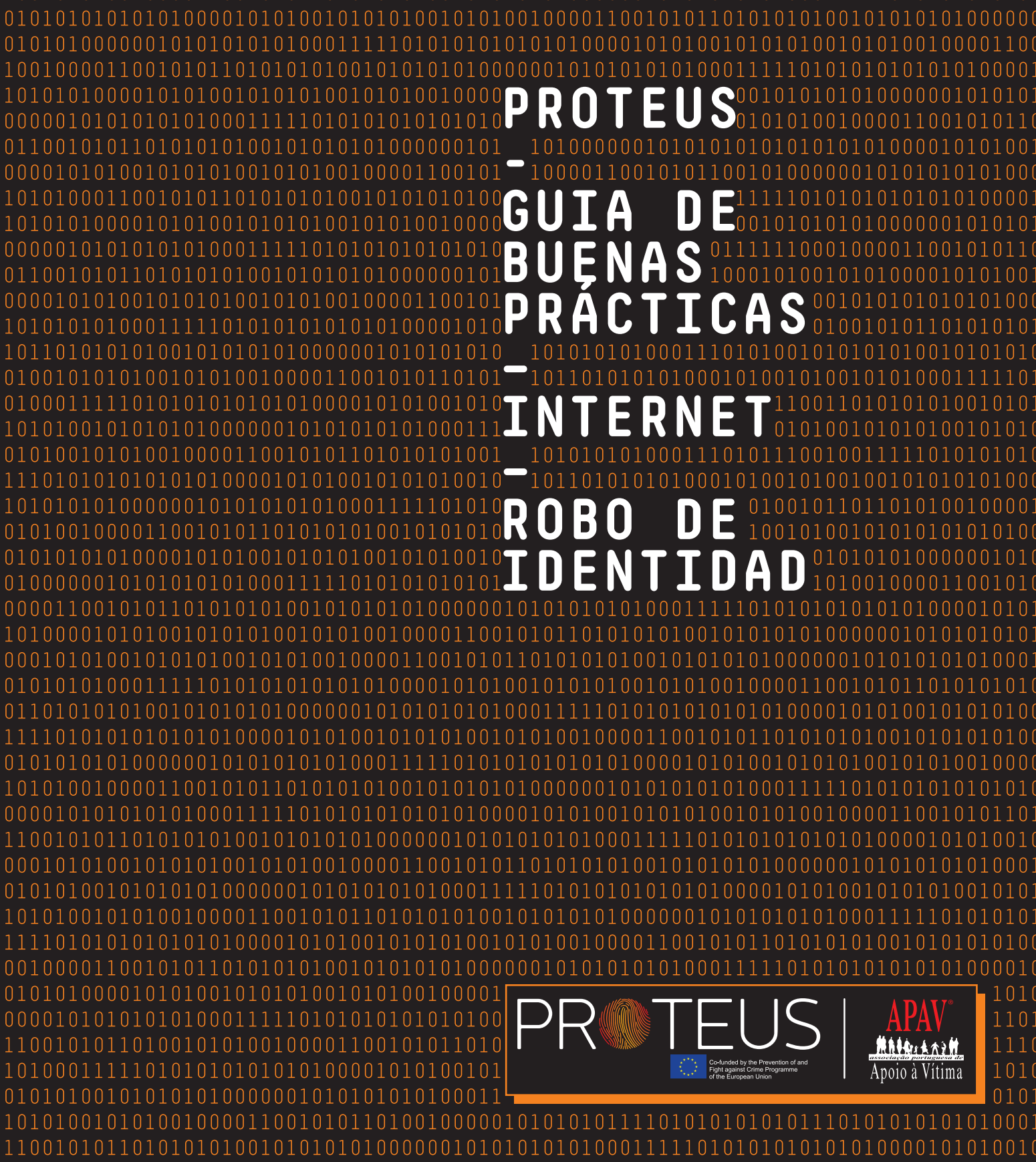




PROTEUS

GUIA DE
BUENAS
PRÁCTICAS

INTERNET

ROBO DE
IDENTIDAD

PROTEUS



Co-funded by the Prevention and
Fight against Crime Programme
of the European Union

APAV®



Associação Portuguesa de
Apoio à Vítima

[illegible]

ISBN	Depósito Legal
978-972-8852-71-9	

Teléfono	Fax
+351 21 358 79 00	+351 21 887 63 51

Título
Proteus - Guia de Buenas Prácticas - Internet -
Robo de Identidad

E-mail	Sitio
apav.sede@apav.pt	www.apav.pt

Autor
2015 © APAV
Associação Portuguesa de Apoio à Vítima

APAV
Rua José Estevão, 135 - A
1150-201 Lisboa
Portugal

INDICE

INTRODUCCIÓN

5

1.CASOS DE ESTUDIO

9

< Caso 1 >

11

< Caso 2 >

11

< Caso 3 >

12

< Caso 4 >

12

< Caso 5 >

12

< Caso 6 >

13

< Caso 7 >

13

< Caso 8 >

13

< Caso 9 >

14

< Caso 10 >

14

2.ENMARCADO - ROBO DE IDENTIDAD

15

2.1. Ciberdelincuencia

17

2.1.1. Globalización

17

2.1.2. Definicion de Ciberdelincuencia

17

2.2. Robo de identidad

19

2.2.1. Dificultad terminológica

19

2.2.2. Definiciones

20

2.3. Modi operandi

21

3.ROBO DE IDENTIDAD - LA REALIDAD

27

3.1. Las situaciones más comunes relacionadas con el Robo de identidad en internet

29

3.2. El delincuente y la víctima

30

3.3. Factores de riesgo

32

3.4. Impacto del robo de identidad

33

3.4.1. En la víctima

33

a. ECONÓMICO

33

b. LEGAL

34

c. EMOCIONAL

35

d. IMPACTO EN LA VIDA DIARIA

36

3.4.2. En la sociedad

36

3.5. Dificultades en la investigación

37

4.MARCO LEGAL

39

4.1. Marco Internacional

41

4.2. Ley Española

42

4.3. El robo de identidad, el derecho nacional y el Convenio sobre la Ciberdelincuencia

53

5.LEY NACIONAL APLICABLE A LOS CASOS DE ESTUDIO

55

< Caso 1 >

57

< Caso 2 >

57

< Caso 3 >

57

< Caso 4 >

57

< Caso 5 >

58

< Caso 6 >

58

< Caso 7 >

58

< Caso 8 >

58

< Caso 9 >

58

< Caso 10 >

59

6. PREVENCIÓN

61

6.1. Medidas de Prevención

63

6.2. Signos de infección de Malware

69

6.3. Como identificar los signos de Robo de identidad

69

7.AYUDA A LAS VICTIMAS

71

7.1. Infección por malware

73

7.2. Robo de Identidad

73

ANEXOS

77

Glosario

79

Números de ayuda al usuario y contacto de las entidades Bancarias en España

81

3

INTRODUCCIÓN

[illegible]

INTRODUCCIÓN

Un estudio realizado en el año 2013 entre 13.022 adultos, de edades comprendidas entre los 18 y los 64 años, en 24 países diferentes, revela que se producen 378 millones de víctimas de la Ciberdelincuencia cada año, un millón de víctimas al día y 12 víctimas por segundo¹.

El porcentaje de población víctima de fraudes por Robo de identidad online a través del acceso al correo electrónico no autorizado, varía entre 1% y 17 % en 21 países del mundo, mientras que esta misma población, son víctimas de robos comunes entre el 1% y el 5% en los mismos países².

Las víctimas se encuentran en una posición de especial fragilidad e indefensión en lo que respecta a delitos Cibernéticos. Debido a su naturaleza reciente, la Ciberdelincuencia está todavía poco valorada y entendida por la población en general, y sus efectos también se han subestimado tanto en la definición como en la aplicación de medidas para luchar contra estos delitos por las autoridades responsables.

Los casos de robo de identidad online pueden ser muy complejos, por lo que las víctimas suelen necesitar asistencia personalizada para ayudarles a reconstruir su equilibrio. Con frecuencia las víctimas del Cibercrimen necesitarán ayuda para trabajar con medios electrónicos que quizás no dominan.

El impacto del Cibercrimen y el robo de identidad llevado a cabo a través de internet en particular, crece de día en día y con él también lo hacen el número de víctimas que denuncian a la policía en busca de ayuda, por lo cual es necesario mejorar la respuesta y el apoyo que se preste a las víctimas.

En este contexto, nace la necesidad de elaborar esta guía, que centrándose específicamente en el Robo de identidad a través de Internet, tiene como objetivo preparar a los trabajadores de los servicios de ayuda a las víctimas y otros profesionales para conocer y comprender este fenómeno y para informar y ayudar a las víctimas de delitos a emprender las mejores medidas contra la ciberdelincuencia.

1 Informe sobre el Cibercrimen Norton 2013.

2 Oficina de Naciones Unidas para la lucha contra la droga y delincuencia, Estudio integral sobre la Ciberdelincuencia - proyecto de Febrero 2013, p. 3.

1.

CASOS DE ESTUDIO

[illegible]

1. CASOS DE ESTUDIO

< Caso 1 >

Josué es un empleado de banca que conoce los datos de acceso con los que opera Joaquim (un cliente) en su cuenta a través de internet. Josué vende sus datos a una organización criminal, la cual accede a la cuenta de Joaquim y realiza una transferencia de 6000€ a una cuenta desconocida.

< Caso 2 >

Joana se considera una persona informada sobre la ciberseguridad y toma precauciones para proteger su equipo.

Un día Joana, impresionada por lo que había leído en la prensa que ofrecen en el metro de su ciudad, sobre el aumento de la ciberdelincuencia en España, decidió investigar sobre el mejor antivirus disponible en el mercado, para instalarlo en su ordenador personal. Para ello utiliza uno de los buscadores más populares y encontró entre muchas páginas, una página extraña, que le proponía la instalación de un potente antivirus, el cual ella eligió no instalar, ya que ella había sido advertida de que sólo acepte la transferencia de información de fuentes fiables. Esa misma noche, Joana realizó algunos pagos a través de la página web de su banco.

Una semana después, Joana consulto los movimientos de su cuenta y se dio cuenta de que había desaparecido una cantidad considerable de dinero.

Esto puede haber sido suficiente para abrir una página web de malware que se ha instalado en su ordenador. En este caso un programa de keylogging se ha instalado en el ordenador de Joana. Esto permitió al delincuente grabar todos los datos introducidos desde el teclado de Joana, incluyendo sus contraseñas para acceder a la web de su banco.

1. CASOS DE ESTUDIO

< Caso 3 >

Jandira y sus hijos usan el ordenador para hacer búsquedas en internet y enviar correos electrónicos.

Sin embargo, desde hace un mes el ordenador de Jandira va muy lento, tan lento que Jandira y sus hijos han renunciado a usarlo. El lunes pasado Jandira recibió un email firmado por ReidosHackers, unos piratas informáticos que le dicen a Jandira que tienen el control de su ordenador y le piden 600€ para devolverle de nuevo el control, para que pueda usarlo de manera normal.

< Caso 4 >

A Josefina le gusta mucho intercambiar correos electrónicos con sus amigos y familiares, entre ellos algunos que habían emigrado a Francia. Un día, mientras comprueba si ha recibido la respuesta al correo que envió a su primo Jean Pierre, encuentra un correo de su banco pidiéndole que haga clic en un enlace y posteriormente que confirme sus datos mediante la cumplimentación de un formulario. Josefina fue a buscar sus documentos e hizo lo que se le pedía de inmediato.

Un mes más tarde, el Gerente de su banco contactó con Josefina porque estaba preocupado y quería preguntarle porque había transferido la mayor parte de sus ahorros a una cuenta para él desconocida, quería aclarar sus dudas con el cliente.

< Caso 5 >

José recibió un email que provenía de una cadena de spam, que aparentemente venía de su servidor de correo electrónico, pidiéndole que actualice su contraseña.

Después de esto, a José le preguntaron algunos de sus compañeros de trabajo y amigos, acerca de algunos mensajes de correo electrónico que habían estado recibiendo remitidos desde la dirección de correo electrónico de José, en los cuales se les estaba pidiendo ayuda financiera.

1. CASOS DE ESTUDIO

< Caso 6 >

Joel y Jessica salieron durante 6 meses y después de este tiempo Jessica dejó a Joel.

Joel muy furioso, le juró venganza y Jessica no le dió importancia. Un día, cuando Jessica llegó a la escuela por la mañana, se dió cuenta de que todos sus compañeros la estaban mirando, susurrando entre ellos y riéndose. Después de entrar en clase le preguntó a su compañera Jurema si sabía la razón de tantas risas y ella le dijo que había un perfil en la red social Facebook, con el nombre de Jessica y con la foto de su perfil, donde ella proponía tener relaciones sexuales a cambio de pequeñas cantidades de dinero.

< Caso 7 >

Joana, que conocía el nombre y la dirección de Juliana, creó una cuenta de correo electrónico con su nombre, y luego inició la sesión en un sitio web de subastas en línea con el nombre y la dirección de Juliana y utilizó el e-mail con su nombre.

Después publicó un anuncio para vender tablets. João, que estaba interesado en comprar una tablet, pagó por una tablet pero nunca la recibió.

Juliana recibió un aviso un tiempo después para informarla de que estaba acusada de un delito de estafa.

< Caso 8 >

Julieta recibió una llamada telefónica de alguien que decía ser de "Novo Banco" y que la llamaba para que le confirmase algunos de sus datos personales. Julieta accedió, aliviada al oír que ella no había estado vinculada al "Banco Mau".

Dos meses después, Julieta recibió los movimientos de su cuenta, relacionados con compras realizadas en internet con su tarjeta de crédito.

1. CASOS DE ESTUDIO

< Caso 9 >

Varios mensajes llegan a muchas direcciones de correo electrónico supuestamente remitidos por el servicio de correo electrónico de atención al cliente, solicitando una actualización de la contraseña. La esposa de Julio introdujo sus datos, de esta forma el delincuente ya tenía acceso a su bandeja de entrada, llegando a conocer mucha de su información personal y la de su familia.

