	Posiblemente monetaria.
Medidas técnicas	Contactar con la empresa representante para contrastar la información.
Edad del acusado	Desconocida.
Sexo del acusado	Hombre.

ID	**03**
Fuente	Periódico La Vanguardia[5].

[4] https://larepublica.pe/tendencias/1150979-neymar-denuncia-suplantacion-de-identidad-en-instagram-imAgenes (16 junio 2018)

Fecha	23 febrero 2017.
Inicio de la investigación	Desconocido.
Lugar	On-line.
Titulo	Suplantan la identidad a Belén Esteban.
Ámbito	Redes sociales.
Descripción	Suplantan la identidad de la colaboradora de Telecinco, Belén Esteban, a través de Facebook. La finalidad de esto es realizar una estafa monetaria utilizando una supuesta recaudación de dinero.
Delitos	Usurpación del estado civil y estafa.
Relación con la victima	Desconocida.
Finalidad	Monetaria.
Medidas técnicas	Generar un aviso cuando varias personas utilicen los mismos nombres y apellidos, o implantar cuentas verificadas.
Edad del acusado	Desconocida.
Sexo del acusado	Desconocido.

ID	**04**
Fuente	Periódico El País[6].
Fecha	4 diciembre 2017.
Inicio de la investigación	Desconocido.
Lugar	On-line.
Titulo	Suplantan la identidad a Chris Pratt.
Ámbito	Redes sociales.
Descripción	El actor Chris Pratt alerta de que su identidad ha sido suplantada en Facebook. El impostor utiliza la red social para ligar con las fans femeninas, pidiéndoles el teléfono y posiblemente información más íntima.
Delitos	Usurpación de estado civil.
Relación con la victima	Desconocida.
Finalidad	Obtención de datos sensibles.
Medidas técnicas	Generar un aviso cuando varias personas utilicen los mismos nombres y apellidos, o implantar cuentas verificadas.
Edad del acusado	Desconocida.

[5] http://www.lavanguardia.com/television/20170322/421097031899/belen-esteban-denuncia-facebook-suplantacion-estafa-salvame.html (16 junio 2018)

[6] https://elpais.com/elpais/2017/12/04/gente/1512389157_857046.html?rel=str_articulo#1524496894239 (16 junio 2018)

Sexo del acusado	Desconocido.

Suplantación de personas ordinarias

ID	05
Fuente	Aranzadi Instituciones[7].
Fecha	3 de septiembre de 2012.
Inicio de la investigación	mayo 2012.
Lugar	Andalucía.
Titulo	Acusado de estafa clama ser víctima de usurpación de identidad.
Ámbito	Compra-venta online.
Descripción	Estafan a un hombre 250 euros con motivo de la compra de un ordenador que nunca llega. El acusado mantiene que alguien le ha usurpado su identidad ya que perdió su DNI en fecha anterior a estos hechos.
Delitos	Estafa.
Relación con la victima	Supuesto vendedor.
Finalidad	Monetaria.
Medidas técnicas	Realizar las compras mediante plataformas seguras o cara a cara.
Edad del acusado	Desconocida.
Sexo del acusado	Hombre.

ID	06
Fuente	Aranzadi Instituciones[8].
Fecha	17 de noviembre de 2016.
Inicio de la investigación	14 de junio de 2016.
Lugar	Gandía.
Titulo	Una madre se hace pasar por su hija para contratar una línea telefónica.
Ámbito	Falsedad documental.
Descripción	La madre de la demandante usurpa la identidad de esta para contratar una línea telefónica y obtener un terminal nuevo.
Delitos	Usurpación de identidad y falsedad documental.
Relación con la victima	Madre.
Finalidad	Contratación de servicio.
Medidas	Corroborar la identidad del que llama.

[7] **ECLI:** ES:APCO:2012:934
[8] **ECLI:** ES:APV:2016:2316A

técnicas	
Edad del acusado	Desconocida.
Sexo del acusado	Mujer.

ID	**07**
Fuente	Aranzadi Instituciones[9].
Fecha	15 de septiembre de 2017.
Inicio de la investigación	Desconocido.
Lugar	Madrid.
Titulo	Suplanta a otra persona por obtener un móvil nuevo.
Ámbito	Falsedad documental.
Descripción	La denunciada efectúa un cambio de contrato telefónico de una compañía a otra para obtener un móvil de regalo y una línea de internet, dando los datos y cuenta bancaria de la demandante. Dichos datos los pudo obtener mientras trabaja en el domicilio, antes de despedirla tras sospechar que podía haber robado un anillo de oro. De este hecho puede darse cuenta al dejar de dar señal su teléfono móvil.
Delitos	Usurpación del estado civil y estafa.
Relación con la victima	Antigua empleada.
Finalidad	Vengativa.
Medidas técnicas	Guardar los documentos con información sensible en un lugar seguro, oculto al ojo ajeno.
Edad del acusado	25.
Sexo del acusado	Mujer.

ID	**08**
Fuente	Europa press[10].
Fecha	30 de noviembre de 2016.
Inicio de la investigación	Desconocido.
Lugar	Burgos.
Titulo	Utiliza la identidad de un familiar fallecido para vender cobre.
Ámbito	Compra-venta.

[9] **ECLI:** ES:TS:2017:8959A

[10] http://www.europapress.es/castilla-y-leon/noticia-detenido-burgos-utilizar-identidad-familiar-fallecido-vender-9300-kilos-cobre-20161130144721.html (16 junio 2018)

Descripción	En una de las investigaciones rutinarias de la policía en una chatarrería, se percatan de un hombre que vende grandes cantidades de cobre a veces a su propio nombre y otras a la de un tercero. Esa otra persona resulta ser una persona fallecida años atrás. La finalidad de esto era repartir las ganancias de modo que no tuviese que declarar las cantidades a hacienda.
Delitos	Usurpación de estado civil.
Relación con la victima	Cliente.
Finalidad	Monetaria.
Medidas técnicas	Llamar a las autoridades ante la sospecha de una posible estafa.
Edad del acusado	48.
Sexo del acusado	Hombre.

ID	**09**
Fuente	Aranzadi Instituciones[11].
Fecha	22 de octubre de 2009.
Inicio de la investigación	Mayo 2009.
Lugar	Madrid.
Titulo	Utiliza un servicio de mensajería para obtener información acusatoria.
Ámbito	Redes sociales.
Descripción	Una mujer se hace pasar por otra en el programa Messenger, añadiendo a amigos en común haciendo uso de correos electrónicos, y dando opiniones privadas y de carácter íntimo en nombre de la demandante, para dañar su imagen. También se ocupaba de recabar datos íntimos de personas concretas para utilizarlos más tarde de manera dañina.
Delitos	Usurpación del estado civil y falsedad documental.
Relación con la victima	Mismo círculo de amistad.
Finalidad	Vengativa.
Medidas técnicas	Contrastar en persona la creación de nuevas cuentas en redes sociales.
Edad del acusado	Desconocida.
Sexo del acusado	Mujer.

[11] **ECLI:** ES:APM:2009:14226A

ID	10
Fuente	Aranzadi Instituciones[12].
Fecha	22 de febrero de 2017.
Inicio de la investigación	Noviembre 2016.
Lugar	Valladolid.
Titulo	Se hace pasar por su sobrina en Instagram.
Ámbito	Redes sociales.
Descripción	La denunciada crea un perfil a su nombre haciendo uso de la imagen de sobrina. Además, comienza una relación virtual con otra persona a la que le continúa mandando fotos de su sobrina como si fuese ella misma.
Delitos	Usurpación de estado civil.
Relación con la victima	Familiar.
Finalidad	Desconocida.
Medidas técnicas	Realizar búsquedas de nuestras fotografías para localizarlas en otros sitios de las que no se tenga constancia.
Edad del acusado	Desconocida.
Sexo del acusado	Mujer.

Suplantación de personas ordinarias para mejorar calificaciones

ID	11
Fuente	Periódico 20 minutos[13].
Fecha	31 octubre 2013.
Inicio de la investigación	7 de diciembre de 2012.
Lugar	Málaga.
Titulo	Suplanta a una compañera de universidad para poder realizar exámenes vía online.
Ámbito	Organización pública.
Descripción	Una alumna de la universidad de Málaga denunció a otra por suplantar su identidad. El propósito del delito era realizar diversos exámenes usando sus claves, de modo que pudiese conocer las preguntas antes de realizar su propio examen.
Delitos	Delitos de daños, usurpación de estado civil y descubrimiento y revelación de secretos.