Después contactaron con Julio dos entidades de crédito que querían confirmar si los créditos solicitados a su nombre eran legítimos. Júlio, que nunca había pedido un crédito, les explicó que él no había solicitado ningún crédito a estas entidades. ¡Julio estaba asombrado por la cantidad de datos personales que el estafador, que había intentado obtener créditos en su nombre, tenía sobre él! Todas estas solicitudes fueron denegadas.

Un mes más tarde, Julio se dirigió a su banco con la intención de solicitar un crédito para la compra de una casa. Dicho crédito le fue rechazado debido a la cantidad de créditos que se habían solicitado a su nombre en los últimos meses.

< Caso 10 >

Jair ha sido víctima de bullying, desde que entró en el instituto Educación Secundaria de Odivelas.

Un día Jair llegó a casa e inició sesión con su perfil en la red social Facebook. Su corazón se paró por un momento cuando vio publicadas en su cuenta varias fotos suyas en ropa interior.

La desesperación se apropió de él, cuando recordó que la única persona que conocía su nombre de usuario y contraseña en Facebook era Jaime, su único amigo.

2.

ENMARCADO - ROBO DE IDENTIDAD

[illegible]

2. ENMARCADO - ROBO DE IDENTIDAD

2.1. Ciberdelincuencia

2.1.1. Globalización

Durante el año 2011 al menos 2,3 billones de personas, es decir, más de un tercio de la población mundial, tuvieron acceso a Internet³. Se estima que para el año 2020 existirán seis dispositivos conectados en red por persona, razón por la cual la criminalidad será cada vez más “alimentada” desde Internet.

Las Tecnologías de la Información (TIC) y la comunicación, representan los nuevos medios para cometer delitos. La conexión global a través de Internet y el uso de estas tecnologías también contribuyen a la aparición de nuevos delitos.

Igualmente, las (TIC) facilitan la internacionalización de la delincuencia. En otras palabras, el autor puede cometer un crimen en Brasil contra una víctima portuguesa sin dificultad, que es lo que sucede frecuentemente en los casos de phishing, como hemos visto en el caso 4 de esta guía.

De esta manera la ciberdelincuencia está aumentando, tanto por las organizaciones criminales como por delincuentes individuales que buscan nuevas oportunidades de obtener beneficios además de otras ventajas, como el hecho de causar daño a alguien cercano, a través de las redes sociales.

2.1.2. Definiciones de Ciberdelincuencia

No hay consenso sobre la definición Universal de ciberdelincuencia. La ley nacional e internacional no lo han establecido y no hay una doctrina consolidada en este tema.

Definiciones de ciberdelincuencia, según la Oficina de Naciones Unidas contra la Droga y el crimen, dependerá del uso al que este destinado este término.

Este mismo departamento se enfrenta a instrumentos nacionales e internacionales que no proporcionan una definición sobre ciberdelincuencia, en esta guía tratamos de describirla, mediante la enumeración de varios actos y conductas aquí incluidas⁴.

En este listado se enumeran, aunque de forma no exhaustiva, catorce comportamientos que puede constituir un delito cibernético, divididos en tres categorías:

3 Oficina de Naciones Unidas para la lucha contra la droga y delincuencia, Estudio integral sobre la Ciberdelincuencia - proyecto de Febrero 2013, p. 1.

4 Oficina de Naciones Unidas para la lucha contra la droga y delincuencia, Estudio integral sobre la Ciberdelincuencia - Proyecto de Febrero 2013, p. 11 y 12.

2. ENMARCADO -
ROBO DE IDENTIDAD

Hechos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos	Actos realizados a través de ordenador para obtener beneficios personales o financieros	Actos realizados a través de ordenador con contenidos delictivos
> Acceso ilegal a sistemas informáticos; > Acceso Ilegal, interceptación o adquisición de datos informáticos; > Intromisión ilegal en sistemas informáticos o de datos; > Producción, distribución o posesión de herramientas para el mal uso de ordenadores; > Violación de los medios de protección de datos o privacidad.	> Fraude o falsificación informática; > Delitos relacionados con la identidad cometidos por internet; > Delitos relacionados con derechos de autor y marcas comerciales cometidos por internet; > Envío o controlar el envío de correo no deseado; > Actos cometidos por ordenador que causan daños personales; > Captación de niños por internet.	> Incitación al odio a través de internet; > Producción, distribución o posesión de pornografía infantil a través de internet; > Actos que apoyan y fomentan el terrorismo a través de internet.

En un comunicado del Parlamento Europeo, el Consejo y el Comité de las Regiones, hacia una política general sobre la lucha contra el cibercrimen, La Comisión Europea define el delito cibernético como «actos criminales cometidos utilizando redes de comunicaciones electrónicas y los sistemas de información o en contra de este tipo de redes y sistemas».

Nos parece que la concreción del concepto de delito cibernético entre un concepto muy amplio y un concepto más restringido proporciona integridad y claridad. El concepto más amplio abarca todos los actos criminales que pueden llevarse a cabo por medios electrónicos, incluso si estos son meros instrumentos para su práctica. En el concepto restringido sólo se incluyen los delitos en los que el componente digital aparece como un elemento legal del delito o incluso como su objeto⁵.

5 Ver Pedro Dias Venâncio, Ciberdelincuencia Ley notas y comentarios, Editorial Coimbra, 2011, p. 17.

|||||

2. ENMARCADO - ROBO DE IDENTIDAD

|||||

2.2. Robo de Identidad

2.2.1. Dificultad Terminológica

Hay mucha polémica en torno al término “identidad” por lo que debemos establecer claramente desde el principio que en el contexto de esta guía, el término se referirá a todos los datos personales de alguien, cuando se utilizan por otra persona, y esto le permite actuar como la víctima con el fin de cometer delitos.

La expresión “Robo de identidad”, a pesar de ser usada en este manual, no define correctamente el fenómeno al cual pretende hacer referencia.

De hecho, ninguno de los términos que se utilizan por lo general en este contexto: “robo de identidad”, “suplantación de identidad” y “fraude de identidad”, por la influencia de los términos empleados en inglés, goza de una correcta terminología.

De hecho, los casos que vamos a conocer implican que el delincuente tiene que obtener datos de carácter personal o determinadas contraseñas o códigos personales de la víctima y utilizarlos para cometer delitos.

No será posible hablar de robo o robo de identidad, ya que los bienes sustraídos a los que se refiere el Código Penal (CP) deben ser cosas muebles ajenas (artículo 237 del Código Penal), entendiendo por tales aquellos objetos susceptibles de trasladarse de un lugar a otro sin sufrir por ello pérdida o menoscabo.

Además no podemos hablar de fraude, ya que este término no tiene un significado legal en el marco jurídico español.

En lo que se refiere al idioma Inglés, los términos “robo de identidad” y “fraude de identidad” son utilizados en la mayoría de los casos con el mismo significado, siendo el término “robo de identidad” más utilizado en los Estados Unidos de América mientras que “fraude de identidad” se utiliza más en el Reino Unido. Sin embargo, en Reino Unido se ha hecho un mayor esfuerzo por diferenciar entre el significado de cada uno de estos términos⁶.

La intención de esta guía es adoptar el término “robo de identidad” para describir el fenómeno

6 El robo de identidad es la obtención de información personal de otra persona sin su conocimiento o consentimiento y fraude de identidad es el uso de la identidad de otra persona en alguna actividad criminal, ya sea para la solicitud de créditos, bienes o servicios en nombre de la víctima o para el uso fraudulento de las cuentas bancarias de la víctima; James Jones, el fraude de identidad comprensión y cómo detenerlo, La Atacante Anónimo, CIFAS, 2009, p. 6. Los significados de ambas expresiones se incluyen en el concepto de suplantación de identidad relacionado con Internet que se presenta en esta guía.

2. ENMARCADO - ROBO DE IDENTIDAD

en cuestión, teniendo en cuenta que en nuestra opinión, la posibilidad de utilizar el término «fraude de identidad» debe ser excluido, debido a su carencia de contenido legal.

El término “robo de identidad”, aunque no constituya una descripción precisa ante la ausencia de violencia o coacción asociada a este tipo de comportamientos, será el término utilizado para describir este fenómeno por cuando es el más se corresponde con los comportamientos destinados a ser definidos y estudiados.

2.2.2. Definiciones

Al igual que en los casos de delitos informáticos, no hay una definición uniforme para el robo de identidad. En este manual trataremos de definir qué hechos encontramos que se pueden incluir en este fenómeno.

Empecemos afirmando claramente que el robo de identidad no es un delito en España, pero si es un fenómeno al que son aplicables un determinado número de sanciones penales.

Según la Oficina Comercial Federal de EE.UU: «Robo de identidad se produce cuando alguien utiliza la información personal de otra persona sin su consentimiento, para cometer fraude u otros delitos».⁷

Según el Grupo de Expertos de Lucha contra el Fraude de la Comisión Europea, la raíz del fenómeno, es la que se incluye en las definiciones previstas en el robo de identidad y fraude de identidad, es la apropiación y uso de información de la identidad personal de otra persona para llevar a cabo actividades ilegales.

Según la División de Delitos Económicos del Consejo Europeo, el término “robo de identidad”, describe actos en los que el autor del delito obtiene y utiliza de manera engañosa la identidad de otra persona. Estas acciones pueden llevarse a cabo sin la ayuda de medios técnicos, o también pueden hacerse con el uso de tecnología informática.

Algunas definiciones, que varían de un país a otro, se centran más en el acto de la obtención de la información, mientras que otros exigen el propósito de obtener estos datos con el fin de practicar ciertos actos ilegales.

7 Esta definición es
utilizada por el servicio
de ayuda a las víctimas
del manual de procedimientos
EE.UU. Departamento de
Justicia.

2. ENMARCADO - ROBO DE IDENTIDAD

El elemento común en todas las definiciones que se están proponiendo, es que los comportamientos descritos se refieren a uno o varios comportamientos de las tres etapas - la etapa de obtención de la información personal, la etapa de la posesión o la transferencia de información (sabiendo que ésta será utilizada para cometer un delito) y por último, la etapa de la utilización de los datos para cometer delitos.

Para formular una definición lo más amplia posible, se puede decir que el robo de identidad abarca la obtención no autorizada de datos personales y/o secretos de la víctima, su posesión o transferencia, sabiendo que serán utilizados con fines delictivos y usados para cometer delitos.

Como este manual se refiere al robo de identidad a través de Internet, los hechos serán cubiertos por esta definición si la información personal de la víctima se obtiene a través de Internet (como en los casos 2 y 4) u obtenidos por otros medios pero transferidos a través de Internet o usados para cometer un delito a través de Internet (como en los casos 1, 8 y 10). Si el delito es llevado a cabo solo en una de las etapas, (obtener, poseer y utilizar datos) tiene que ser llevado a cabo a través de Internet para encajar en el concepto de este enfoque.

Como hemos dicho con anterioridad, una vez obtenidos los datos de la víctima, el delincuente puede usarlos para cometer delitos. Esos delitos serán de tres tipos: delitos sin relación directa con la víctima pero que se practican en su nombre (como en los casos 5 y 7), delitos que tienen como objetivo el enriquecimiento del delincuente o de una tercera persona y causan daño directo a la víctima (como en los casos 1, 2, 4, 8 y 9) y delitos que tienen como objetivo la difamación de la víctima (como en los casos 6 y 10).

2.3. *Modi operandi*

La obtención de los datos de la víctima puede llevarse a cabo por un gran número de medios, que tienden a multiplicarse y diversificarse. En este contexto, la innovación con el objetivo de “inducir a error” en los mecanismos de detención de los usuarios y en los mecanismos de detención de las autoridades es constante. Por esta razón, el acercamiento de los distintos medios tendrá que ser genérico, para que no se queden rápidamente obsoletos.

Existen métodos tradicionales para obtener información personal, como por ejemplo y entre otros rebuscar en la basura, interceptar el correo, robar documentos de identidad u otros docu-

2. ENMARCADO - ROBO DE IDENTIDAD

mentos que contengan información personal o financiera de la víctima, hacerse pasar por un potencial empleador u otra persona que puede pedir este tipo de documentos, tratar de obtener información de personas cercanas a la víctima, contactar con la víctima o con los Bancos con falsos pretextos para obtener información privilegiada (véase el caso 8), comprar esta información, o incluso observar a la víctima mientras utiliza esta información (como es el caso de un compañero de trabajo de la víctima que lo observa en el momento de introducir los datos de acceso a su cuenta bancaria y luego los utiliza para retirar dinero de ella).

Todas estas formas se pueden incluir en el concepto de robo de identidad relacionada con Internet, de acuerdo con esta definición la información obtenida por medios no informáticos, puede ser utilizada para cometer cualquier delito a través de Internet.

Otro método de obtención de los datos de una víctima, “robo físico no tradicional”, es el robo del hardware, por ejemplo el robo del teléfono móvil de la víctima, que contiene información personal o secreta.

Vistos los principales métodos tradicionales para cometer el delito de robo de identidad relacionado con Internet, veamos ahora los métodos que hacen uso de las nuevas tecnologías, específicamente de Internet.

Las comúnmente llamadas “cartas nigerianas” que inicialmente aparecieron en forma de cartas, télex y fax, y en la actualidad suelen consistir en correos electrónicos, son un medio para cometer robo de identidad y utilizan tanto los medios tradicionales de obtención de datos personales, como el acceso a Internet.

El correo llega generalmente redactado en un español incorrecto y han sido dirigidas tradicionalmente a personas con altos cargos en empresas, en la administración pública, en la política y en otros sectores influyentes de la sociedad, pero en la actualidad se envía a todo el mundo. El remitente se presenta como un alto cargo del Gobierno, de una empresa estatal de algún país africano o como familiar de alguno de estos altos cargos.

Al principio, Nigeria fue el principal país emisor de este tipo de cartas. Posteriormente, se extendió a algunos países geográficamente cercanos a Nigeria y últimamente este tipo de correspondencia también llega desde Sudáfrica.

2. ENMARCADO - ROBO DE IDENTIDAD

El mensaje consiste en una propuesta de negocio. El remitente afirma poseer una alta suma de dinero obtenido por su condición privilegiada, y estar bien relacionado con la administración de su país.

Dice que él no puede asociar públicamente esta fortuna con su origen, y el delincuente justifica la necesidad de transferir dinero al extranjero. El delincuente le pide a la víctima que reciba en su cuenta bancaria una cantidad de dinero con la condición de ofrecerle a cambio entre el 20% y el 35% de esta cantidad. Con esta intención, el remitente solicita toda la información personal y la de sus cuentas bancarias y la de sus empresas u organizaciones.

Todos estos datos no se solicitan siempre en la primera carta o e-mail, sino en los siguientes cuando la víctima responde, permitiendo de esta manera el diálogo.

Con los datos de personas físicas, personas jurídicas y las cuentas bancarias, los defraudadores pueden cometer delitos a escala internacional.

Anuncios de empleo publicados en periódicos, Internet, etc., pueden ser falsos, solo con la intención de llamar la atención de la víctima con el fin de obtener sus datos personales para cometer un robo de identidad. Estas son las llamadas estafas de trabajo, que también hacen uso de los medios tradicionales de obtención de los datos personales o de Internet.

También es importante hablar de las peticiones de ayuda enviadas a través de correo electrónico o Facebook. El Phishing para obtener acceso a la cuenta de correo electrónico de alguien, es otra manera de dar credibilidad a estas peticiones de ayuda, (mira el caso de estudio 5). Con el mismo propósito se accede a la cuenta de la víctima en Facebook. Las solicitudes de ayuda podrán publicarse en el perfil de la víctima o se le envían a través de mensajes privados.

Facebook puede ser utilizado para obtener los datos de nuevas víctimas de robo de identidad. Mediante la instalación de malware en ordenadores, los delincuentes pueden publicar enlaces en los portales de la víctima que redireccionan a la víctima a una nueva página que solicita información personal. Un ejemplo de este tipo de situación es la publicación de un vídeo en la página de alguien para que los amigos de la víctima al hacer clic en “me gusta” tengan que dar algunos de sus datos personales en una página controlada por el delincuente.

Los motores de búsqueda como Google, permiten la búsqueda de millones de páginas en cuestión de segundos, y pueden ser utilizados para fines ilícitos.

2. ENMARCADO - ROBO DE IDENTIDAD

Google hacking es un término usado para describir búsquedas complejas en este motor de búsqueda, las cuales tienen como objetivo encontrar dispositivos desprotegidos y datos sensibles en sitios web. La base de datos de *Google Hacking* facilita esta tarea. Es una base de datos de búsquedas que identifican datos sensibles. Identifica vulnerabilidades del servidor y advertencias, mensajes de error que contienen demasiada información, archivos que contengan contraseñas, directorios sensibles, páginas que contienen portales o datos de la red vulnerables como los registros del firewall, y aunque *Google* bloquea algunas de las preguntas más conocidas, nada puede detener a un hacker de rastrear un sitio y el lanzamiento de las consultas de la base de datos de *Google Hacking*.

A menudo son los empleados de una compañía (o alguien haciéndose pasar por ellos) que tienen acceso a los datos e información secreta de la compañía para la que trabajan, o los gestores o administradores, o los clientes de la empresa, que obtienen los datos de entidades o clientes con intenciones delictivas para vender la información a organizaciones criminales. (Ver Caso 1)

Uno de los métodos más comunes para obtener datos personales para suplantar la identidad y que ha recibido mucha atención por las autoridades y por los medios de comunicación es el llamado phishing.

Este método consiste en el envío de un gran número de mensajes de correo electrónico (spam), que contiene un enlace a una página en la www. Esta página es normalmente una reproducción muy parecida a otra de un banco o una entidad emisora de crédito, y contiene elementos idénticos a la entidad verdadera. Sin embargo es una página falsa. Cuando la víctima utiliza el enlace para acceder a la página falsa, se le pedirá que se identifique introduciendo sus códigos secretos para acceder a su cuenta bancaria o tarjeta de crédito. Al introducir estos datos permitirán al delincuente que ha creado esta página falsa, acceder a la cuenta bancaria de la víctima y transferir dinero a otra cuenta o utilizar su tarjeta de crédito.⁸ El Caso de estudio 4 representa un ejemplo clásico de este tipo de métodos.

En los casos de phishing, se pueden identificar cuatro fases: La fase inicial consiste en el envío masivo de mensajes de correo electrónico con un enlace a una página web; En la segunda fase la víctima da información personal (contraseñas, códigos de acceso, etc.) al delincuente, ese momento consiste en la introducción de sus datos personales en el sitio falso; En la tercera fase el delincuente entra en la página real del banco de la víctima, introduce sus datos y retira el dinero de su cuenta. La cuarta fase consiste en el lavado de dinero (proceso en el cual los au-

8 Pedro Verdelho, *Phishing y otras formas de fraude en las redes de comunicación*, Ley de la Sociedad de la Información, Vol. VIII, p. 417.

2. ENMARCADO - ROBO DE IDENTIDAD

tores de algunas actividades delictivas ocultan el origen de sus bienes y los ingresos obtenidos ilegalmente, la transformación de este dinero conseguido en actividades delictivas en capital legalmente reutilizable, ya sea mediante la ocultación de su origen o la ocultación de la identidad del verdadero dueño de los fondos).

Si hablamos de nuevos métodos de obtención de datos privados para cometer delitos con el robo de identidad, se debe prestar atención al “pharming”, (técnica que utiliza los métodos de difusión de malware con formato de gusano - los gusanos. Consiste en la difusión a través de spam de archivos ocultos, que también de manera oculta, se auto-instalan en los aparatos informáticos de las víctimas. Estos archivos se instalan sin el conocimiento del propietario del equipo en los archivos del sistema, incluidos los archivos que contienen ‘Favoritos’ y el registro de las cookies del equipo. Como resultado de esta alteración, cuando el propietario del ordenador accede al sitio web del Banco el sistema lo redirige a otro sitio web, construido con el fin de conocer sus datos y robar la identidad de la víctima, utilizando idénticos métodos de Phishing.⁹

Otra técnica que es importante mencionar en este contexto es “sniffing”. La red de ordenadores comparte canales de comunicación. En canales compartidos los ordenadores pueden recibir información enviada a otros ordenadores. Al hecho de capturar información enviada a otros ordenadores se le llama sniffing.

Por último vamos a referirnos al “*hacking y cracking*” piratería informática, una forma de acceder de manera ilícita a sistemas informáticos para la obtención de información privada. Ambos términos se refieren al acceso a las claves de seguridad privada para obtener ilegalmente códigos de licencia de programas que permiten acceder a ordenadores de una persona sin su autorización. En el estudio del caso 3 describe una situación en la que el Hacker accede al ordenador de la víctima, se hace con su control y lo inutiliza para poder pedir después “un rescate” es decir una cantidad de dinero para resolver el problema que el mismo ha causado. En este caso no estamos frente a un robo de identidad relacionado con Internet, a menos que el hacker haya obtenido datos de Jandira accediendo a su ordenador.

La extracción de datos “Data mining” consiste en analizar datos con la intención de crear patrones y establecer relaciones entre ellos. Esta técnica se utiliza en muchas áreas de investigación. Hay programas de ordenador, los llamados extractores de datos, “data miners” que recopilan la información disponible en Internet o en el equipo de la víctima sin su autorización, la analizan y crean patrones. Esto permite por ejemplo a las empresas el poder predecir el comportamiento

9 Pedro Verdelho,
*Phishing y otras formas
de fraude en las redes de
comunicación*, Ley de la
Sociedad de la Información,
Vol. VIII, p. 415 y 416.

2. ENMARCADO - ROBO DE IDENTIDAD

de los consumidores y en cuanto al robo de identidad, hace posible la organización de los datos de identidad de la víctima, para que después puedan ser utilizados por el ciberdelincuente.

Finalmente vamos a ver en qué consiste el “keylogging”, esta técnica consiste en la utilización de un programa informático “keylogger” que una vez instalado en el ordenador permite grabar todo lo que se escribe en el teclado. Este método induce a error a los usuarios más cautelosos con Internet, como Joana, el personaje principal del Caso 2.

3.

ROBO DE
IDENTIDAD -
LA REALIDAD

[illegible]

3. ROBO DE IDENTIDAD - LA REALIDAD

3.1. Las situaciones más comunes relacionadas con el Robo de identidad en internet

Las principales situaciones tratadas en esta guía, han sido elegidas por ser las más comunes, una es el “phishing” utilizado tanto para obtener el acceso a la cuenta de correo electrónico de otra persona (véase el caso 5 y el caso 9) como para acceder a la cuenta bancaria (véase el caso 4) o para difamar en las redes sociales (véanse los casos 6 y 10).

Vamos a ver primero el “phishing” utilizado para acceder a una cuenta de correo electrónico. Una vez obtenidos los datos confidenciales y personales de la víctima a través de uno de los sofisticados métodos mencionados en el capítulo anterior, el delincuente puede acceder a la cuenta de correo electrónico de la víctima con el fin de ver el contenido del correo, para después establecer contacto con el Banco de la víctima, normalmente con el gestor de su cuenta. Utilizando esa cuenta de correo electrónico dará credibilidad a sus mensajes de correo electrónico y que consistirán, habitualmente, en solicitudes de ayuda financiera.

De esta manera, los dos objetivos principales del “phishing” son acceder a una cuenta de correo electrónico para obtener datos confidenciales y personales de la víctima (revisando su correo electrónico o contactando con el Banco) para cometer fraude financiero o simplemente, para engañar a la víctima ante amigos o conocidos, para que éstos últimos hagan transferencias de dinero a favor del delincuente. Hemos observado, que con frecuencia el phishing que realizan obteniendo acceso a la cuenta de correo electrónico de la víctima, tiene como objetivo final el acceso a su cuenta bancaria para realizar fraude bancario.

El «típico» caso de phishing utilizado para acceder a la cuenta bancaria de las víctimas, que hemos descrito anteriormente, es por desgracia, muy común en nuestro país.

En un contexto diferente, aparece el caso de robo de identidad por difamación en las redes sociales. Este tipo de situación se presenta con frecuencia en el contexto de las relaciones personales, bien de amistad o de pareja, y se presenta sobre todo entre los adolescentes y los jóvenes.

Podemos considerar la existencia de dos posibles casos de robo de identidad para la difamación en las redes sociales: la creación de una página falsa o perfil falso con los datos de la víctima y en su nombre, en esta página y a través de fotografías o frases tratar de ofender su honor y

3. ROBO DE IDENTIDAD - LA REALIDAD

faltarle al respeto (véase el caso 6) y el uso del perfil real de la víctima para difundir conductas, o juicios e imágenes igualmente ofensivas (véase el caso 10).

En estos casos, algunas veces es la propia víctima la que, en el ámbito de las relaciones personales, le proporciona los datos necesarios al delincuente, y permiten al delincuente acceder al perfil personal en la red social de la víctima para usar imágenes y otras informaciones personales para humillarlo/a.

3.2. El delincuente y la víctima

Es necesario distinguir, entre el perfil del criminal que suplanta la identidad con fines lucrativos y el robo de identidad para difamar en las redes sociales.

En el perfil del autor del robo de identidad en el primer caso, cabe distinguir entre el autor que conoce a la víctima porque es amigo, familiar o porque mantiene una relación con la víctima y por lo tanto, tiene mayor facilidad de acceder a su información personal y elige a esta víctima por esa razón, y el autor de robo de identidad que busca una víctima al azar. En el último caso el delincuente es más difícil de identificar, ya que además de que a menudo el delito se comete desde el lado opuesto del mundo, el delincuente siempre utiliza la identidad de la víctima, por lo que su identidad no es revelada en ningún momento. Por esta razón no se ha descubierto a muchos delincuentes que realizan este tipo de delitos, por lo tanto sus características nos son también desconocidas.

Al principio, la tendencia era ver el delincuente cibernético como un hombre, estudiante, experto en informática, con un coeficiente intelectual superior a la media, introvertido y con habilidades sociales limitadas, que le motiva el reto de desafiar a las máquinas y con el deseo de demostrar su superioridad intelectual a la sociedad.

Sin embargo la realidad ha cambiado. Hoy en día el autor del robo de identidad a través de internet puede ser cualquier persona con la intención de obtener información personal de las víctimas y después obtener beneficios de ellas.

Después de ver los múltiples y diversos medios disponibles de obtener los datos personales de las víctimas, que puede requerir desde conocimientos especializados hasta el modo más elemental como puede ser el de llevar a cabo la búsqueda en el cubo de basura de las víctimas, el autor del

3. ROBO DE IDENTIDAD - LA REALIDAD

robo de identidad puede ser una persona muy formada o con muy poca formación, de cualquier nivel social y con los rasgos personales más diversos.

El hecho de que haya varias páginas web en internet que enseñen cómo cometer delitos informáticos, determina que cualquier persona, independientemente de su cualificación, pueda ser autor, como en algunos de los casos que hemos visto anteriormente.

Un autor de este tipo de delitos es el llamado “insider” trabajador de confianza. Nos referimos a un empleado muy capacitado y que tiene la confianza del empleador y utiliza esa influencia y conocimientos sobre la empresa para la que trabaja. Sabe del funcionamiento interno del sistema informático y sus fallos, de los cuales obtiene, vende, o utiliza la información secreta y privilegiada para cometer delitos.

Los autores más peligrosos de este tipo de delitos son las organizaciones criminales que controlan todo el proceso del robo de identidad, desde la obtención de datos personales, hasta el blanqueo de capitales¹⁰.

En cuanto a las víctimas, debemos tener en cuenta que cualquiera podemos ser una víctima. El factor más decisivo en la selección de la víctima por el delincuente será la facilidad con la que puede obtener sus datos personales. Esto no quiere decir que el autor sea necesariamente alguien cercano a la víctima o con acceso a su correo electrónico, documentos personales o equipo informático, como un miembro de la familia, amigo u otra persona relacionada con la víctima, aunque también puede ser en muchos casos.

En el Reino Unido, las estadísticas indican que el objetivo más común de estos delincuentes son hombres trabajadores de entre 40 y 50 años de edad¹¹. Los delincuentes tratan de suplantar la identidad de personas con dinero, ya sea porque quieren robarles o dar credibilidad con sus datos a la hora de solicitar un crédito en su nombre.

En los Estados Unidos de América hay mayor incidencia de robo de identidad en los hogares con ingresos anuales superiores a \$ 75.000 y en las capas de población con edades comprendidas entre los 16 y 34 años de edad¹².