[12] **ECLI:** ES:APVA:2017:187A

[13] https://www.20minutos.es/noticia/1963957/0/detienen-universitaria/suplantar-companera/examinarse-internet/ (16 junio 2018)

Relación con la victima	Excompañera de piso.
Finalidad	Obtener mejores calificaciones.
Medidas técnicas	Cerrar sesión en cualquier sitio web donde se esté registrado al dejar sin vigilancia cualquier dispositivo.
Edad del acusado	26.
Sexo del acusado	Mujer.

ID	**12**
Fuente	Periódico La Vanguardia[14].
Fecha	21 marzo 2017.
Inicio de la investigación	17 de febrero.
Lugar	Las Palmas de Gran Canaria.
Titulo	Suplantación de identidad para realizar el examen teórico de conducir.
Ámbito	Organización pública.
Descripción	Se detienen a dos personas en Las Palmas debido a un intento de suplantación de identidad en el examen teórico de conducción. Con el beneplácito de la persona suplantada el acusado se presentó a la prueba, donde se produjeron las dudas de su verdadera identidad y posteriormente se descubrió la verdad. Como agravante de la situación, era la séptima vez que se presentaba al examen debido a que las seis anteriores lo suspendió.
Delitos	Usurpación del estado civil y falsedad documental.
Relación con la victima	Vivían en la misma ciudad.
Finalidad	Aprobar el examen.
Medidas técnicas	Hacer uso de medidas biométricas para validar las identidades de las personas.
Edad del acusado	41.
Sexo del acusado	Hombre.

ID	**13**
Fuente	Periódico Europa Press[15].

[14] http://www.lavanguardia.com/local/canarias/20170321/421063970181/dos-detenidos-por-suplantacion-de-identidad-en-el-examen-del-carne-conducir.html (16 junio 2018)

[15] http://www.europapress.es/murcia/noticia-detenidos-dos-aspirantes-examen-permiso-conduccion-suplantar-identidad-otras-personas-20180202144139.html (16 junio 2018)

Fecha	2 febrero 2018.
Inicio de la investigación	Desconocido.
Lugar	Murcia.
Titulo	Suplantación de identidad en un examen de conducción.
Ámbito	Organización pública.
Descripción	Detienen a dos personas suplantando a otras dos, de la misma nacionalidad, en un examen para el permiso de conducción. Según sus declaraciones no iban a obtener ninguna compensación económica.
Delitos	Usurpación de estado civil y falsedad documental.
Relación con la victima	Misma nacionalidad.
Finalidad	Obtención del permiso de conducción.
Medidas técnicas	Hacer uso de medidas biométricas para validar las identidades de las personas.
Edad del acusado	28 y 22.
Sexo del acusado	Ambos son hombres.

ID	**14**
Fuente	Periódico La Opinión de Murcia[16].
Fecha	25 enero 2018.
Inicio de la investigación	Desconocido.
Lugar	Murcia.
Titulo	Suplantación de identidad para la realización de un examen de conducción.
Ámbito	Organización pública.
Descripción	La Guardia Civil detiene a un hombre, tras darse a la fuga, cuando se descubre que está suplantando la identidad de otra persona, en un examen de conducción, a cambio de dinero.
Delitos	Usurpación de estado civil y falsedad documental.
Relación con la victima	Misma nacionalidad.
Finalidad	Monetaria.
Medidas técnicas	Hacer uso de medidas biométricas para validar las identidades de las personas.
Edad del acusado	30.
Sexo del	Hombre.

16 http://www.laopiniondemurcia.es/murcia/2018/01/25/detenido-aspirante-examen-permiso-conduccion/892877.html (16 junio 2018)

acusado	

ID	15
Fuente	Noticias Castilla y León[17].
Fecha	9 de mayo de 2018.
Inicio de la investigación	Desconocido.
Lugar	Territorio nacional.
Titulo	Detienen a 47 personas dedicadas a hacerse pasar por otras para obtener el diploma de español.
Ámbito	Organización pública.
Descripción	La policía ha detenido a 47 individuos de distintas nacionalidades a lo largo de todo el territorio español. Se dedicaban a pedir entre 1000 y 2000 euros, según era para el examen de conocimiento del idioma o también en el examen de conocimiento general y cultural, así como en relación a la nacionalidad del aspirante y la dificultad atribuida a la misma para aprender el idioma de nuestro país. Después, iban al examen con el DNI de la persona a la que suplantaban o con un documento falso.
Delitos	Usurpación del estado civil y falsedad documental.
Relación con la victima	Desconocida.
Finalidad	Monetaria.
Medidas técnicas	Hacer uso de medidas biométricas para validar las identidades de las personas.
Edad del acusado	Desconocida.
Sexo del acusado	Desconocido.

Suplantación de organizaciones

ID	16
Fuente	Periódico La Opinión de Zamora[18]
Fecha	31 octubre 2017
Inicio de la investigación	A finales de 2016
Lugar	Zamora
Titulo	Suplantan a una compañía eléctrica para estafar al ayuntamiento

[17] https://www.noticiascyl.com/regional/sucesos-regional/2018/05/09/tres-detenidos-en-avila-y-soria-por-suplantar-identidades/ (16 junio 2018)

[18] http://www.laopiniondezamora.es/benavente/2017/11/02/red-rumana-fraude-benavente-estafa/1041750.html (16 junio 2018)

	de Benavente
Ámbito	Phising
Descripción	El Ayuntamiento de Benavente es víctima de una ciberestafa por *phishing* de 42.000 euros tras recibir un correo electrónico en el que se suplanta la identidad de la compañía eléctrica Watium, y se le proporcionaba una nueva cuenta corriente donde ingresar la cuantía de las facturas. Se trata de una banda rumana que estafó a decenas de ayuntamientos y servicios públicos haciendo uso la información sobre contratación de servicios que las empresas publican debido a la Ley de Transparencia. En este caso, el dinero fue devuelto al ayuntamiento dado que se dieron cuenta a tiempo.
Delitos	Estafa, usurpación de estado civil y falsedad documental.
Relación con la victima	Desconocida.
Finalidad	Monetaria.
Medidas técnicas	Comprobar el remitente y la dirección web a la que redirijan los mensajes de compañías para comprobar que son legítimas.
Edad del acusado	Desconocida.
Sexo del acusado	Desconocido.

ID	**17**
Fuente	Aranzadi Instituciones[19].
Fecha	20 de junio de 2012.
Inicio de la investigación	Desconocido.
Lugar	Sevilla.
Titulo	Estafan a varias compañías de seguros al simular distintos siniestros.
Ámbito	Organización privada.
Descripción	El acusado utilizaba facturas falsas a nombre de una empresa de Sevilla con los datos de diversas personas que ya habían denunciado casos de usurpación de estado civil. La estafa consistía en abrir por internet pólizas de seguros en varias aseguradoras simulando siniestros antes del primer mes de pago. De este modo, la aseguradora pagaba por los desperfectos, pero a la hora del cobro mensual se le devolvían los recibos por impagados. Ambos números utilizados, tanto el de cuenta bancaria para recibir los ingresos, como el de la cuenta bancaria de donde debían cobrarse los pagos, eran siempre los mismos.
Delitos	Estafa, usurpación de estado civil y falsedad documental.
Relación con la victima	Supuesto cliente.

[19] **ECLI:** ES:TS:2012:7063A

Finalidad	Monetaria.
Medidas técnicas	Contactar con la empresa de reparación de daños y comprobar que la cuenta bancaria utilizada no esté relacionada con ningún impago.
Edad del acusado	Desconocida.
Sexo del acusado	Hombre.

ID	**18**
Fuente	Instituto Nacional de Ciberseguridad[20].
Fecha	5 de septiembre de 2017.
Inicio de la investigación	Desconocido.
Lugar	Territorio nacional.
Titulo	Suplantan al Banco Sabadell para apoderarse de los datos de acceso a cuentas bancarias.
Ámbito	Phising.
Descripción	Se han detectado una serie de correos electrónicos que simulan provenir del Banco Sabadell alertando de intentos fracasados de entrar en sus cuentas vía internet. Piden a los usuarios que hagan clic en un enlace para confirmar sus datos por motivos de seguridad, y de este modo hacerse con sus datos.
Delitos	Usurpación de estado civil.
Relación con la victima	Desconocida.
Finalidad	Conseguir datos bancarios.
Medidas técnicas	No dar datos personales a bancos por correo electrónico.
Edad del acusado	Desconocida.
Sexo del acusado	Desconocido.