A menudo las víctimas suelen ser empresas, bancos, aseguradoras o instituciones financieras que prefieren no informar de estas situaciones de robo de identidad, y resolver el problema de

10 En este contexto, se pueden distinguir tres tipos de autores: Los que obtienen datos personales de la víctima, los que encuentran varias maneras de utilizar una identidad robada, por ejemplo falsificando documentos, y los que utilizan la identidad de otras personas para cometer delitos. El reparto del trabajo en las organizaciones criminales, tiene la intención de dividir el delito en varios autores y mantener en el anonimato de la organización, con el fin de proteger el núcleo de la organización, en caso de que uno de los autores pueda ser descubierto por las autoridades policiales.

11 Sandra Peaston, *The anonymous attacker and the not so anonymous victim*, The Anonymous Attacker, CIFAS, 2009 p. 20.

12 Lynn Langton y Michael Planty, *Victimas de suplantación de Identidad*, 2008, Oficina de Justicia informes de estadísticas especiales, 2010 p. 3.

3. ROBO DE IDENTIDAD - LA REALIDAD

manera interna asumiendo las pérdidas, por temor a que lo conozca el público en general y esta situación desacredite a la compañía.

En el contexto de las redes sociales el robo de identidad normalmente se lleva a cabo por personas que mantienen una estrecha relación con la víctima, y que por alguna razón deciden hacerle daño, por ejemplo mediante la creación de un perfil falso para difamar a la víctima o utilizando su perfil real para hacerlo. Esto ocurre frecuentemente en las relaciones rotas en la que los ex novios buscan la venganza.

3.3. Factores de Riesgo

Dado que la víctima puede ser cualquier persona, es muy importante reconocer las situaciones que hacen a los usuarios de Internet más vulnerables y aumentan el riesgo de ser una de las víctimas.

La información personal es cada vez más accesible a cualquier persona, en particular cuando se trata de las redes sociales y los Ciberdelincuentes son conscientes de este hecho y se aprovechan de ello.

Hay algunos comportamientos que la gente adopta usando las redes sociales, que aumentan el riesgo de sufrir el robo de identidad, veamos algunos de estos comportamientos:

- › No activar opciones de seguridad o mantener un perfil muy accesible;
- › Compartir mucha información personal en las redes sociales;
- › Aceptar solicitudes de amistad de desconocidos;
- › Publicar fotos íntimas en las redes sociales.

Trabajar muchas horas en línea aumenta el riesgo de ser víctima de la ciberdelincuencia, especialmente cuando alguien trabaja desde su casa y hace uso de su ordenador personal, ya que a diferencia de los empleados de una empresa más grande, en la cual los ordenadores están protegidos por técnicos especializados, los equipos informáticos de los trabajadores autónomos suelen estar menos protegidos.

Hay muchos comportamientos que aumentan el riesgo de ser víctima de los Cyberdelincuentes, veamos algunos de estos comportamientos:

3. ROBO DE IDENTIDAD - LA REALIDAD

- › No tener instalado en los equipos un programa antivirus o antispyware;
- › Hacer clic en enlaces desconocidos;
- › Mirar en la red contenidos para adultos;
- › Responder a mensajes en las redes sociales, responder a correos electrónicos u otros medios de comunicación de personas desconocidas;
- › Llevar las contraseñas o códigos PIN de acceso a información secreta en la cartera o almacenar estos datos en archivos sin protección;
- › Revelar nuestros códigos PIN o contraseñas, incluso a personas que son de nuestra confianza;
- › Usar información sencilla a la hora de crear una contraseña, por ejemplo la fecha de nacimiento, el nombre de una mascota o el nombre de la madre;
- › Mantener documentos importantes en un sitio poco seguro;
- › Tirar a la basura documentos sin antes haberlos destruido;
- › Enviar información confidencial por email;
- › No ejecutar las actualizaciones de los antivirus y otros programas de seguridad instalados en el ordenador;
- › Utilizar conexiones wi-fi gratis.

3.4. Impacto del robo de identidad

3.4.1. En la víctima

Aunque cualquiera puede ser víctima, hay ciertos grupos, especialmente los de menores ingresos económicos, las minorías étnicas y las personas mayores, que sufren un mayor impacto emocional, físico y financiero, debido principalmente a sus escasos recursos económicos, barreras lingüísticas o problemas de salud, por poner un ejemplo estos colectivos pueden tener más dificultades a la hora de denunciar el delito, rellenar formularios, leer ciertos documentos y mantener el contacto y la comunicación con los servicios de apoyo a las víctimas y las autoridades. También pueden tener más dificultades para recuperarse de las pérdidas económicas y del impacto emocional.

a. ECONÓMICO

El impacto económico sufrido puede ser de dos tipos: La pérdida económica directa, que se refiere a la cantidad económica que el autor del delito obtiene utilizando la identidad

3. ROBO DE IDENTIDAD - LA REALIDAD

13 LYNN LANGTON Y
MICHAEL PLANTY, *Victimas de
suplantación de Identidad*
2008, Oficina de Justicia
informes especiales de es-
tadísticas, 2010 p. 4.

14 LYNN LANGTON Y
MICHAEL PLANTY, *Victimas de
suplantación de Identidad*
2008, Oficina de Justicia
informes especiales de es-
tadísticas 2010 p. 4.

15 Informe sobre
Ciberdelincuencia Norton,
2011

16 Artículo 29 No-
tificación de operaciones no
autorizadas o de opera-
ciones de pago ejecutadas
incorrectamente:1. Cuando
el usuario de servicios
de pago tenga conocimien-
to de que se ha producido
una operación de pago no
autorizada o ejecutada in-
correctamente, deberá comu-
nicar la misma sin tardanza
injustificada al proveedor
de servicios de pago, a fin
de poder obtener rectifica-
ción de éste.2. Salvo en
los casos en los que el
proveedor de servicios de
pago no le hubiera propor-
cionado o hecho accesible
al usuario la información
correspondiente a la opera-
ción de pago, la comunica-
ción a la que se refiere el
apartado precedente deberá
producirse en un plazo
máximo de trece meses desde
la fecha del adeudo o del
abono. Así mismo, el artícu-
lo 31 establece el régimen
de responsabilidad del pro-
veedor de servicios de [->]

de la víctima, esto incluye bienes o servicios, o el valor económico obtenido y la pérdida económica indirecta que incluye todos los gastos sufridos por la víctima como consecuencia del robo de identidad como pueden ser (tasas judiciales, llamadas telefónicas, gastos de correo, etc.). Alrededor del 62% de las víctimas del robo de identidad reclaman estas pérdidas económicas sufridas, según un estudio elaborado en los años 2006 y 2007¹³.

El coste económico para las víctimas de robo de identidad fue de alrededor de 17,3 mil millones de dólares durante los años 2006 y 2007¹⁴ en los EE.UU., y 388 mil millones de dólares para un total de 24 países del mundo en el año 2011¹⁵.

En los casos de fraude a bancos o a través de tarjetas de crédito, los bancos normalmente prefieren abonar la cantidad defraudada a la víctima ya que no suelen ser cantidades significativas y para las instituciones financieras el conocimiento público de estos hechos haría mucho daño a su imagen. A pesar de esto las instituciones pueden verse obligadas a indemnizar a las víctimas.

En España, la Ley 16/2009 de 13 de Noviembre de Servicios de pago que incorporó a nuestro ordenamiento la Directiva 2007/64/CE, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, establece que en las operaciones de pago no autorizadas por el titular de la cuenta, el banco ha de devolver de inmediato el importe de la operación no autorizada, siempre y cuando el cliente no haya actuado fraudulentamente o con negligencia grave a la hora de aplicar las medidas de seguridad (secreto clave bancaria, etc) o haya comunicado de inmediato a la entidad bancaria la transferencia inconsentida¹⁶.

La víctima puede perder su casa y sus ahorros. La víctima de un fraude enfocado en el uso de sus cuentas de crédito, hace que en el futuro pueda tener dificultades en la obtención de nuevos créditos, préstamos, o incluso para pedir una hipoteca.

b. LEGAL

La víctima puede ser acusada y procesada por crímenes que no ha cometido (véase el caso 7) y puede ser demandada por la responsabilidad civil de los daños que no ha causado o por la responsabilidad contractual de las obligaciones que no ha asumido.

|||||

3. ROBO DE IDENTIDAD - LA REALIDAD

|||||

c. EMOCIONAL

Aunque los efectos psicológicos varían de una persona a otra, teniendo en cuenta las características de la víctima, algunos de los síntomas más comunes son: el miedo, la ansiedad, el odio, o incluso un constante y prolongado tiempo de desconfianza ante todo y ante todos, lo que muchas de las víctimas describen como «paranoia». El impacto emocional que causa el robo de identidad, es descrito de forma similar a las reacciones que sufren las víctimas de crímenes violentos.

Muchas víctimas sienten que su privacidad ha sido violada, y se sienten indefensos, impotentes y temen que les pueda volver a ocurrir.

La inseguridad creada por la pérdida de la estabilidad financiera tiene un impacto muy fuerte en estas víctimas. Ocurre lo mismo con la necesidad creada de demostrar su inocencia como en el caso de estudio 7.

Muchas de las víctimas se culpan a sí mismas de lo que les ha pasado y se preguntan en quien o quienes pueden confiar y si se hará justicia.

Las víctimas de robo de identidad relacionado con Internet y así como las de delitos informáticos en general, pueden sentirse victimas «de segunda clase» porque se sienten menos apoyadas que el resto de victimas de otros delitos, ya que los delitos informáticos están todavía infravalorados por la sociedad y hay pocos servicios de ayuda para apoyar a las víctimas.

Estas víctimas también tienen que saber cómo lidiar con la decepción que sufrirán en muchos casos en los que es imposible identificar al autor del delito. Es importante no subestimar a las víctimas, ya que cada vez que la víctima se enfrenta a nuevas deudas u otras consecuencias del delito, «se convierte de nuevo en víctima» (re-victimización).

Los efectos de este tipo de delincuencia son diferentes cuando el agresor es alguien cercano a la víctima. En estos casos las víctimas pueden sentirse presionadas a asumir la responsabilidad por el delito, con el fin de proteger al delincuente de las consecuencias. Las víctimas pueden ser reacias a denunciar el delito a las autoridades policiales, por si descubren que el autor del delito es alguien cercano y de confianza a la víctima, como un familiar o un amigo. También pueden sentirse avergonzados por haberse dejado engañar.

[->] pago. :Artículo 31 Responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas- Sin perjuicio de lo dispuesto en el artículo 29 de la presente Ley, y de las indemnizaciones por daños y perjuicios a las que pudiera haber lugar conforme a la normativa aplicable al contrato celebrado entre el ordenante y su proveedor de servicios de pago, en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante le devolverá de inmediato el importe de la operación no autorizada y, en su caso, restablecerá en la cuenta de pago en que se haya adeudado dicho importe el estado que habría existido de no haberse efectuado la operación de pago no autorizada.

3. ROBO DE IDENTIDAD - LA REALIDAD

d. IMPACTO EN LA VIDA DIARIA

El robo de identidad implica una molestia y una gran pérdida de tiempo cuando la víctima pretende reparar las consecuencias del delito. Se estima que en los EE.UU las víctimas pasan un promedio de 97 horas para reparar los daños causados por este tipo de delitos y gastan un promedio de \$1.884 (datos del Centro de Recursos Americano para el robo de identidad, *Identity Theft Resource Center*). En el Reino Unido la víctima va a pasar entre 3 y 48 horas para «limpiar su nombre»¹⁷.

El 40% de las víctimas afirmó que la pérdida de su tiempo fue la peor consecuencia del delito¹⁸.

3.4.2. En la sociedad

En el Reino Unido el coste del robo de identidad para la economía del país se ha estimado en 1, 3 billones de libras al año. En Australia las pérdidas anuales varían entre \$1 billón y más de \$3 billones. En los Estados Unidos durante el año 2005 se estimaron unas pérdidas de \$56.5 billones¹⁹. En el municipio de Lisboa, los daños causados por “phishing” durante el año 2011 superaron los €2 millones²⁰. En España, según la memoria anual de reclamaciones del Banco de España de 2012, las reclamaciones recibidas por pagos fraudulentos a través de Internet suponen un 0,3% del total de las recibidas.

El robo de identidad tiene un coste cada vez mayor para las instituciones como bancos, compañías de seguros y compañías que ofrecen bienes y servicios. Estas instituciones pueden ser obligadas a soportar la pérdida económica de la víctima, excepto cuando pueda demostrarse que es debido a la negligencia de la víctima. Este impacto para las instituciones no debe pasar desapercibido, porque en una última instancia se reflejará en los costes que el consumidor tendrá que soportar para poder beneficiarse de los servicios de estas instituciones.

También las empresas pueden sufrir el robo de su identidad, en este caso las pérdidas indirectas estarán relacionadas con la búsqueda de culpables entre sus empleados, la apuesta por la prevención y la contratación de seguros.

El desprestigio que pueden sufrir estas empresas tampoco debe subestimarse por su impacto en el sistema económico.

17 Grupo de expertos en prevención contra el fraude, Informe sobre la suplantación de identidad / fraude, Bruselas, 2007, p. 10.

18 Informe sobre Ciberdelincuencia Norton, 2011.

19 Marco Gercke, suplantación de identidad en Internet, División de Delitos Económicos de la Dirección General de Derechos Humanos y Asuntos Jurídicos, Estrasburgo, Francia, Consejo Europeo, 2007, pp. 5 y 6.

20 <http://www.asjp.pt/2012/04/03/judiciaria-cria-unidade-especial-para-investigar-cibercrime/>

3. ROBO DE IDENTIDAD - LA REALIDAD

Los Estados y sus Gobiernos pueden sufrir pérdidas directas, puesto que muchas suplantaciones de identidad están relacionadas con organismos públicos, y sufren pérdidas indirectas al tener que centrarse en la prevención, en la formación y en proveer recursos y medios a la policía y a las autoridades judiciales.

3.5. Dificultades en la investigación

El robo de identidad relacionado con Internet y los delitos cibernéticos en general plantean problemas graves tanto para la policía como a las autoridades judiciales en lo que se refiere a su investigación. Las características de este tipo de delincuencia, así como otros factores relacionados con ésta, hacen muy difícil identificar al responsable de estas conductas, en algunos casos casi imposible también dificulta definir este tipo de delito.

El robo de identidad en internet tiene una dimensión internacional, que cruza nuestras fronteras como la ciberdelincuencia. Si el autor del delito y la víctima no están en el mismo país se convierte en un obstáculo para la investigación, ya que aparte de tener que perseguirlos por un cybersendero que puede abarcar todo el mundo, se requiere la cooperación policial y judicial de todos los países implicados. El principio de la soberanía nacional, no permite a un país llevar a cabo investigaciones en otro país sin el permiso de las autoridades locales. La cooperación entre las autoridades de los diferentes países implica trámites y tiempo, lo cual debilita las investigaciones.

Se dice que la investigación de los delitos ciberderneticos puede hacerse eterna, desde que el autor comete el delito hasta que hay algún resultado, puede pasar un tiempo indefinido, que tampoco facilita la investigación.

Muchos de los métodos para cometer delitos cibernéticos pueden ser automatizados (no el de spam) para conseguir la reiteración independiente y convertir así el delito en permanente.

Los delincuentes utilizan tecnologías que les permiten mantener su anonimato, como programas de anonimato y encriptación.

El alto grado de conocimientos que exige la investigación de la ciberdelincuencia, requiere la participación y colaboración de varios organismos con conocimientos específicos y el uso de muchos recursos, tanto logísticos como humanos, y estos recursos son limitados.

3. ROBO DE IDENTIDAD - LA REALIDAD

Además de estas características específicas, hay otros factores que perjudican la investigación de los delitos cibernéticos.

Se estima que el 80% de las víctimas de delitos informáticos no los denuncian a las autoridades²¹. Esto es debido a la falta de conciencia de su condición de víctima y a la falta de información acerca de cómo denunciar, así como a la falta de esperanza en la eficacia de la investigación policial y la confianza en la impunidad de estos delitos. Otra de las razones que hacen que las víctimas no denuncien, es por la vergüenza que sienten por haber sido engañadas.

Empresas, bancos, compañías de seguros e instituciones financieras, deciden afrontar el problema internamente, asumiendo las pérdidas y no presentan una denuncia ante las autoridades, por temor a que el conocimiento del público general de un ataque informático puede traer descredito y pérdida de confianza tanto por los mercados como por sus clientes.

El número de víctimas crece diariamente tanto como el de usuarios de internet.

Hay páginas web que contienen información explicando cómo cometer cierto tipo de delitos informáticos, la cual es muy sencilla de obtener utilizando los buscadores más conocidos.

Cada día los delincuentes crean nuevas formas de acceder a la información personal de las víctimas y de cometer delitos usando esta información. Estas nuevas técnicas se difunden muy rápidamente a través del mercado negro online.

Un gran obstáculo para la investigación de los delitos cibernéticos, es la dificultad existente en el acceso a las pruebas electrónicas. Para localizar el origen de la comunicación, es decir la dirección IP (Protocolo de Internet) es necesario acceder al registro histórico de los archivos almacenados en los servidores de Internet, para esto su colaboración es fundamental.

También es muy importante garantizar la validez de las pruebas digitales. Por lo tanto, el acceso a las pruebas, su recogida, conservación y análisis siempre debe hacerse por especialistas y de acuerdo con protocolos específicos. La recogida de pruebas tiene que hacerse lo más pronto posible, ya que pueden ser destruidas con gran facilidad. Para hacer esto posible, la cooperación de los servidores de Internet es fundamental, ya que los servidores sólo están obligados a conservar determinados datos y por un período limitado de tiempo.

21 Oficina de las
Naciones Unidas contra la
Droga y la delincuencia,
Estudio sobre la Ciber-
delincuencia, Proyecto,
febrero de 2013 p. 117.

4.

MARCO
LEGAL

[illegible]

4. MARCO LEGAL

La implantación de una legislación adecuada juega un papel esencial en la prevención y la lucha contra la ciberdelincuencia.

Su existencia es muy importante en el marco de la penalización de los comportamientos delictivos, capacidades y competencias en la investigación por parte de las autoridades policiales, la recolección y almacenamiento de pruebas, la jurisdicción, la cooperación y el intercambio de información, tanto entre los diferentes organismos nacionales como internacionales y la responsabilidad de los servidores de Internet.

Aunque a nivel nacional los Estados tienden en centrarse más en la penalización de ciertos comportamientos, ya es reconocido que existe la necesidad de desarrollar la legislación respecto a otras cuestiones.

4.1. Marco Internacional

En los últimos años se ha puesto de manifiesto una gran preocupación internacional para luchar contra la ciberdelincuencia. En este sentido destaca la actividad llevada a cabo en este ámbito por el Consejo Europeo, la Unión Europea y las Naciones Unidas.

El Convenio del Consejo Europeo sobre la Ciberdelincuencia (ECCC) del 23 de noviembre de 2001 está siendo el instrumento internacional más ampliamente utilizado para la elaboración de leyes nacionales en materia de delitos cibernéticos.

El ECCC, se enfrenta a la informatización del mundo y al riesgo de las nuevas tecnologías e Internet utilizados para cometer delitos, su objetivo es desarrollar una política penal común y proteger a la sociedad de la ciberdelincuencia mediante la adopción de una legislación armonizada y la promoción la cooperación internacional. Nos ocuparemos a continuación de algunos de los delitos que este instrumento internacional ha establecido (acceso ilegal, interceptación ilegal, interferencia en los datos, interferencia en el sistema, mal uso de dispositivos, engaños informáticos, fraude informático, delitos relacionados con la pornografía infantil y delitos relacionados con los derechos de autor y derechos afines) y a su aplicación a las diferentes etapas del robo de identidad relacionado con Internet. La ECCC también establece normas de procedimiento y de cooperación internacional en las cuales se inspira la legislación española.

4. MARCO LEGAL

Dentro del contexto de la Unión Europea destaca la decisión marco 2005/222/ JAI relativa a los ataques contra los sistemas de información y la Directiva del Parlamento Europeo 2013/40 / UE y del Consejo Europeo que sustituye a la primera.

La decisión marco 2005/222 / JAI del Consejo Europeo destinada a mejorar la cooperación entre la policía y las autoridades judiciales de los Estados miembros y a armonizar las normas penales sobre los delitos informáticos.

La Directiva Europea 2013/40 / UE del Parlamento y del Consejo Europeo, se aprobó como hemos indicado, para sustituir la decisión marco que establece como su principal objetivo «el de aproximar la legislación penal de los Estados miembros en el ámbito de los ataques contra los sistemas de información, estableciendo normas mínimas relativas a la definición de los delitos y las sanciones pertinentes, y con la intención de mejorar la cooperación entre las autoridades» y establece los delitos de acceso ilegal, la interferencia ilegal en los sistemas informáticos, la interferencia ilegal en los datos y la interceptación ilícita, y también tipifica como delito el mal uso de los dispositivos informáticos.

4.2. Ley Española

En España la suplantación de identidad no se encuentra tipificada específicamente (con la excepción de la usurpación del estado civil así como el uso de datos personales de un tercero para adquirir productos o contratar servicios o hacer que contacten con aquel), sino que se considera un medio para cometer un ilícito civil o criminal. El uso ilegal de la identidad de otro se castiga, entre otros supuestos, cuando se hubiere llevado a cabo una apropiación de los datos de un tercero, cuando los hechos se hubieran cometido con una finalidad lucrativa, para provocar perjuicio económico a la víctima o un tercero o para causar perjuicio personal a la víctima.

La conducta consistente en la usurpación o suplantación de identidad puede separarse en tres fases²²:

- › **Fase 1.** La obtención de la información de la identidad, por ejemplo, por medio de robo físico, motores de búsqueda, atentados por infiltrados, atentados desde fuera (acceso ilegal a sistemas informáticos, Troyanos, Keyloggers, programas espías u otros malware) o por medio de la utilización de fraude electrónico u otras técnicas de ingeniería social;

22 Según T-CY Guidance Note # 4 Identity theft and phishing in relation to fraud. Adopted by the 9th Plenary of the T-CY (June 2013)

4. MARCO LEGAL

- › **Fase 2.** La posesión y la disposición de la información referente a la identidad, la cual incluye la venta de estos tipos de información a terceros;
- › **Fase 3.** El uso de información de identidad para cometer fraude u otros delitos, por ejemplo, por asumir la identidad de otro para explotar cuentas bancarias y tarjetas de crédito, crear nuevas cuentas, sacar préstamos y crédito, pedir bienes y servicios o diseminar malware.

Las Leyes que se pueden aplicar son:

- › El Código Penal;
- › La Ley Orgánica 15/99 de 13 de diciembre de protección de datos;
- › Ley General de Telecomunicaciones 9/14 de 9 de Mayo;
- › Ley Orgánica 1/82 DE 5 de mayo, de protección civil del Derecho al Honor, la intimidad personal y familiar y la propia imagen.

- **Regulación en España de la suplantación de identidad.**

La suplantación de identidad en sentido estricto no está tipificada como delito en la actualidad en España. Se entiende por tal la conducta consistente en hacerse pasar por otro, utilizando sus datos identificativos a través de Internet, medio electrónico o sistema informático en línea, de tal modo que genere error sobre la intervención en esos medios de la persona suplantada.

La Memoria de la Fiscalía General del Estado, ya en el año 2012 alertaba acerca del grave problema de la suplantación de identidad online y sobre la conveniencia de tipificar este tipo de conductas. En el año 2014, la Memoria presentada por dicha Fiscalía General da un paso adelante y recoge como propuesta de reforma legislativa la tipificación del delito de suplantación de identidad en medios electrónicos, señalando que el problema de la suplantación de identidad no ha hecho más que aumentar, puesto que se está detectando un incremento de este tipo de conductas en foros, chats, o redes sociales y, en general, en los medios de comunicación electrónicos con el evidente perjuicio que las mismas pueden generar en el normal desarrollo de la vida y actividad personal y profesional de quien es víctima de esa suplantación de identidad on-line.

4. MARCO LEGAL

En España, actualmente, está castigada tanto la usurpación del estado civil, como el uso de datos personales de un tercero para adquirir productos o contratar servicios o hacer que contacten con aquel.

En cuanto a la usurpación del estado civil, el mismo está tipificado en el artículo 401 del Código Penal en los siguientes términos: el que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años. Doctrinalmente, se viene entendiendo que la conducta típica consiste no sólo en usar nombre y filiación de otra persona, sino, al tiempo, ejercer como propios sus derechos y acciones. Es evidente, que en los supuestos de suplantación on-line, por la propia naturaleza del medio empleado para ello, el alcance de la simulación se limita a las relaciones y/o actividades que la víctima desarrolla en el ciberespacio, quedando siempre fuera del ámbito de la simulación toda la proyección personal de la víctima en el mundo físico o, dicho de otro modo, off-line. En estos supuestos se puede afectar muy seriamente a la fama, al honor, a la consideración pública o a la intimidad de la víctima y también al nivel de confianza exigible en el ámbito de las relaciones interpersonales particulares o profesionales y por tanto a bienes jurídicos necesitados de especial protección.

En lo relativo a la segunda conducta, hemos de señalar que la reforma operada en el Código Penal por LO 1/15, introduce el artículo 172 ter, y aborda de forma tímida este problema, castigando al que, mediante el uso de los datos personales de un tercero, adquiera productos o mercancías o contrate servicios o haga que terceras personas contacten con ella. Si bien, este delito está pensado para los supuestos de acoso con incidencia en la libertad de las personas y que se lleven a efecto con una de las tres finalidades expresadas. Dice así este artículo : “ 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:...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.”

Al margen de esta exigua regulación, hemos de señalar que el Congreso de los Diputados está estudiando la posibilidad de tipificar la suplantación de identidad como delito, y así se refleja en el informe de la Subcomisión del estudio sobre las Redes Sociales constituida en la Comisión de Interior del congreso de los Diputados, publicada en el BOE el 9 de Abril de 2015.

4. MARCO LEGAL

- **Regulación en España de los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. Cumplimiento por España del Convenio sobre ciberdelincuencia y del resto de normativa Europea en este ámbito.**

En el marco de los delitos informáticos, para cumplimentar la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, ya la LO 5/10 de reforma del Código Penal, incluyó como delito tanto el acceso sin autorización vulnerando las medidas de seguridad a datos o programas informáticos contenidos en un sistema o en parte del mismo, como los daños, deterioros, alteración, supresión o hacer inaccesibles datos o programas informáticos ajenos, así como la obstaculización o interrupción del funcionamiento de un sistema informático ajeno.

Con posterioridad, para trasponer a nuestro derecho interno la Directiva Europea 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión Marco 2005/222/JAI del Consejo, se ha dictado la LO 1/15. El objetivo es dotar de la necesaria protección a los sistemas de información, para considerar delictivas aquellas conductas que consistan en el acceso e interferencia ilegales de los mismos, así como de los datos informáticos que contengan.

En este sentido, se incorpora como conducta delictiva el llevar a cabo sin autorización y mediante la utilización de artificios o instrumentos técnicos, la interceptación de 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 (artículo 197 bis, apartado 2).

Se considera delictiva igualmente la producción y la adquisición para su uso, importación o facilitación a terceros, de programas informáticos concebidos o adaptados para cometer delitos informáticos, y también proporcionar contraseñas de ordenador o códigos de acceso que permitan acceder a todo o parte de un sistema de información (artículo 197 ter).

Igualmente se tipifica el delito de sabotaje informático, consistente en borrar deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos (artículo 264 cp), produciéndose una importante elevación de penas y, en cumplimiento de la Directiva precitada, se castigan con mayor gravedad, entre otros supuestos, cuando el hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales y cuando haya afectado al sistema informático de una

4. MARCO LEGAL

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.

En relación a los daños que afecten a una infraestructura crítica, se ha optado por incorporar en el texto del precepto un concepto de infraestructura crítica, tomándose como referencia la contenida en la propia Directiva.

La definición que se ha acogido para permitir la aplicación del tipo penal es la de considerar 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 “(artículo 264.2.4)

En la siguiente tabla podemos comprobar la correspondencia entre las conductas delictivas incluidas en la Convención sobre Ciberdelincuencia y la legislación española.

Articulo codigo penal	Comportamiento	Correspondencia con convenio sobre ciberdelincuencia
197 BIS.1 CODIGO PENAL	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.	Artículo 2 ACCESO ILÍCITO FASE 1
197 BIS.2 CODIGO PENAL	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.	Artículo 3 INTERCEPTACIÓN ILÍCITA FASE 1

.....