ID	**19**
Fuente	Centro Criptológico Nacional[21].
Fecha	26 de marzo de 2018.

[20] https://www.incibe.es/protege-tu-empresa/avisos-seguridad/campana-phishing-suplantando-al-banco-sabadell (16 junio 2018)

[21] https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/5979-detienen-el-alicante-al-lider-del-grupo-creador-del-apt-carbanak.html (16 junio 2018)

Inicio de la investigación	2013.
Lugar	Alicante.
Titulo	Arrestado el líder detrás de Cobalt y Carbanak.
Ámbito	Spear-phising.
Descripción	La red criminal detenida se dedicaba a enviar correos fraudulentos usurpando la identidad de empresas de cajeros o bancos a las entidades bancarias Una vez los empleados se descargaban el fichero adjunto malicioso del correo y penetraba el virus se encargaban de robar el dinero. Para ello, realizaban transferencias o creaban cuentas fantasmas para mover el efectivo, o hacían que los cajeros expulsasen el dinero para ser recogido por otro de los delincuentes. Más tarde, hacían uso de criptomonedas para eliminar su rastro en la medida de lo posible. Los robos se han producido en más de 100 entidades bancarias diferentes en 40 países de todo el mundo.
Delitos	Estafa, usurpación del estado civil, falsedad documental, blanqueo de capitales y pertenencia a organización criminal.
Relación con la victima	Desconocida.
Finalidad	Monetaria.
Medidas técnicas	Comprobar los remitentes de los correos electrónicos y no descargar adjuntos sin confiar en su destinatario.
Edad del acusado	34.
Sexo del acusado	Hombre.

ID	**20**
Fuente	Oficina de Seguridad del Internauta[22].
Fecha	24 de marzo de 2017.
Inicio de la investigación	Desconocido.
Lugar	Ámbito nacional.
Titulo	Apple cae víctima del phising.
Ámbito	Phising.
Descripción	Un correo fraudulento se hace pasar por Apple y avisa a sus clientes de que debido una violación de seguridad es necesario que validen sus datos. En el formulario que enlazan se solicitan datos personales y bancarios que posteriormente son utilizados para sustraer dinero.
Delitos	Estafa y usurpación del estado civil.
Relación con la	Desconocida.

[22] https://www.osi.es/es/actualidad/avisos/2017/03/nuevo-phishing-apple-quieren-robarte-datos-personales-y-bancarios (16 junio 2018)

victima	
Finalidad	Monetaria.
Medidas técnicas	Comprobar el remitente y la dirección web a la que redirijan los mensajes de compañías para comprobar que son legítimas, y nunca ingresar el PIN de la tarjeta de crédito en formularios web.
Edad del acusado	Desconocida.
Sexo del acusado	Desconocido.

Acoso

ID	21
Fuente	Aranzadi Instituciones[23].
Fecha	16 de marzo de 2012.
Inicio de la investigación	Octubre de 2009.
Lugar	Madrid.
Titulo	Usurpan su identidad y crean un perfil falso ofreciendo sexo gratis.
Ámbito	Redes sociales.
Descripción	Una mujer demanda a tres personas, una antigua amiga, la expareja de la misma y el hijo de este, por crear un perfil falso a su nombre tanto en la red social Tuenti como en Mundo Anuncio, ofreciendo servicios sexuales de manera gratuita. En estas páginas webs aparecía su nombre completo, dirección, número de teléfono y diversas fotografías.
Delitos	Usurpación de identidad e injurias graves proferidas con publicidad.
Relación con la victima	Amistad.
Finalidad	Vejatoria.
Medidas técnicas	Generar un aviso cuando varias personas utilicen los mismos nombres y apellidos.
Edad del acusado	Desconocida.
Sexo del acusado	Dos hombres y una mujer.

[23] **ECLI:** ES:APM:2012:4455A

ID	22
Fuente	Aranzadi Instituciones[24].
Fecha	19 de septiembre de 2011.
Inicio de la investigación	Diciembre de 2010.
Lugar	Sevilla.
Titulo	Se hace pasar por otra persona en distintas páginas con carácter sexual.
Ámbito	Redes sociales.
Descripción	La demandante descubre que alguien se está haciendo pasar por ella en distintas páginas web y chats de contactos con finalidades sexuales. Además, el nombre de usuario utilizado tiene connotaciones negativas.
Delitos	Usurpación de estado civil e injurias graves.
Relación con la victima	Desconocida.
Finalidad	Vejatoria.
Medidas técnicas	Realizar búsquedas por imágenes periódicamente.
Edad del acusado	Desconocida.
Sexo del acusado	Hombre.

ID	23
Fuente	Univisión 34 Los Ángeles[25].
Fecha	10 de abril de 2018.
Inicio de la investigación	2013.
Lugar	California.
Titulo	Concedida una de las mayores indemnizaciones por porno de venganza hasta la fecha.
Ámbito	Redes sociales.
Descripción	Una pareja mantiene una relación a distancia durante un año. Durante este tiempo, la mujer comparte con él una serie de vídeos e imágenes de carácter íntimo que habían acordado que se mantuviesen en privado. Tras su ruptura él comienza a difundir por internet todo este contenido, incluyendo a conocidos personales y profesionales. Además, suplanta la identidad de ella en distintas webs invitando a hombres a ir a casa de ella para mantener relaciones sexuales y pidiendo que envíen imágenes de contenido sexual al teléfono de su expareja. Más tarde crea un

[24] **ECLI:** ES:APSE:2011:2484A

[25] https://www.univision.com/los-angeles/kmex/noticias/actos-delictivos/porno-venganza-su-ex-difundio-videos-y-fotos-intimas-y-ahora-recibe-indemnizacion-de-645-millones (16 junio 2018)

	perfil en una web pornográfica donde sube también todo el material. Finalmente, la víctima debe registrar todo el contenido a su nombre para poseer los derechos de autor y pedir su cese del acceso público. Finalmente, debido al daño que ha sufrido, el estrés emocional y la violación de derechos de autor se la indemniza con más de seis millones.
Delitos	Suplantación de identidad, violación de copyright e injurias.
Relación con la victima	Expareja.
Finalidad	Vengativa.
Medidas técnicas	No compartas ningún tipo de contenido íntimo con otra persona.
Edad del acusado	Desconocida.
Sexo del acusado	Hombre.

ID	**24**
Fuente	Periódico El País[26].
Fecha	13 de febrero de 2017.
Inicio de la investigación	Desconocido.
Lugar	Cádiz.
Titulo	Nuevo caso de grooming en Algeciras.
Ámbito	Redes sociales.
Descripción	Una menor, de 14 años, denuncia a un hombre de 21. Todo comienza en Instagram, donde el detenido se crea una cuenta falsa para atraer a adolescentes. Poco a poco comienzan una amistad por chat y llega un momento en que el acusado amenaza con divulgar información privada que ella le ha compartido si no le envía fotografías eróticas o tienen un encuentro sexual.
Delitos	Abusos de menores, corrupción de menores y descubrimiento y revelación de secretos.
Relación con la victima	Amistad.
Finalidad	Pornográfica.
Medidas técnicas	No compartir información que pueda ser dañina para uno mismo con otras personas.
Edad del acusado	21.
Sexo del acusado	Hombre.

[26] https://politica.elpais.com/politica/2017/02/13/actualidad/1486987884_060902.html (16 junio 2018)

ID	25
Fuente	CNN[27].
Fecha	21 de abril de 2014.
Inicio de la investigación	2013.
Lugar	Florida.
Titulo	Se suicida una niña de 12 años tras sufrir acoso.
Ámbito	Ciberbulling.
Descripción	Detienen a dos estudiantes tras ser acusadas de amenazar y sugerir que se suicidara a una de sus compañeras. El acoso se produjo tanto en el colegio como a través de las redes y desembocó en el suicidio de la joven.
Delitos	Acoso con agravantes.
Relación con la victima	Compañeras de colegio.
Finalidad	Vejatoria.
Medidas técnicas	Tomar medidas ante el primer signo de acoso y enseñar la importancia de la empatía.
Edad del acusado	12 y 14.
Sexo del acusado	Mujer.