4. MARCO LEGAL

.....

	cas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.»	
Artículo 264 CODIGO PENAL	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.	Artículo 4 INTERFERENCIA DATOS FASE 1
Artículo 264 BIS CODIGO 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 triple 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	Artículo 5 INTERFERENCIA DE SISTEMAS FASE 1

.....

4. MARCO LEGAL

	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 CODIGO 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.»	Artículo 6 ABUSO DE DISPOSITIVOS FASE 2
Artículo 197 TER	Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis: a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o b) una contraseña de ordenador, un	Artículo 6 ABUSO DE DISPOSITIVOS

4. MARCO LEGAL

|||||

4. MARCO LEGAL

Artículo 197 QUINQUIES	Quando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.»	Artículo 12 RESPONSABILIDAD DE LAS PERSONAS JURÍDICAS
Artículo 264 QUATER	Quando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los tres artículos anteriores, se le impondrán las siguientes penas: a) Multa de dos a cinco años o del quintuplo a doce veces el valor del perjuicio causado, si resulta una cantidad superior, cuando se trate de delitos castigados con una pena de prisión de más de tres años. b) Multa de uno a tres años o del triple a ocho veces el valor del perjuicio causado, si resulta una cantidad superior, en el resto de los casos. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.»	Artículo 12 RESPONSABILIDAD DE LAS PERSONAS JURÍDICAS

- Regulación en España sobre la conservación de datos.

El Convenio sobre Ciberdelincuencia en sus artículos 16,17, 18 y 19 obliga a los Estados parte a adoptar medidas que garanticen la conservación rápida de datos informáticos almacenados, la conservación y revelación parcial rápidas de datos sobre el tráfico y el registro y confiscación de datos informáticos almacenados.

En el ámbito español la primera norma que impuso a los operadores una obligación de conservar los datos generados en las comunicaciones fue el artículo 132 de la Ley 34/2002 de 11 de julio de servicios de la sociedad de la información y de comercio electrónico (los operadores de redes y

4. MARCO LEGAL

servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos deberán retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un periodo máximo de doce meses, en los términos establecidos en este artículo y en su normativa de desarrollo” y el apartado tercero “los datos se conservarán para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional, poniéndose a disposición de los Jueces o Tribunales y del Ministerio Fiscal que así lo requieran. La comunicación de estos datos a las Fuerzas y Cuerpos de Seguridad se hará con sujeción a lo dispuesto en la normativa sobre protección de datos personales”.

Con posterioridad, ha sido dictada la Ley 25/2007 de 18 de octubre de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, modificada por la disposición final cuarta de la Ley 9/2014, de 9 de mayo, de Telecomunicaciones. Esta Ley debe ser interpretada a la luz de las exigencias de la Sentencia del Tribunal de Justicia de la Unión Europea de 8 de abril de 2014, que declara inválida la Directiva 2006/24/CE.

Conforme a la citada normativa, para que los operadores que prestan servicios de comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo es necesaria la autorización judicial, que debe adoptar la forma de auto y tener la suficiente motivación que justifique la adopción de la medida, y que se dicte en el marco de un proceso penal abierto por un delito grave. Una vez autorizada dicha cesión, los datos sólo pueden ser entregados para su análisis a los miembros de las Fuerzas y Cuerpos de Seguridad cuando desempeñen funciones de policía judicial, a los funcionarios de la Dirección Adjunta de Vigilancia Aduanera cuando ejerzan competencias como policía judicial y al Centro Nacional de Inteligencia en el curso de investigaciones de seguridad sobre personas o entidades.

Recientemente se ha publicado la LO 13/15 de 5 de octubre de modificación de la Ley de Enjuiciamiento Criminal sigue la citada línea garantista confirmando la necesidad de la preceptiva autorización judicial para recabar los datos electrónicos.

- **Existen actividades en las que, sin llegar a constituir la conducta de suplantación de identidad en sentido estricto, se produce el acceso a los datos de terceros sin su consentimiento, la utilización, remisión de estos datos a terceros, la estafa a través de Internet utilizando datos personales, entre otras. Estas conductas están tipificadas en el código penal de la siguiente forma:**

4. MARCO LEGAL

Artículo 197.1 CODIGO PENAL VIOLACION DE PRIVACIDAD	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.
Artículo 197.3 DIFUSION A TERCEROS DE DATOS OBTENIDOS MEDIANTE VIOLACIÓN DE PRIVACIDAD	3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.
Artículo 197.4 AGRAVACIONES	4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando: a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima. Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.
Artículo 197.5 DATOS SENSIBLES	5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.
Artículo 197	7. Será castigado con una pena de prisión de tres meses

4. MARCO LEGAL

FOTOGRAFÍAS	a un año o multa de seis a doce meses el que, sin auto- rización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aqué- lla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad nece- sitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.»
ARTÍCULO 298 CODIGO PENAL BLANQUEO DE CAPITALES POR IMPRUDENCIA GRAVE	El que, con ánimo de lucro y con conocimiento de la comisión de un delito contra el patrimonio o el orden socioeconómico, en el que no haya intervenido ni como autor ni como cómplice, ayude a los responsables a apro- vecharse de los efectos del mismo, o reciba, adquiera u oculte tales efectos, será castigado con la pena de prisión de seis meses a seis años. Castigándose la imprudencia grave con la pena de prisión de seis meses a dos años y multa del tanto al triple en el artículo 301 del CP.

4.3. El robo de identidad, el derecho nacional y el Convenio sobre la Ciberdelincuencia

Conceptualmente, como hemos señalado ut supra, la suplantación de identidad, puede ser dividida en tres fases, la de obtención de la información de identidad, la de posesión y disposición de dicha infor-
mación y, finalmente, la de uso de la información de identidad para cometer fraude u otros delitos.

En la primera fase, la obtención de la información de identidad, son aplicables varios artículos de la Convención sobre Cibercrimen²³, concretamente, los artículos 2²⁴, 3²⁵, 4²⁶,5²⁷ y 7²⁸.

El Código Penal español castiga en su articulado la obtención de la información de identidad de

23 Tabla comparati-
va recogida en epígrafe 4.2
del presente trabajo

24 Acceso ilícito

25 Interceptación
ilícita

26 Interferencia
datos

27 Interferencia de
sistemas

28 Falsificación de
datos

4. MARCO LEGAL

forma ilegítima, específicamente, los artículos 197 bis 1, 197 bis 2, 248.2.b, 264,264 bis y 197.2.

La violación de la intimidad también sería aplicable a esta primera fase, estando tipificada como conducta delictiva la consistente en interceptar mensajes de correo electrónico, o telecomunicaciones, la utilización de artículos técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación²⁹, y en los supuestos en los que se cometa por las personas encargadas de los ficheros o soportes informáticos o mediante la utilización no autorizada de datos personales de la víctima³⁰.

La segunda fase, posesión y/o transferencia de datos, está regulada en el artículo 6³¹ de la Convención sobre Cibercrimen.

La legislación Española se ocupa de esta segunda fase en los artículos 264 ter, y 197 ter.

La violación de la intimidad también parece encajar en esta segunda fase, al castigar la difusión, revelación o cesión de los datos descubiertos o de las imágenes captadas³², considerando mas grave esta conducta lo que determina la imposición de una pena agravada.

Se considera delictiva igualmente, la difusión de imágenes captadas con consentimiento de la víctima, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona, imponiéndose pena más grave en los supuestos en los que el autor fuera cónyuge o persona unida a él por análoga relación de afectividad, o cuando la victima fuera menor o discapacitado³³.

La tercera fase, el uso de la identidad de otra persona para cometer fraude u otros delitos, se refiere a ella el artículo 8³⁴ de la Convención sobre Cibercrimen.

La legislación española dedica los artículos 197.6, 172 ter y 248.2 del Código Penal. Este último precepto recoge específicamente el fraude informático.

La violación de la intimidad también sería aplicable a esta tercera fase, castigando la difusión de imágenes captadas con consentimiento de la víctima, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona, y sea realizada con fines lucrativos³⁵.

29 Artículo 197.1 CP violación de privacidad.

30 Artículo 197.4 CP

31 Abuso de dispositivos

32 Artículo 197.3 CP difusión a terceros de datos obtenidos mediante violación de privacidad.

33 Artículo 197 CP

34 Fraude informático

35 Artículo 197.7 CP

5.

LEY
NACIONAL
APLICABLE

[illegible]

5. LEY NACIONAL APLICABLE A LOS CASOS DE ESTUDIO

< Caso 1 >

La conducta de Josué es incardinable en el delito de descubrimiento y revelación de secretos del artículo 197 apartados 2,3,4 y 6 del Código Penal al ceder a un tercero datos reservados de carácter personal de los que tenía conocimiento por razón de su cargo y con ánimo de lucro.

La organización criminal al acceder de forma ilícita a la cuenta de Josué podría incurrir en el delito del artículo 248.2 del Código Penal.

< Caso 2 >

En el caso de Joana, con respecto al uso de keyloggers para obtener los datos de acceso a sus cuentas bancarias se aplica el delito previsto como acceso ilícito a la cuenta bancaria estaríamos ante la conducta tipificada en el artículo 197 bis apartado 1 en concurso con un delito del artículo 197 del Código Penal.

El fraude informático recogido en el artículo 248.2 del Código penal sería aplicable en el caso en el que verdaderamente se apoderara de dinero de la cuenta.

< Caso 3 >

En este supuesto al encontrarnos ante una obstaculización del funcionamiento de un sistema informático, sería aplicable el relativo a la interferencia de sistemas, que se corresponde con el artículo 264 bis del Código Penal.

La segunda conducta, la consistente en pedir dinero para llevar a cabo el desbloqueo, sería tipificada como un delito de extorsión del artículo 243 del Código Penal.

< Caso 4 >

En el caso de Josefina podría incardinarse la conducta en el artículo 248.2 del Código Penal.

5. LEY NACIONAL APLICABLE A LOS CASOS DE ESTUDIO

< Caso 5 >

El caso de José estaríamos ante un acceso ilícito del artículo 197.1 del Código Penal al haber accedido al correo electrónico y una ulterior estafa informática del artículo 248.2 del Código Penal en grado de tentativa.

< Caso 6 >

La conducta de Joel podría ser calificada como el delito previsto en el artículo 172 ter del Código Penal, por cuanto el autor ha utilizado datos personales de Jessica para que terceras personas se pongan en contacto con ella.

< Caso 7 >

La conducta de Joana estaría incardinada en el artículo 172 ter del Código Penal, por cuanto de forma insistente y reiterada, sin estar legitimamente autorizada y alterando gravemente el desarrollo de la vida cotidiana de Juliana, mediante el uso de sus datos personales, contrató servicios e hizo que terceras personas se pusieran en contacto con ella.

< Caso 8 >

En este supuesto estaríamos ante el delito de estafa informática del artículo 248.2 del Código Penal.

< Caso 9 >

En este caso estaríamos ante un delito de descubrimiento de secretos del artículo 197 del Código Penal y así como un delito de tentativa de estafa informática [artículo 248.2 en relación con el artículo 16 del Código Penal].

5. LEY NACIONAL APLICABLE A LOS CASOS DE ESTUDIO

< Caso 10 >

El acceso ilícito a la cuenta de Facebook estaría tipificado en el artículo 197 del Código Penal.

6.

PREVENCIÓN

[illegible]

6. PREVENCIÓN

Según un estudio realizado por la Comisión Europea en 2012, el 70% de la población estudiada había escuchado o visto información sobre los delitos cibernéticos, el 31% de la población se consideraba suficientemente informada sobre la ciberdelincuencia, y el 7% de la población se consideraba muy bien informada³⁶.

Otro estudio centrado en más de 13.000 usuarios de Internet en 24 países, reveló que el 90% de esta población borra los correos electrónicos sospechosos recibidos de remitentes desconocidos, y el 80% de los usuarios utiliza antivirus y no abre archivos adjuntos o enlaces que aparecen en los correos electrónicos o mensajes de remitentes desconocidos³⁷.

Sin embargo, en lo que a las redes sociales se refiere, sólo el 50% afirmó utilizar las opciones de privacidad que se ofrecen para controlar la información que comparten en la red, y el 35% de la población estudiada acepta solicitudes de amistad de desconocidos.

Los estudios realizados sobre niños y adolescentes en países menos desarrollados, muestran que este grupo de edad tiene mayor riesgo de convertirse en víctimas. Un estudio centrado en más de 25.000 niños en edad escolar de 7 países de América Central y América del Sur, reveló que alrededor del 45% de los niños que tenían conexión a Internet en su casa, y que sólo el 10% de estos tenía protección antivirus o filtros web en su ordenador.

Los Estados deben utilizar sus recursos para educar a la población antes de que sus ciudadanos se conviertan en víctimas. Enseñar a las comunidades a protegerse con antelación del robo de identidad es la medida más eficaz para hacer frente a este fenómeno.

6.1. Medidas de prevención

Cuando se usan las redes sociales el usuario debe:

- › Ser consciente de la información que se publica en las redes sociales. La información que puede hacerle vulnerable no debe publicarla;
- › Conocer la información que publican sobre él en las redes sociales;
- › Elegir cuidadosamente a las personas a las que les da acceso a su información personal;
- › Estar atento a personas desconocidas;
- › Desconfiar y no creer en todo lo que oye o lee en internet;

36 Commission
Europea. 2012 Barometro
especial 390.

37 Symantec. 2012.
Informe Norton Cyberdelin-
cuencia 2012.

6. PREVENCIÓN

- › Conocer y ser consciente de las condiciones que se aceptan al entrar en una red social que con frecuencia incluyen la pérdida de los derechos sobre el contenido subido.