ID	26
Fuente	Diario ABC[28].
Fecha	14 de mayo de 2013.
Inicio de la investigación	Desconocido.
Lugar	Málaga.
Titulo	Arrestan a cuatro estudiantes por acosar a una compañera.
Ámbito	Ciberacoso.
Descripción	Detienen a cuatro jóvenes tras acosar durante meses a una compañera que sufría anorexia y a la que mandaron un vídeo una joven con la misma enfermedad que murió. También usaron redes sociales para menoscabar su autoestima y produjeron daños al vehículo de la demandante.
Delitos	Delito contra la integridad moral y daños.
Relación con la victima	Compañeros de instituto.
Finalidad	Vejatoria.

[27] https://edition.cnn.com/2014/04/18/living/rebecca-sedwick-bullying-suicide-follow-parents/index.html (16 junio 2018)
[28] http://www.abc.es/espana/20130514/abci-ciberbullyng-malaga-201305132055.html (16 junio 2018)

Medidas técnicas	Tomar medidas ante el primer signo de acoso y enseñar la importancia de la empatía.
Edad del acusado	Desconocida.
Sexo del acusado	Desconocido.

ID	**27**
Fuente	Periódico El País[29].
Fecha	2 de marzo de 2017.
Inicio de la investigación	Desconocido.
Lugar	Badajoz.
Titulo	Difunden fotos íntimas de una compañera de clase.
Ámbito	Divulgación de datos sensibles.
Descripción	Una niña de 14 años envía a un amigo fotos en ropa interior tras la insistencia de él. Más tarde, las fotografías son divulgadas por el colegio y crean una cuenta en una red social a su nombre donde suben las imágenes y realizan comentarios. A causa de esto se ha detenido a tres menores que fueron los encargados de realizar estas acciones.
Delitos	Descubrimiento y revelación de secretos y usurpación de estado civil.
Relación con la victima	Compañeros de colegio.
Finalidad	Vejatoria.
Medidas técnicas	No compartir información que pueda ser dañina para uno mismo con otras personas.
Edad del acusado	Entre 14 y 16.
Sexo del acusado	Desconocido.

ID	**28**
Fuente	Aranzadi Instituciones[30].
Fecha	29 de mayo de 2017.
Inicio de la investigación	Desconocido.
Lugar	Madrid.

[29] https://politica.elpais.com/politica/2017/03/02/actualidad/1488454374_710153.html (16 junio 2018)
[30] **ECLI:** ES:APM:2017:8783

Titulo	Manipulan fotografías para burlarse de una joven.
Ámbito	Redes sociales.
Descripción	Tres jóvenes suplantan la identidad de otra en la red social Twitter utilizando fotografías extraídas de Tuenti, alterándolas para añadir comentarios obscenos con el objetivo de menoscabar su fama y de humillarla.
Delitos	Falsedad documental, usurpación de estado civil y delito contra la integridad moral.
Relación con la victima	Ex de su actual pareja.
Finalidad	Vengativa.
Medidas técnicas	Generar un aviso cuando varias personas utilicen los mismos nombres y apellidos, o implantar cuentas verificadas.
Edad del acusado	24.
Sexo del acusado	Mujer.

Falsedad documental

ID	29
Fuente	Aranzadi Instituciones[31].
Fecha	3 de mayo de 2018.
Inicio de la investigación	13 de mayo de 2005.
Lugar	Madrid.
Titulo	Una mujer usa una falsa identidad para realizar una demanda.
Ámbito	Falsedad documental.
Descripción	Una mujer demanda a varios hombres por obligarla a prostituirse, violarla y causarle daños físicos. Para realizar dicha demanda utiliza una falsa identidad que le suministraron tiempo atrás para entrar al país. Más tarde, cuando varios de los acusados ya están en la cárcel se descubre la verdadera identidad de la demandante y sus intenciones. Se trata de una trama urdida por otro proxeneta desde la cárcel, el cual fue quien trajo a la demandante al país y con la que tiene una relación sentimental. Los motivos por los que se da este caso son, tanto por el control del ejercicio de prostitución como un impago de la venta de un vehículo.
Delitos	Usurpación de estado civil, falsedad documental y falso testimonio.
Relación con la victima	Supuesto proxeneta.
Finalidad	Vengativa.
Medidas	Comprobar la veracidad del pasaporte al tomar la declaración.

[31] **ECLI:** ES:TS:2018:1572

técnicas	
Edad del acusado	23.
Sexo del acusado	Mujer.

ID	30
Fuente	Noticias de Castilla y León[32].
Fecha	12 de mayo de 2018.
Inicio de la investigación	Desconocido.
Lugar	Madrid.
Titulo	El caso máster de Cifuentes.
Ámbito	Organización pública.
Descripción	Tras la denuncia de una de las profesoras de la URJC, donde afirma que su firma ha sido falsificada en una de las actas del tribunal en que Cifuentes, política del Partido Popular, presentó su TFM, comienza una investigación exhaustiva. Se descubren dos firmas falsificadas y varias incongruencias en diversas calificaciones y convalidaciones.
Delitos	Falsedad documental y cohecho.
Relación con la victima	Supuesta estudiante.
Finalidad	Obtención de un título universitario.
Medidas técnicas	No aceptar sobornos y contrastar todos los documentos antes de expedirlos.
Edad del acusado	54.
Sexo del acusado	Mujer.

Acceso ilícito a datos

ID	31
Fuente	Periódico Levante [33].
Fecha	6 de abril de 2018.
Inicio de la	Desconocido.

[32] https://www.noticiascyl.com/trending-topic-regional/2018/05/12/cifuentes-investigada-por-cohecho-y-falsedad-documental-por-el-caso-master/ (16 junio 2018)

[33] https://www.levante-emv.com/comunitat-valenciana/2018/04/06/alumnos-politecnica-piratean-notas-40/1700473.html (16 junio 2018)

investigación	
Lugar	Valencia.
Titulo	Uso de la técnica de keylogger en la Universitat Politécnica.
Ámbito	Organización pública.
Descripción	Mediante el uso de un keylogger físico, dos estudiantes de la Universitat Politécnica de Valencia modificaron sus notas durante dos años, convirtiendo suspensos en aprobados o sobresalientes. Para ello, piratearon las cuentas de hasta 40 profesores evitando que les llegasen los avisos de modificación de actas.
Delitos	Acceso ilícito a datos y programas informáticos, daños informáticos, descubrimiento y revelación de secretos, usurpación de estado civil y falsedad documental.
Relación con la victima	Estudiantes de la universidad.
Finalidad	Mejorar las calificaciones.
Edad del acusado	20.
Sexo del acusado	Desconocido.

ID	**32**
Fuente	Periódico El Mundo[34].
Fecha	9 de junio de 2018.
Inicio de la investigación	Desconocido.
Lugar	Madrid.
Titulo	Patricia Conde se enfrente a dos años de cárcel por revelación de secretos.
Ámbito	Divulgación de datos sensibles.
Descripción	Patricia Conde, modelo y presentadora española, ha sido acusada por revelación de secretos al extraer una serie de correos electrónicos del ordenador familiar, tras su ruptura con su ahora exmarido. Estos documentos los presentó en el juzgado de familia en un intento de conseguir la custodia de su hijo.
Delitos	Descubrimiento y revelación de secretos.
Relación con la victima	Exmujer.
Finalidad	Vengativa.
Medidas técnicas	No compartir las claves de acceso de ningún tipo de cuenta con nadie.
Edad del acusado	39.
Sexo del	Mujer.

[34] http://www.elmundo.es/loc/famosos/2018/06/09/5b1a75dce5fdea0a088b458f.html (16 junio 2018)

acusado	

ID	33
Fuente	Diario El Correo[35].
Fecha	24 de junio de 2007.
Inicio de la investigación	Desconocido.
Lugar	Valencia.
Titulo	Detenido el primer hacker en España.
Ámbito	Cracking.
Descripción	El acusado lanzó más de veinte variantes de un virus que afectaba a teléfonos de gama alta. Cuando uno de ellos se infectaba comenzaba a propagar el virus a través de bluetooth a todos los teléfonos a su alcance enviándose como mensaje multimedia a todos los números tanto de la agenda como en las listas de llamadas o mensajes. Como resultado se estiman pérdidas millonarias para las operadoras y los usuarios.
Delitos	Daños informáticos.
Relación con la victima	Desconocida.
Finalidad	Desconocida.
Medidas técnicas	No abrir mensajes sospechosos.
Edad del acusado	28.
Sexo del acusado	Hombre.

Estafas

ID	34
Fuente	Periódico 20 minutos[36].
Fecha	9 de mayo de 2018.
Inicio de la investigación	Desconocido.
Lugar	Pontevedra.
Titulo	Un hombre finge ser una mujer por más de dos años para estafar a su víctima.

[35] http://www.elcorreo.com/vizcaya/prensa/20070624/otros/joven-dana-virus-moviles_20070624.html (16 junio 2018)
[36] https://www.20minutos.es/noticia/3364024/0/hombre-canarias-estafa-36000-euros-gallego-haciendose-pasar-novia/ (16 junio 2018)

Ámbito	Redes sociales.
Descripción	Un hombre, con ayuda de su padre, se hace pasar por una mujer en una página de contactos y engaña a una persona por más de dos años. Tras pagarle en cuotas una cuantía de hasta 16000 euros, debido a la intención de subsanar una presunta deuda que posee la mujer, empieza a sospechar cuando ella le dice que está retenida en Gerona y debe darle más dinero.
Delitos	Estafa y usurpación de estado civil.
Relación con la victima	Supuestamente amorosa.
Finalidad	Monetaria.
Medidas técnicas	Asegurar por medio de videollamadas que la persona es quien dice ser.
Edad del acusado	26 y 49.
Sexo del acusado	Hombre.

ID	**35**
Fuente	Aranzadi Instituciones[37].
Fecha	10 de marzo de 2014.
Inicio de la investigación	Agosto 2012.
Lugar	Andalucía.
Titulo	Estafan la reserva de un piso en segundamano.es.
Ámbito	Compra-venta online.
Descripción	Con motivo de la reserva de un piso en alquiler en Benalmádena, un hombre le requiere a otro el pago de 105 euros. Semanas después le informa de un supuesto incendio en dicho piso por lo que le abonará la devolución de la reserva, pero este dinero nunca le es devuelto.
Delitos	Estafa, usurpación de estado civil y falsedad documental.
Relación con la victima	Vendedor.
Finalidad	Monetaria.
Medidas técnicas	Hacer uso de una compañía inmobiliaria.
Edad del acusado	Desconocida.
Sexo del acusado	Hombre.

[37] **ECLI:** ES:APSE:2014:1029

ID	36
Fuente	Aranzadi Instituciones[38].
Fecha	25 noviembre de 2013.
Inicio de la investigación	Febrero 2013.
Lugar	Madrid.
Titulo	Descubierta red de estafas a través de una empresa de envíos.
Ámbito	Compra-venta online.
Descripción	Se desmantela una red de estafas a través de la empresa "All World-Logistic" por medio de segundamano.es. Los acusados hacían uso de esta web con distintos teléfonos falsos para enviar productos a través de la empresa anteriormente citada, y que nunca alcanzaban su destino. Los distintos perjudicados se encuentran repartidos por todo el territorio nacional.
Delitos	Estafa, usurpación de estado civil, falsificación documental y blanqueo de capitales.
Relación con la victima	Supuesto vendedor.
Finalidad	Monetaria.
Medidas técnicas	Realizar las compras mediante plataformas seguras.
Edad del acusado	Desconocida.
Sexo del acusado	Hombre y mujer.

ID	37
Fuente	Aranzadi Instituciones[39].
Fecha	16 de febrero de 2017.
Inicio de la investigación	Desconocido.
Lugar	Madrid.
Titulo	Arrestada organización criminal dedicada a la estafa.
Ámbito	Compra-venta online.
Descripción	Un acusado de estafa por el precio de un alquiler de 300 euros en segundamano.es resulta ser víctima de usurpación de identidad. Investigaciones posteriores relacionan la cuenta bancaria usada para este delito con una trabajadora de una oficina bancaria. Esta persona debía ser la encargada de trasladar el dinero sustraído a distintas cuentas en el extranjero a cambio de una comisión. Se han arrestado a nueve personas que pueden estar implicadas en

[38] **ECLI:** ES:TS:2014:2832A
[39] **ECLI:** ES:TS:2017:928A

	una organización criminal dedicada a este tipo de estafas.
Delitos	Estafa, usurpación del estado civil y falsedad documental.
Relación con la victima	Supuesto vendedor.
Finalidad	Monetaria.
Medidas técnicas	Realizar las compras mediante plataformas seguras o cara a cara.
Edad del acusado	Desconocido.
Sexo del acusado	Mujer.

ID	**38**
Fuente	Aranzadi Instituciones[40].
Fecha	20 de septiembre de 2017.
Inicio de la investigación	Desconocido.
Lugar	Madrid.
Titulo	Acusado de estafa es víctima de usurpación de identidad tras una estafa anterior.
Ámbito	Compra-venta online.
Descripción	Tras la denuncia de estafa interpuesta tras la compra de un móvil por valor de 210 euros que no llega a recibirse, el acusado resulta ser víctima, a su vez, de un delito de usurpación de identidad acontecido tras una estafa de distinta índole que sufrió a través de la entidad "Todoverbenas".
Delitos	Estafa y usurpación del estado civil.
Relación con la victima	Supuesto vendedor.
Finalidad	Monetaria.
Medidas técnicas	Realizar las compras mediante plataformas seguras o cara a cara.
Edad del acusado	Desconocida.
Sexo del acusado	Hombre.

ID	**39**
Fuente	Aranzadi Instituciones[41].
Fecha	20 de junio de 2017.
Inicio de la	Desconocido.

[40] **ECLI:** ES:TS:2017:9201A
[41] **ECLI:** ES:APB:2017:5499A

investigación	
Lugar	Barcelona.
Titulo	Delincuente pide un préstamo con los datos de una cartera robada.
Ámbito	Falsedad documental.
Descripción	Tras el robo del móvil y la cartera de la víctima en Madrid, se abre días después una cuenta bancaria a su nombre en Barcelona haciendo uso de esos datos. El fin para el que esto es realizado es la petición de un préstamo vía internet de 300 euros.
Delitos	Estafa, usurpación del estado civil y falsedad documental.
Relación con la victima	Desconocida.
Finalidad	Monetaria.
Medidas técnicas	Denunciar los robos sin demora y cancelar todas las tarjetas bancarias que puedan haberse sustraído.
Edad del acusado	Desconocida.
Sexo del acusado	Hombre.

ID	**40**
Fuente	Periódico Castellón Diario[42].
Fecha	18 de octubre de 2017.
Inicio de la investigación	Desconocido.
Lugar	Comunidad Valenciana.
Titulo	Destapan una trama de estafas de telefonía móvil en el territorio nacional.
Ámbito	Compra-venta online.
Descripción	La policía detiene a un repartidor de teléfonos móviles e identifica a otras seis personas por formar parte de una red de estafas. Los delincuentes usaban datos personales de terceras personas para contratar teléfonos móviles de alta gama sin el consentimiento de los titulares. Después los trasladaban a Rumanía desde donde los vendían a todo el mundo. Además, descubrieron que los repartidores de las empresas eran sobornados para poder cometer estas acciones.
Delitos	Estafa, usurpación de estado civil, relevación de secretos y falsedad documental.
Relación con la victima	Desconocida.
Finalidad	Monetaria.
Medidas	No acceder a sobornos y denunciar las acciones ilegales.

[42] http://castellondiario.com/not/65148/la-guardia-civil-detiene-a-una-persona-e-identifica-a-otras-seis-por-numerosos-delitos-de-estafa-usurpacion-de-estado-civil-relevacion-de-secretos-falsedad-documental-en-vall-de-uxo- (16 junio 2018)

técnicas	
Edad del acusado	Desconocida.
Sexo del acusado	Desconocido.

ID	41
Fuente	Aranzadi Instituciones[43].
Fecha	23 de mayo de 2013.
Inicio de la investigación	Junio 2012.
Lugar	Madrid.
Titulo	Un hombre realiza una estafa al simular vender su coche para comprarse una moto.
Ámbito	Compra-venta online.
Descripción	Tras abonar 200 euros en concepto de fianza por la compra de un coche, dando su nómina, cuenta bancaria y otros datos personales a fin de llevar a cabo la transacción, el vendedor no aparece. Más tarde una entidad bancaria llama al denunciante para comunicarle la aprobación de un préstamo a su nombre para una moto que no había solicitado.
Delitos	Usurpación del estado civil y estafa.
Relación con la victima	Supuesto vendedor.
Finalidad	Monetaria.
Medidas técnicas	Realizar las compras mediante plataformas seguras o cara a cara.
Edad del acusado	Desconocida.
Sexo del acusado	Hombre.