Cuando se utiliza el correo electrónico el usuario debe:

- › Tener en cuenta que los correos electrónicos escritos en un mal español, con faltas de ortografía, errores gramaticales o frases incoherentes probablemente serán parte de sistemas de phishing, aunque vengan de un remitente conocido;
- › Esto ocurre especialmente con los e-mails que informan al usuario que ganó un premio o es finalista en un concurso, que hay un problema con la cuenta de correo electrónico o que es necesario validar sus datos del banco u otros datos importantes;
- › No descargar archivos adjuntos, no hacer «clic» en enlaces que nos llegan, y no responder a los correos electrónicos de desconocidos o con contenidos sospechosos;
- › Esforzarse en reconocer la dirección de correos electrónicos de bancos o de cualquier otra institución con la que se trabaja;
- › En caso de no reconocer la dirección de un correo electrónico, ponerse en contacto con la institución correspondiente y averiguar si el e-mail realmente es suyo;
- › Pasar el ratón sobre cualquier enlace antes de descargarlo y revisar con el navegador en la esquina inferior izquierda, a que dirección nos va a dirigir;
- › Si el dominio del enlace es externo al dominio de la entidad que parece estar enviándonos el correo electrónico, el usuario debe abstenerse de hacer clic en el enlace;
- › En caso de duda, se debe validar el enlace a través del sitio web <https://www.virustotal.com/es> o contactando con la supuesta entidad que envió el correo electrónico o accediendo al sitio www.cert.fnmt.es poniéndose en contacto con el equipo CERT;
- › Siempre hay que contactar con el banco en caso de recibir un correo electrónico supuestamente enviado por ellos, ya que los bancos no suelen contactar con sus clientes por medio de correo electrónico;
- › Si se recibe un e-mail extraño de una persona conocida pidiendo ayuda o nuestros datos personales, el usuario debe sospechar, ya que nuestra cuenta de correo electrónico puede no ser segura;
- › Evitar la utilización del correo electrónico de empresa para el uso personal;
- › No utilizar el correo electrónico para enviar datos e información confidencial;
- › Mantener actualizado el programa que se utiliza para el envío de correos electrónicos;
- › Desactivar las opciones que permiten abrir o ejecutar archivos o programas adjuntos a los mensajes de correo de forma automática;
- › Desactivar los programas de *Java* o las opciones que ejecutan los programas de *JavaScript*.

6. PREVENCIÓN

Para proteger los ordenadores o dispositivos móviles el usuario debe:

- › Evitar crear situaciones favorables en las que pueda sufrir el robo de ordenadores, teléfonos móviles y tabletas, como por ejemplo, dejarlos en el coche;
- › Proteger el equipo frente a usuarios malintencionados, mediante la creación de una contraseña para iniciar la sesión y cerrar la sesión cuando no se está utilizando el ordenador;
- › Cuando se presta el ordenador, hay que tener presente los datos personales que puede contener el equipo y tener en cuenta que se puede acceder a estos datos guardados en el disco duro, aunque estén almacenados en una cuenta protegida por contraseña;
- › En el momento de vender o tirar el ordenador, teléfono móvil o tableta, eliminar toda la información personal que pueda contener;
- › Siempre hay que mantener actualizado el equipo con antivirus, antispyware, firewall y con la protección antispam;
- › Configurar el navegador para evitar el almacenamiento de las cookies y de pop-ups;
- › Incrementar el nivel de seguridad del navegador hasta un nivel medio o alto;
- › Prestar atención a los programas instalados, comprobar su procedencia, siempre deben venir de la empresa que los ha creado o desde un sitio web de confianza;
- › Evitar acceder a sitios web donde la información personal va a ser compartida en redes públicas, redes de wi-fi abiertas, o en equipos desconocidos;
- › Prestar especial atención a sitios web donde se van a dar datos personales, especialmente sitios web de bancos, evitar sitios web con errores ortográficos o tipográficos y sin las debidas normas de seguridad;
- › Comprobar siempre si la conexión a un sitio web se está haciendo por «https» (modo seguro) y no por «http» (modo falso) y también comprobar si nos aparece un icono que representa un candado o una llave;
- › Usar solo la web oficial de su banco;
- › Leer las políticas de privacidad de los sitios web de las entidades financieras u otros que impliquen la divulgación de los datos personales, y si no se entiende o no se aceptan, contemplar la elección de otra entidad;
- › En los dispositivos móviles, el protector de pantalla debe estar en modo activo;
- › Activar la opción de borrado remoto en el caso de tener información sensible almacenada en el dispositivo³⁸;
- › Realizar copias de seguridad del contenido del dispositivo con frecuencia, teniendo especial cuidado con estas (guardar copias de forma encriptada con una buena contraseña);
- › Cuando se instalan aplicaciones en el dispositivo, hay que verificar si la descarga pro-

38 Para los diferentes tipos de dispositivos, existen aplicaciones gratuitas y servicios que en caso de pérdida o robo permiten al usuario borrar todos los datos de forma remota (si tienes Android las aplicaciones son "Mobile Defense" o "WaveSecure" y si tienes un iPhone hay aplicaciones como "Find My iPhone" o "MobileMe").

6. PREVENCIÓN

viene de una fuente segura y de confianza, y prestar atención a los permisos solicitados, por ejemplo si una aplicación que no necesita acceder a nuestro correo electrónico nos pide estos datos, el usuario deberá optar por otra aplicación alternativa.

Con el fin de proteger los documentos de identidad y datos personales, el usuario debe:

- › Llevar solamente los documentos que necesita cada día en su cartera;
 - › Llevar la cartera en un sitio seguro en el trabajo;
 - › Mantener los documentos en un lugar seguro en casa, como por ejemplo en una caja fuerte;
 - › Destruir los documentos físicos o digitales antiguos que pueden contener datos personales u otra información de naturaleza similar, con el fin de que nadie pueda hacer uso de ellos;
 - › Al pedir un nuevo talonario de cheques, pedir que estos sean enviados a la oficina de correos en vez de a su casa;
 - › Tener muy poca información personal impresa en los cheques bancarios;
 - › Comprobar la identidad de cualquiera que nos pide información personal por teléfono, por correo electrónico o por cualquier otro medio y conocer porque tiene la necesidad de pedirnos esta información:
- » Pedir la identificación de la persona que solicita la información y la del contacto principal de esta entidad a la que supuestamente representa, valorar la posibilidad de no proporcionar ningún dato de inmediato y posteriormente contactar con él para darle la información requerida;
 - » Pensar porque la persona que contacta con él tiene la necesidad de saber esta información, la institución financiera en la que trabaja tal vez necesite saber el apellido de su madre para verificar su identidad cuando llama para obtener información sobre su cuenta. Sin embargo, si alguien nos llama o envía un e-mail preguntando cual es el apellido de su madre y dice pertenecer a la institución financiera con la que un cliente trabaja, el usuario debe saber que esta persona no necesita esa información, ya que estará en la base de datos de la entidad, y probablemente esta llamada o correo electrónico será simplemente para obtener información privada en beneficio propio;
 - » Si un extraño llama o envía a un usuario un correo electrónico informándole de que ha ganado un premio u otro beneficio y solicita información personal, el usuario debe pedir a esta persona que le solicite esta información por escrito, si no lo hace, el usuario debe finalizar con este contacto, si le envía esta solicitud por escrito el usuario debe leerlo atentamente y cuando envíe sus datos personales asegurarse de que se dirigen a una conocida empresa o institución financiera.

6. PREVENCIÓN

- › Si se está viajando y se le debe proporcionar información personal por teléfono a alguien de confianza, hay que asegurarse de que no hay nadie alrededor que puede interceptar la conversación y quedarse con estos datos;
- › Informar a empresas o instituciones financieras que su información personal no debe ser revelada a nadie;
- › Guardar la información importante en archivos y directorios protegidos por contraseña.
- › Encriptar información crítica.

Al utilizar el servicio de correos postal, el usuario debe:

- › Procurar mantener su buzón de correo con una buena cerradura para que sea inaccesible a otras personas;
- › Evitar que el correo se acumule y se llene, permitiendo acceder a él por la de la boca del buzón;
- › Cuando se viaje, pedir a un familiar o amigo que lo recoja o que lo retengan en la oficina de correos más cercana;
- › Controlar la llegada de cartas periódicas o predecibles, que contienen información sobre créditos, débitos, estados de cuentas o facturas;
- › Retirar y enviar desde la oficina de correos si nos es posible, todas las cartas o documentos que contengan información personal;
- › Anular la emisión de correspondencia a lugares donde ya no se vive y solicitar a través de la oficina de correos que redirijan el correo a la dirección actual.

Para realizar transacciones financieras seguras, el usuario debe:

- › Hacer transacciones financieras en línea sólo a través de sitios web seguros con direcciones que empiezan por “https:”;
- › Tener en cuenta que para realizar operaciones de banca online, nunca nos piden más de una parte de los números que figuran en la tarjeta de crédito (normalmente tres);
- › Tener en cuenta que los bancos no piden la instalación de aplicaciones móviles para mejorar la seguridad en sus operaciones, estas aplicaciones son generalmente malware;
- › En caso de duda, contacte con el banco por teléfono;
- › Mantener las aplicaciones como Java y Flash actualizadas;
- › Proteger todas las cuentas bancarias con contraseñas.

6. PREVENCIÓN

Para chatear por Mensajería Instantánea, IRC y chats en línea con seguridad, el usuario debe:

- › Utilizar un nombre falso que no permita su identificación;
- › Usar espacios que tienen un moderador (sólo se aplica a espacios de chat);
- › Mantener en secreto su información personal;
- › Grabar las sesiones de chat;
- › No abrir archivos adjuntos de correo electrónico enviados en las conversaciones de chat.

Para crear una contraseña segura el usuario debe:

- › Evitar secuencias fáciles de predecir al crear una contraseña;
- › Evitar la creación de contraseñas con caracteres del teclado. Además de ser conocidas, estas contraseñas son fácilmente identificables en el momento de escribirlas;
- › Al crear una contraseña no utilizar elementos personales asociados a usted o que se saben otras personas, como la fecha de nacimiento, parte del nombre y apellidos, dirección, número de contribuyente o número de identidad;
- › Utilizar contraseñas con la longitud máxima permitida y tener cuidado de que no formen palabras existentes en el diccionario de lengua portuguesa o en cualquier otro diccionario;
- › Combinar letras, números y símbolos de manera no consecutiva;
- › Ser creativo (por ejemplo pensar en una frase con un significado especial y utilizar la primera letra de cada palabra, en la contraseña);
- › Cambiar entre mayúsculas y minúsculas, y cambiar las letras por números o símbolos;
- › Asignar una contraseña diferente para cada servicio (si existe la necesidad de anotarla, guardar la anotación en un lugar seguro y no en un archivo en su ordenador);
- › Cambiar las contraseñas de manera regular.

NOTA: Los padres o tutores de menores, deben supervisar las actividades que realizan los niños y adolescentes en línea, asegurándose que éstos tomen las precauciones mencionadas anteriormente.

6. PREVENCIÓN

6.2. Signos de infección de Malware

La probabilidad de ser víctima de robo de identidad aumenta si el equipo está infectado por malware. Por lo tanto es importante conocer los síntomas de estar infectado de malware:

- › Lentitud en el equipo;
- › Bloqueos frecuentes del equipo;
- › Aparición de mensajes o imágenes emergentes, sonidos extraños o aplicaciones instaladas sin nuestro consentimiento;
- › Apagado espontáneo de los mecanismos de protección como el antivirus;
- › Incapacidad del sistema de reconocer las vocales acentuadas;
- › La actividad constante e inexplicable en la conexión a Internet;
- › Cambio de página de inicio o del buscador Web favorito;
- › Redirección constante a páginas desconocidas de Internet;
- › Aparición de nuevos sitios favoritos o barra de herramientas en el navegador;
- › Publicación de comentarios en redes sociales;
- › Establecer conversaciones y avisos de mensajería instantánea (Skype, Google Talk, etc.);
- › Devolución de varios correos electrónicos, que el usuario no reconoce haber enviado;
- › Aparición del icono de Java en la barra de tareas, sin que el usuario haya ejecutado ninguna aplicación basada en esta tecnología.

6.3. Como identificar los signos de Robo de identidad

Los efectos de la Robo de identidad pueden ser más perjudiciales si no se detecta pronto. Por lo cual y con el fin de frenar sus efectos, es importante que el usuario conozca las señales que indican que está siendo víctima del robo de identidad. Vamos a ver a continuación algunas estrategias para detectar este fenómeno a tiempo.

Para detectar el robo de identidad a tiempo, el usuario debe:

- › Mantenerse atento a cualquier actividad extraña en su cuenta de correo electrónico y en sus perfiles de las redes sociales;
- › Mantener una vigilancia constante en todas sus cuentas bancarias, cuentas de inver-

6. PREVENCIÓN

sión y tarjetas de crédito;

- › Comprobar que recibe los extractos bancarios mensuales con las últimas operaciones realizadas.
- › Examinar con atención si hay operaciones no realizadas por él;
- › Revisar el informe de sus créditos de manera regular para ver si hay alguna actividad anormal;
- › Suscribirse a las alertas de actividad sospechosa que las entidades financieras ofrecen;
- › Investigar cualquier negativa de crédito, lo cual puede ser una señal de que se ha producido robo de identidad y el uso indebido de sus cuentas;
- › Ponerse en contacto con la institución financiera si no se reciben los recibos mensuales;
- › Si el usuario recibe la información de que sus recibos van a ser enviados a una dirección que no es la suya, debe informar al representante de la institución que este cambio de dirección no lo hemos autorizado y que alguien puede estar haciendo un uso incorrecto de la cuenta. En esta situación es fundamental solicitar copias de todos los recibos y un listado de todas las operaciones realizadas desde el último recibo recibido.

7.

AYUDA A
LAS VICTIMAS

[illegible]

7. AYUDA A LAS VICTIMAS

7.1. Infección por malware

En el caso de estar infectado por malware, el usuario debe:

- › Desconectar el ordenador de la red para que no infecte a otros ordenadores (si es posible);
- › Formatear el ordenador, este formateo puede implicar volver a instalar todo el sistema y puede ser realizado por un especialista o por la víctima en caso de que esta tenga conocimientos suficientes para hacerlo;
- › Desinfectar el ordenador, es decir hacer funcionar la herramienta de limpieza en “modo seguro” o desde una unidad de CD o flash con un antivirus desde un ordenador seguro;
- › Cambiar todas las contraseñas.

7.2. Robo de identidad

Después de haber sido víctima de robo de identidad relacionada con Internet, el usuario tiene que conocer que medios tiene para frenar los efectos de este tipo de delitos y para suavizar el impacto en su vida personal, social y financiera.