ID	42
Fuente	Wired[44].
Fecha	23 de de abril de 2018.
Inicio de la investigación	Desconocido.
Lugar	Atlanta.
Titulo	El ramsomware SamSam ataca Atlanta.

[43] **ECLI:** ES:TS:2013:5150A
[44] https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/ (16 junio 2018)

Ámbito	Cracking.
Descripción	El ataque de ransomware SamSam a Atlanta causó la desconexión o parcial inhabilitación de más de un tercio de los 424 programas de software utilizados por la ciudad. El 30% de ellos de gran importancia por afectar a servicios básicos de la ciudad, incluidos la policía y los tribunales. Atlanta no llegó a pagar el rescate de 52.000 dólares en bitcoins, por lo que no han podido salvar ninguno de los datos capturados.
Delitos	Estafa, daños informáticos, blanqueo de capitales y organización criminal.
Relación con la victima	Desconocida.
Finalidad	Monetaria.
Medidas técnicas	Asegurarse de tener todo el software actualizado y realizar backups periódicas.
Edad del acusado	Desconocida.
Sexo del acusado	Desconocido.

ID	**43**
Fuente	Diario El Correo[45].
Fecha	21 de mayo de 2013.
Inicio de la investigación	Desconocido.
Lugar	Europa.
Titulo	Estafan 750.000 euros usando tarjetas clonadas.
Ámbito	Phising.
Descripción	La Policía Nacional ha detenido a siete personas por fraude en internet y a la madre de uno de ellos, de 82 años, por encargarse de enviar al extranjero el dinero estafado. Los miembros de la red compraban en internet productos electrónicos de alta gama, con tarjetas de crédito clonadas obtenidas mediante phishing o pharming, y posteriormente los vendían en páginas de compraventa para enviar los productos a otros países.
Delitos	Falsedad documental, blanqueo de capitales, pertenencia a organización criminal, estafa y alzamiento de bienes.
Relación con la victima	Desconocida.
Finalidad	Monetaria.
Medidas técnicas	No compartir tus datos personales o bancarios con organizaciones por correo electrónico.

[45] http://www.elcorreo.com/vizcaya/rc/20130521/sociedad/tarjetas-clonadas-201305211154.html (16 junio 2018)

Edad del acusado	Desconocida.
Sexo del acusado	Desconocido.

ID	44
Fuente	El Correo Digital[46].
Fecha	11 de julio de 2006.
Inicio de la investigación	Desconocido.
Lugar	Vizcaya.
Titulo	Estafan casi 30.000 euros a un colegio del Getxo.
Ámbito	Phising.
Descripción	Detienen a un hombre por abrir cuatro cuentas corrientes distintas en Sevilla a donde iba a parar el dinero estafado a un colegio de Vizcaya. Para lograr los traspasos de dinero se instaló un troyano a través de un correo que robaba las claves de acceso y las mandaba a Estonia. Desde allí o desde Estados Unidos se realizaban las trasferencias al banco de Sevilla. Todavía se investiga quien puede estar a cargo de la operación.
Delitos	Estafa, falsedad documental y usurpación del estado civil.
Relación con la victima	Desconocida.
Finalidad	Monetaria.
Medidas técnicas	No abrir correos sospechosos.
Edad del acusado	30.
Sexo del acusado	Hombre.

ID	45
Fuente	Diario El Correo[47].
Fecha	23 de abril de 2010.
Inicio de la investigación	Desconocido.
Lugar	Vitoria.

[46] https://inza.wordpress.com/2006/07/11/condenado-por-un-caso-de-phishing-pharming-troyano/ (16 junio 2018)

[47] http://www.elcorreo.com/alava/20100423/local/estafan-euros-mediante-transferencias-201004231042.html (16 junio 2018)

Titulo	Detenidos dos intermediarios en una estafa de 27.000 euros.
Ámbito	Phising.
Descripción	Agentes de la Ertzaintza detiene a dos sospechosos de transferir dinero robado por medio de técnicas de phising y pharming a distintos particulares. Los detenidos fueron captados por una oferta de trabajo en la que mandarían el dinero a supuestas ONGs a cambio de un porcentaje.
Delitos	Estafa, falsedad documental y usurpación del estado civil.
Relación con la victima	Desconocida.
Finalidad	Monetaria.
Medidas técnicas	No compartir tus datos personales o bancarios con organizaciones por correo electrónico.
Edad del acusado	41 y 22.
Sexo del acusado	Hombre.

11. Guías de ayuda

A continuación, se muestran dos guías relacionadas con la suplantación de identidad. La primer de ellas ofrece consejos sobre cómo evitar, en la medida de lo posible, que los posibles delincuentes accedan a nuestros datos de manera sencilla.

Por otra parte, la segunda guía, muestra cómo actuar en el caso de que el delito ya se haya llevado a cabo. Ofrece, por tanto, una serie de enlaces de interés y consejos para propiciar que la usurpación de identidad dure el menor tiempo posible.

Guía de prevención

1. **No distribuyas información sensible.**

Datos personales, así como bancarios, contraseñas, etc. pueden resultar de riesgo si llegan a malas manos. Por ello es necesario tener mucho cuidado con donde se ingresan los datos y a quienes se les da a conocer.

2. **Evita ingresar datos bancarios en páginas web que no posean un protocolo seguro (https).**

El protocolo https cifra tu información protegiéndola de posibles atacantes. Debido a esto las páginas que cuenten con este protocolo son más confiables.

3. **No compartas cosas de las que puedas arrepentirte después.**

No publiques ni compartas imágenes o textos que no puedan ser aptas para todo el mundo. Piensa en que pasaría si llegasen a la vista de familia, trabajo u otros amigos y actúa en consecuencia.

4. **Usa contraseñas seguras.**

Es importante utilizar contraseñas que no estén demasiado relacionas contigo para que sean más difíciles de revelar. También es buena idea usar números, letras capitales y una longitud mínima de 6 caracteres.

5. **Mantén el antivirus actualizado y realiza análisis periódicamente.**

Tanto el antivirus como cualquier otro software instalado en un ordenador debe permanecer constantemente actualizado. De este modo, las posibles brechas de seguridad que hayan detectado las compañías pueden ser subsanadas en el menor tiempo posible.

6. **Bloquea el móvil o el ordenador cada vez que vayas a dejarlo sin vigilancia.**

Sin importar el período de tiempo que vaya a quedar desprotegido, cinco minutos o una hora, debe evitarse que otras personas puedan tener acceso a cualquier tipo de dispositivo.

7. **Cuidado con las redes wifi abiertas.**

El administrador y otras personas que usen esa red podrían acceder a nuestra información haciendo uso de ciertas técnicas. Si aun así debes conectarte a este tipo de red no te registres en ningún sitio haciendo uso de usuario y contraseña y elimina los datos almacenados después de desconectarte.

8. **Lee las condiciones de uso y privacidad de los servicios que uses en internet.**

Estas condiciones son un contrato que firmamos con las compañías por lo que es importante conocer que les estamos cediendo. Algunas de estas condiciones explican quién tiene la autoría de los datos y que puede pasar con ellos después, por lo que es bueno conocerlo para saber actuar en consecuencia.

9. **Tritura bien todos los documentos con información sensible.**

Algunas facturas o cartas que recibas pueden contener datos sensibles que, de no ser eliminados debidamente, pueden caer en manos de personas equivocadas.

10. **Descarga programas y ficheros solo de sitios confiables.**

Distintos tipos de malware pueden ocultarse en los archivos por lo que es mejor alejarse de webs desconocidas y que puedan transmitir desconfianza. En cualquier caso, realiza un análisis con el antivirus antes de abrir estos archivos.

11. **Desconfía de las cosas gratis.**

Envíos de regalos gratuitos a cambio de ciertos datos, ofertas de trabajo demasiado buenas o cupones son sólo algunos ejemplos de lo que los ciberdelincuentes pueden utilizar para captar tus datos y usarlos contra ti.

Guía de actuación

1. **Reúne pruebas.**

   Antes de realizar acciones para que se elimine el contenido asegúrate de tener pruebas de su existencia. Una simple captura de pantalla o el historial de mensajes puede ser de mucha ayuda en procesos posteriores.

2. **Denuncia en la propia red social.**

Cada red social posee en su centro de ayuda la opción de denunciar una suplantación de identidad, como es el caso de las siguientes:

- Twitter: https://help.twitter.com/forms/impersonation
- Facebook: https://www.facebook.com/help/contact/295309487309948?helpref=faq_content
- Google+: https://support.google.com/plus/troubleshooter/1715140?hl=es
- Linkedln: https://www.linkedin.com/help/linkedin/answer/30432?lang=es
- Instagram: https://help.instagram.com/446663175382270/

3. **Denuncia ante las autoridades.**

Si el problema persiste no te limites a denunciar una y otra vez a la red social ya que posiblemente se trate de un caso de acoso. Acude a la policía y presenta una denuncia formal del caso para que puedan empezar a investigarlo.

4. **Sigue las indicaciones de las fuerzas de seguridad**

Si ya hemos acudido a poner la denuncia las autoridades deben haberte orientado de qué hacer a continuación. Sigue sus indicaciones y orientaciones para no interferir en la investigación.

12. Conclusiones

La elaboración de este trabajo me ha permitido ser más consciente sobre la realidad del mundo en que vivimos, así como de la importancia que pueden tener nuestros datos y el protegerlos.

A través de la realización de este estudio se ha podido explorar la suplantación de identidad, y realizar varias guías a fin de combatirla. Todo ello, junto con la ayuda de una recopilación de casos reales, ha servido para alcanzar las siguientes conclusiones:

1. La suplantación de identidad, además de ser un ciberdelito, suele ser utilizada como medio para conseguir realizar otros, tales como estafas o ciberacosos, por ello es tan importante proteger los datos.

2. Con el avance de las tecnologías ha sido preciso una actualización en las leyes para hacer frente a la nueva tipología de delitos. Los nuevos reglamentos y directivas forman una base sobre la que esto puede llevarse a cabo.

3. La información debe ser tratada como si pudiese volverse pública en cualquier momento, de esta manera se pueden evitar posibles extorsiones o chantajes en un futuro.

4. Es importante realizar un mayor y más profundo estudio sobre el alcance del ciberacoso y sus consecuencias, así como la identificación de sus causas para poder identificarlo antes, tanto en menores como en jóvenes y adultos.

5. Se debe mejorar la educación emocional y relacional desde la infancia, de modo que las personas puedan comprender lo más pronto posible, las consecuencias que puede tener para los demás los distintos tipos de acoso a los que se les puede someter.

6. La asistencia a talleres, conferencias y eventos de concienciación son fundamentales para visibilizar el problema de ciberseguridad y tomar medidas contra él. Aprender a manejar datos de manera segura, a no dar nuestra información libremente o a saber cuándo tratar o no con las personas a través de las pantallas son factores clave para asegurar nuestra protección y la de los demás.

7. Realizar búsquedas periódicas de nosotros mismos en Internet o nuestras imágenes puede ser un buen método de asegurarse de que nuestra información sigua a buen recaudo.

8. Los procesos de denuncia pueden ser largos y costosos, por lo que conseguir la mayor recopilación de pruebas, hacer caso de las autoridades e intentar mantener un buen estado de ánimo es primordial.

Sería interesante, para futuras líneas de investigación, analizar cómo ha afectado la instauración del nuevo reglamento de protección de datos a las empresas. Asimismo, se podrían recopilar nuevas noticias, contrastando las anteriores, para comprobar si las penas han variado o si hay un mayor número de condenas. También se podría crear una campaña contra la suplantación de identidad y efectuar un seguimiento de la misma. Además, podría realizarse una encuesta o herramienta para analizar los conocimientos de las personas sobre la seguridad de sus datos.

13. Bibliografía

Ciberdelitos

- **20 minutos**. *El enlace que te roba la cuenta de Facebook.* 2018A. Web. 17 mayo 2018.
- **Avast** (2018). *Qué es el malware.* 2018. Web. 17 mayo 2018.
- **Casabona**, **Romeo**. "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal". *Dialnet*, p. 1-43. Web. 17 mayo 2018.
- **CERT-PY.** *¿Qué son los rootkits?.* 2018. Web. 17 mayo 2018.
- ***Estudio del universo** digital de EMC con investigación y análisis por IDC*. Dellemc. 2014. Web. 10 junio 2018.
- **Interpol**. *Global Cybercrime Strategy. 2017*. Web. 17 mayo 2018.
- **Kaspersky Lab**. *¿Qué es el pharming?.* 2018. Web. 17 mayo 2018.
- **Martínez Nadal, A. & Alcover Garau, G.** *Comercio Electrónico, Firma Digital Y Autoridades De Certificación.* Civitas. 1998. Web. 17 mayo 2018.
- **Ministerio del Interior**. *Estudio sobre la cibercriminalidad en España.* 2016. Web. 17 mayo 2018.
- **Oficina de Seguridad del internauta**. *Aprendiendo a identificar los 10 phishing más utilizados por ciberdelincuentes.* 2014. Web. 17 mayo 2018.
- **Oficina de Seguridad del internauta**. *Phishing al Banco Santander*. 2018A. Web. 17 mayo 2018.
- **Pantallas amigas**. *Protección de la infancia*. 2018. Web. 17 mayo 2018.
- **Ramos Varón, Antonio**. *Hacking con ingeniería Social: Técnicas para hackear humanos*. Ra-Ma. 2015. Web. 17 mayo 2018.
- **Thomson Reuters**. *Aranzadi Instituciones.* 2018. Web. 17 mayo 2018.

Legislación

- **Agencia Española de Protección de Datos**. *Consultas más frecuentes*. 2018C. Web. 28 mayo 2018.
- **Agencia Española de Protección de Datos**. *Ejercicio del derecho de supresión.* 2018B. Web. 28 mayo 2018.
- **Agencia Estatal Boletín del Estado.** *Constitución Española.* 1978. Web. 28 mayo 2018.
- **Agencia Estatal Boletín del Estado**. *Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia.* 2015. Web. 28 mayo 2018.

- **Agencia Estatal Boletín del Estado**. *Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil*. 1996. Web. 28 mayo 2018.
- **Agencia Estatal Boletín del Estado**. *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.* 1995. Web. 28 mayo 2018.
- **Agencia Estatal Boletín del Estado**. *Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.* 2000. Web. 28 mayo 2018.
- **Agencia Estatal Boletín del Estado**. *Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil*. 1889. Web. 28 mayo 2018.
- **Diario Oficial de la Unión Europea**. *Carta de los derechos fundamentales de la Unión Europea*. 2000. Web. 28 mayo 2018.
- **Diario Oficial de la Unión Europea**. *Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo*. 2016A. Web. 28 mayo 2018.
- **Diario Oficial de la Unión Europea**. *UE Reglamento general de protección de datos*. 2016B. Web. 28 mayo 2018.
- **EU General Data Protection Regulation**. *GDPR Portal: Site Overview*. 2018. Web. 28 mayo 2018.
- **Naciones Unidas**. *La Declaración Universal de Derechos Humanos. 2018. Web.* 28 mayo 2018.

Ciberacoso

- **"Netiqueta:** normas de buen uso de Internet". *Anales de mecánica y electricidad*. 6 (2012): 56-57. Web. 28 mayo 2018.
- **Pachés, Fernando de** Vicente. "El ciberacoso: un fenómeno de violencia emergente en el ámbito de las relaciones de trabajo". *Dialnet*. 2 (2017): 99-120. Web. 28 mayo 2018.

Guías

- **Agencia Española de Protección de Datos**. *Adaptación al RGPD – Sector Privado*. 2018E. Web. 28 mayo 2018.
- **Agencia Española de Protección de Datos**. *Facilita RGPD.* 2018D. Web. 28 mayo 2018.
- **Agencia Española de Protección de Datos**. *Guía del Reglamento General de Protección de Datos para responsables de tratamiento.* 2018A. Web. 28 mayo 2018.
- **Agencia Española de Protección de Datos**. *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*. 2018G. Web. 28 mayo 2018.

- **Agencia Española de Protección de Datos**. *Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD*. 2018F. Web. 28 mayo 2018.
- **Universitat de Valencia**. *Preguntas frecuentes sobre la protección de datos.* 2018. Web. 28 mayo 2018.

Visualización

- **Centro de Ciberseguridad Industrial.** *Primera jornada de Seguridad en Hospitales 4.0 el 10 de julio.* 2018. Web. 10 junio 2018.
- **Hackron.** *¿#Hackron & #Hackronlabs?.* 2018. Web. 10 junio 2018.
- ***Identity Thief.*** Dir. Seth Gordon. Act. Jason Bateman, Melissa McCarthy y John Cho. Star Thrower Universal Pictures / Aggregate Films. 2013 (Fílmico).
- ***Ingrid Goes West.*** Dir. Matt Spicer. Act. Aubrey Plaza, Elizabeth Olsen, O'Shea Jackson Jr. y Wyatt Russell. Star Thrower Entertainment / 141 Entertainment / Mighty Engine. 2017 (Fílmico).
- **Instituto Nacional de Ciberseguridad.** *Hackend: Se acabó el juego.* Google Play. 20 dic. 2016A. Web. 10 junio 2018.
- **Instituto Nacional de Ciberseguridad**. *Hackers vs. Cybercrook.* Google Play. 30 nov. 2016B. Web. 10 junio 2018.
- **Instituto Nacional de Ciberseguridad.** *Herramienta de Autodiagnóstico: Conoce tus riesgos en cinco minutos.* 2018A. Web. 10 junio 2018.
- **Instituto Nacional de Ciberseguridad.** *Juego de rol: ¿Estás preparado para ser atacado?.* 2018. Web. 10 junio 2018.
- **Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.** *Vulnerómetro: evita riesgos a tu identidad.* 2018. Web. 10 junio 2018.
- **Jané, Carmen.** *Las aseguradoras entran a proteger a los menores del ciberacoso*. El Periódico de Catalunya. 16 oct. 2017. Web. 10 junio 2018.
- **La Rioja.** *Campaña de concienciación de los jóvenes en las redes sociales.* 1 febrero 2018. Web. 10 junio 2018.
- **La Sexta TV**. *Cazadores de trolls: Contra el acoso en internet*. 2018. Web. 6 junio 2018.
- **Legálitas Abogados**. "Sé un héroe contra el ciberbullying". *YouTube.* 23 noviembre 2016. Web. 6 junio 2018.
- **Movistar España**. "MOVISTAR: Love Story, por un internet seguro". *YouTube.* 5 febrero 2018. Web. 6 junio 2018.
- **MTV**. *Catfish: the tv show.* 2017. Web. 6 junio 2018.
- **Noticiascyl.** *Es.pabila e Incibe organizan conferencias sobre seguridad en las redes.* 10 mayo 2018. Web. 10 junio 2018.
- **Oficina de Seguridad del Internauta.** *CONAN mobile.* 2018C. Web. 10 junio 2018.

- **Oficina de Seguridad del Internauta.** *Servicio AntiBotnet.* 2018B. Web. 10 junio 2018.
- **UNICEF Comité Español**. "¿Eres tan anónimo en la Red como te crees? #NoSeasEstrella". *YouTube.* 6 febrero 2017. Web. 6 junio 2018.
- **ViveInternet_es_Gobierno_de_Canarias**. "Campaña #noseasanimal". *YouTube.* 12 junio 2015. Web. 6 junio 2018.
- **ViveInternet_es_Gobierno_de_Canarias**. "Campaña #OjitoconlaRed". *YouTube.* 11 agosto 2017. Web. 6 junio 2018.
- **ViveInternet_es_Gobierno_de_Canarias**. "Campaña #TICconcabeza". *YouTube.* 19 octubre 2016. Web. 6 junio 2018.

Recopilación de casos

- **20 minutos.** *Detienen a una universitaria por suplantar a una compañera para examinarse por Internet.* 31 oct. 2013. Web. 16 junio 2018.
- **Almoguera, Pablo.** *Los estudiantes detenidos por «ciberbullying» acosaban a una compañera con anorexia.* Diario ABC. 14 mayo 2013. Web. 16 junio 2018.
- **Cabanes, Ignacio.** *Dos alumnos de la Politècnica piratean las notas de 40 profesores durante dos años.* Levante-EMV. 6 abril 2018. Web. 16 junio 2018.
- **Cañas, Jesús**. *Detenido por acosar a una menor a través de las redes sociales en Algeciras.* El País. 13 feb. 2017. Web. 16 junio 2018.
- **Castellón Diario.** *La Guardia Civil detiene a una persona e identifica a otras seis por numerosos delitos de estafa, usurpación de estado civil, relevación de secretos, falsedad documental en Vall de Uxó.* 18 oct. 2017. Web. 16 junio 2018.
- **Centro criptológico nacional.** *Detenido en Alicante el líder del grupo cibercriminal que está detrás de "Carbanak" y "Cobalt".* 26 marzo 2018. Web. 16 junio 2018.
- **Diario El Correo.** *Cae una red que estafó 750.000 euros en Internet con tarjetas clonadas.* 21 mayo 2013. Web. 16 junio 2018.
- **Diario El Correo.** *Un joven daña con un virus 115.000 móviles y provoca daños millonarios a las operadoras.* 24 junio 2007. Web. 16 junio 2018.
- **El Norte de Castilla.** *Suplantan la identidad en Facebook de Silvia Abascal*. 1 enero 2018. Web. 16 junio 2018.
- **El País.** *Chris Pratt denuncia que un "pervertido" le suplanta en Facebook*. 4 dic. 2017. Web. 16 junio 2018.
- **El País.** *Detenidos tres menores por difundir fotos íntimas de una compañera de 14 años.* 2 marzo 2017. Web. 16 junio 2018.
- **Europa Press.** *Detenido en Burgos por utilizar la identidad de un familiar fallecido para vender 9.300 kilos de cobre.* 30 nov. 2016. Web. 16 junio 2018.
- **Europa Press.** *Detenidos dos aspirantes al examen del permiso de conducción por suplantar la identidad de otras personas*. 2 feb. 2018. Web. 16 junio 2018.

- **Europa Press**. *Un hombre de Canarias estafa 36.000 euros a un gallego haciéndose pasar por su novia.* 20 minutos. 9 junio 2018. Web. 16 junio 2018.
- **Hay Newman, Lily.** *Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare.* Wired. 23 abril 2018. Web. 16 junio 2018.
- **Instituto Nacional de Ciberseguridad.** *Campaña de phishing suplantando al Banco Sabadell.* 5 sept. 2017. Web. 16 junio 2018.
- **Inza, Julián.** *Condenado por un caso de phishing, pharming, troyano.* Todo es electrónico. 2006. Web. 16 junio 2018.
- **La opinión de Murcia.** *Detenido por suplantar la identidad de otra persona en un examen de conducir*. 25 enero 2018. Web. 16 junio 2018.
- **La Opinión de Zamora.** *La red rumana del fraude a Benavente estafa millones en varios ayuntamientos del país.* 5 nov. 2017. Web. 16 junio 2018.
- **La República**. *Neymar denuncia suplantación de identidad en Instagram*. 28 nov. 2017. Web. 16 junio 2018.
- **La Vanguardia.** *Belén Esteban denuncia que le han suplantado la identidad en Facebook.* 22 marzo 2017. Web. 16 junio 2018.
- **La Vanguardia.** *Dos detenidos por suplantación de identidad en el examen del carné conducir.* 21 marzo 2017. Web. 16 junio 2018.
- **Miranda, Beatriz.** *La Fiscalía pide dos años y medio de cárcel para Patricia Conde por revelación de secretos.* El Mundo. 9 junio 2018. Web. 16 junio 2018.
- **Noticiascyl.** *Cifuentes, investigada por cohecho y falsedad documental por el 'Caso Máster'.* 12 mayo 2018. Web. 16 junio 2018.
- **Noticiascyl.** *Tres detenidos en Ávila y Soria por suplantar identidades.* 9 mayo 2018. Web. 16 junio 2018.
- **Oficina de Seguridad del Internauta.** *Nuevo phishing a Apple: Quieren robarte datos personales y bancarios.* 24 marzo 2017. Web. 16 junio 2018.
- **Univisión.** *'Porno venganza': su ex difundió videos y fotos íntimas y ahora la justicia la indemniza con 6.45 millones.* 10 abril 2018. Web. 16 junio 2018.
- **Vasco Press.** *Estafan 8.500 euros mediante transferencias bancarias ilegales.* Diario El Correo. 23 abril 2010. Web. 16 junio 2018.
- **Wallace, Kelly.** *Police file raises questions about bullying in Rebecca Sedwick's suicide.* CNN. 21 abril 2014. Web. 16 junio 2018.