En el caso de robo de identidad el usuario debe:

- › Contactar inmediatamente con su entidad financiera;
- › Cancelar todas las tarjetas de crédito, solicitar la expedición de otras nuevas y cambiar todos los códigos PIN por si el delincuente ha tenido acceso a sus cuentas o datos secretos;
- › Cancelar las cuentas a las que crea que el delincuente haya tenido acceso o haya abierto;
- › Cancelar los accesos al banco desde casa y pedir nuevos códigos si cree que el ciberdelincuente puede haber accedido a este servicio;
- › Pedir a la entidad financiera que le proporcione los impresos o formularios necesarios con el fin de probar y negar, ciertas acciones delictivas que se han llevado a cabo por el usuario;
- › Cuando no haya formularios específicos, la víctima debe redactar y enviar una carta al servicio de ayuda a las víctimas de la entidad;
- › Pedir toda la información sobre los créditos, extractos bancarios y las operaciones que no hayan sido llevadas a cabo por la víctima, revisarlos con atención para encontrar posibles errores, e informar a la entidad financiera si se encuentra algún error para

7. AYUDA A LAS VICTIMAS

- impugnar las correspondientes acciones penales;
- › En caso de que el usuario encuentre errores, debe pedir a la entidad financiera que ponga en marcha el dispositivo de alerta por estafa en la tarjeta de crédito;
- › Pedir a la entidad financiera que impida la disponibilidad de los datos contenidos en los informe de crédito;
- › Después del robo de identidad, el usuario debe examinar atentamente en los años posteriores los informes de las tarjetas de crédito;
- › Verificar que no haya deudas de créditos asumidos bajo su identidad ligadas al “Banco de España” en el Centro de Información de Riesgos;
- › Denunciar el delito en la oficina del fiscal general o en la policía;
- › Presentar el recibo de la denuncia ante la entidad financiera;
- › Solicitar sus antecedentes penales y verificar que esta información es correcta;
- › Cambiar la contraseña de su cuenta de correo electrónico por si el delincuente tuviera acceso a esta;
- › Anular los documentos de identidad a los que el delincuente haya tenido acceso;
- › Notificar a los organismos con los que el usuario trabaja, la oficina de correos más cercana a su casa, la Seguridad Social y la oficina de tráfico, del robo de identidad que ha sufrido;
- › Advertir a los posibles empresarios, de que ha sido víctima de robo de identidad, por si reciben información falsa sobre la víctima;
- › Guardar todos los correos electrónicos, sms, cartas, o cualquier otro registro de la comunicación mantenida entre el usuario y el sospechoso o entre el usuario y las entidades financieras, que se puedan utilizar como pruebas si fuese necesario.

En el caso de robo de identidad y calumnias a través de la red social Facebook, el usuario debe:

1. Si el autor ha creado un perfil falso de la víctima para publicar calumnias sobre esta, la víctima procederá como indicamos más abajo con el uso de Facebook:
 - › Informar sobre esta nueva cuenta y con este objetivo la victima debe:
 - » Hacer clic en la opción de “Mensaje” en la esquina superior derecha de la cuenta;
 - » Aparecerán cuatro opciones y se debe seleccionar la opción “Denunciar”;
 - » A continuación, seleccione la opción “Denunciar esta cuenta”;
 - » Se mostrará el mensaje ¿Qué problema hay con en esta cuenta? Después se debe hacer clic en la opción “Esta cuenta se hace pasar por mí o alguien que conozco”;

7. AYUDA A LAS VÍCTIMAS

- » Entonces aparecerá en la pantalla la pregunta “¿Quién finge ser?” A lo que la víctima debe hacer clic en “yo”;
- » El siguiente mensaje aparecerá “Basado en lo que se ha elegido, aquí hay algunas cosas que puede hacer.” y luego el usuario debe seleccionar la opción “Enviar a Facebook para su revisión”;
- » Finalmente él usuario debe hacer clic en la opción “hecho”.

› Para informar del contenido publicado, la víctima debe:

- » Hacer clic en la flecha que indica hacia abajo situada en la esquina superior derecha y seleccionar la opción “No me gusta esta publicación”.

2. Si el infractor crea una página falsa con el nombre de la víctima para publicar contenido difamatorio:

› Para informar sobre la página y el contenido publicado en ella, la víctima debe:

- » Hacer clic en la opción de “Mensaje” en la esquina superior derecha de la cuenta;
- » Veremos cinco opciones y la víctima debe seleccionar la opción “Informe sobre página”;
- » Después la víctima debe seleccionar la opción “me están molestando a mi o a alguien que conozco”;
- » Aparece el mensaje: “sentimos que tengas que sufrir esta experiencia: Aquí verás algunas opciones que puedes hacer para tratar de solucionar esto”. Después se debe seleccionar la opción “Enviar a Facebook para su revisión”;
- » Finalmente el usuario debe hacer clic en la opción “hecho”.

3. Si el ofensor hizo uso del perfil de la víctima para publicar contenido difamatorio:

› Cambie la clave de acceso, para poder hacer esto la víctima debe:

- » Hacer clic en el icono con un candado en la esquina superior derecha de la barra azul en la parte superior de la página;
- » A continuación, seleccione la opción “Ver más ajustes”;
- » Posteriormente la víctima debe hacer clic en la opción “General” en la esquina superior izquierda de la página;
- » A continuación nos lleva a la pantalla de ajustes de la cuenta «general» y en esta

7. AYUDA A LAS VÍCTIMAS

- » pantalla la víctima debe hacer clic en la opción “Contraseña” y después en “Editar”;
- » Después de esto la víctima debe introducir su contraseña antigua y escribir una nueva dos veces;
- » A continuación la víctima debe hacer clic en la opción “Guardar cambios”;
- » El siguiente mensaje que aparecerá es «Su contraseña ha sido cambiada. La víctima debe hacer clic en la opción «Cerrar sesión en otros dispositivos»;
- » Por último la víctima debe hacer clic en “Enviar”.

› Para eliminar el contenido publicado la víctima debe:

- » Hacer clic en la flecha que apunta hacia abajo en la esquina superior derecha de la página de entrada y seleccionar la opción “Borrar”;
- » A continuación nos aparecerá el siguiente mensaje ¿Seguro que quieres borrar esto? y la víctima debe seleccionar de nuevo la opción “Borrar”.

4. En todo caso:

- › Bloquear al ofensor para que deje de tener acceso a la cuenta de la víctima, así como a las cuentas de todos los usuarios molestos en Facebook;
- › Para ello la víctima debe:
 - » Hacer clic en la opción “Mensaje” en la esquina de la parte superior derecha del perfil del usuario que quiere bloquear;
 - » Aparecen cuatro opciones y debe seleccionar la opción “Bloquear”;
 - » A continuación aparece el mensaje “¿estás seguro que lo quieres bloquear...?” y después la víctima tiene que seleccionar la opción “Confirmar”.
- › Presentar un informe en la oficina del fiscal general o en la policía.

ANEXOS

[illegible]

ANEXOS

Glosario

Bots y botnets – La expresión Bots es una forma abreviada para robots. Los delincuentes que distribuyen software maliciosos (malware) pueden convertir el ordenador del usuario en un bot (robot) o también suelen llamarse zombi. Cuando ocurre esto, el equipo del usuario puede ejecutar tareas automatizadas a través de Internet sin su conocimiento. Los delincuentes suelen utilizar los robots para infectar un gran número de equipos. Estos equipos forman una red o una red de bots. Los delincuentes usan botnets para enviar spam, distribuir virus, atacar a otros ordenadores y servidores, y cometer otros tipos de delitos y fraudes. Si el ordenador del usuario se convierte en parte de una botnet, puede hacerse muy lento y el usuario puede estar ayudando a delincuentes aunque él lo desconozca;

Navegador – Programa para acceder a Internet que ya viene instalado en el equipo;

Chat – Conversación en línea;

Cookies – Una cookie es un archivo creado por un sitio web para almacenar información del equipo del usuario, incluyendo sus preferencias al visitar ese sitio. Al entrar a un sitio que usa cookies, el sitio podrá solicitar al navegador instalado en el ordenador, ejecutar una o más cookies en el disco duro del ordenador del usuario. Después, al regresar a este sitio, el navegador enviará las cookies que pertenecen a ese sitio. Esto permite al sitio presentar información personalizada a las necesidades de sus usuarios. Hay cookies que crean sitios web en los que el usuario no tiene la necesidad de introducir su contraseña al entrar en el mismo sitio por segunda vez. Otros sitios utilizan cookies para almacenar las preferencias de los usuarios;

Datos informáticos – Cualquier representación, información o conceptos en una forma adecuada para procesar en un sistema informático, incluido un programa que haga al sistema informático realizar una función. La definición de “sistema informático” según el ECCC cubre todas las formas de tecnología que van más allá de los sistemas informáticos tradicionales de ordenador de sobre mesa, como los modernos teléfonos móviles, teléfonos inteligentes, PDAs, tabletas o similares;

Sistema informático – Todo dispositivo o conjunto de dispositivos interconectados o relacionados, uno o más de los cuales, en virtud de un programa permiten el tratamiento automático de datos;

Descargar – Transferencia de contenido de Internet al equipo del usuario;

E-mail – Mensaje de correo electrónico;

Flash – Archivos generados por Adobe Flash Player, que es un tipo de software utilizado para crear animaciones interactivas;

Java – Lenguaje de programación;

Link – Enlace a un sitio Web;

Iniciar Sesión – Proceso por el cual se accede a un sistema informático que se controla a través de la identificación y autenticación del Usuario, usando las credenciales suministradas por ese mismo usuario;

ANEXOS

Malware – Abreviatura de software malicioso, es un software diseñado para infiltrarse de manera ilegal en un sistema informático ajeno con la intención de causar daños, cambios, o robar información (confidencial o no). Los virus informáticos, gusanos y software espía se consideran malware;

Pop-ups – Ventana nueva que se abre en el navegador al entrar en una página web o abriendo un enlace específico;

Limpieza remota – Una función de seguridad que permite a un administrador de red o propietario del dispositivo, enviar una orden a un dispositivo informático y eliminar datos;

Servidor – Entidad pública o privada que ofrece a los usuarios de su servicio la capacidad de comunicarse por medio de un sistema informático. También es cualquier otra entidad que procesa o almacena los datos informáticos en nombre de dicho servidor de comunicación o de los usuarios de dicho servicio;

Robo – El robo, es una situación en la que una persona o programa se hace pasar con éxito por otro, falsificando sus datos y obteniendo con ello beneficios de manera ilegítima;

Spyware – Programa informático automático que recoge y almacena información sobre el usuario y sus hábitos en Internet, y transmite esta información a una organización extranjera en Internet sin el conocimiento ni consentimiento del usuario. Por un lado, el spyware puede ser desarrollado por empresas que deseen monitorizar los hábitos de usuarios y anunciarse a estos usuarios adaptando los anuncios a sus intereses, con el objetivo de vender sus productos a través de Internet. Por otro lado, muchos de los virus llevan spyware que tiene la intención de robar datos confidenciales de los usuarios, como sus datos bancarios;

Datos de tráfico – Cualquier dato informático relativo a la comunicación por medio de un sistema informático, generado por un sistema informático que formaba parte de la cadena de comunicación, indicando el origen de la comunicación, el destino, la ruta, la hora, fecha, tamaño, duración o tipo de servicio subyacente;

Página web/Sitio – Ubicación / correspondiente a la página de Internet o página Web;

Wi-Fi – Conexión inalámbrica a Internet;

World Wide Web/WWW/Web – Es un sistema de documentos hipertexto que están interconectados y vinculados que se ejecutan en Internet.

ANEXOS

Números de ayuda al usuario y contacto de las entidades Bancarias en España

BANCO DE DEPOSITOS

914 352 018
atencioncliente@bancodepositos.com

ALLFUNDS BANK

atencionalcliente@allfundsbank.com

DEUTSCHE BANK

atencion.clientes@db.com

SANTANDER INVESTMENT

SANTANDER SECURITIES SERVICES

BANCO SANTANDER

OPEN BANK

SANTANDER CONSUMER FINANCE

912 573 080
atenclie@gruposantander.com

BANCO DEPOSITARIO BBVA

BANCO INDUSTRIAL DE BILBAO

BANCO OCCIDENTAL

BBVA BANCO DE FINANCIACION

BANCO DE PROMOCION DE NEGOCIOS

BANCO BILBAO VIZCAYA ARGENTARIA

UNOE BANK

servicioatencioncliente@grupobbva.com

BNP PARIBAS ESPAÑA

atencioncliente@bnpparibas.com

BANCO DE MADRID

sac@bancomadrid.com

BANCA MARCH

atencion_cliente@bancamarch.es

GRUPO BANCO POPULAR ESPAÑOL

BANCO POPULAR

POPULAR BANCA PRIVADA

BANCO PASTOR

atencionclientes@bancopopular.es

BANCA PUEYO

bancapueyo@bancapueyo.es

BANCO DE SABADELL

sac@bancsabadell.com

RENTA 4 BANCO

913 848 500
defensor@renta4.es

ANEXOS

RBC INVESTOR SERVICES ESPAÑA
913609900
servicio.es@rbc.com

BANCO DE CASTILLA-LA MANCHA
942 204 533
atencionalcliente@liberbank.es

CITIBANK ESPAÑA
reclamaciones.clientes@citigroup.com

BANCOFAR
913 193 448
atencionalcliente@bancocaminos.es

BANKINTER
900 802 081
incidencias_sac.bankinter@bankinter.es

BANCO CAIXA GERAL
913 099 037
serviciodeatencionalcliente@bancocaixageral.es

NUEVO MICRO BANK
CAIXABANK
CAIXABANK ELECTRONIC MONEY
934 046 379
servicio.cliente@lacaixa.es

ARESBANK
913 149 595
atencioncliente@aresbank.es

BANKOA
servicioatencioncliente@bankoa.es

BANCO EUROPEO DE FINANZAS
atencioncliente@bef.es

BANCO MEDIOLANUM
932 535 400
servicio.defensa.cliente@mediolanum.es

BANCO ALCALA
atencionalcliente@bancoalcala.com

BANCO COOPERATIVO ESPAÑOL
915 956 700
a.c.banco_cooperativo_bce@cajarural.com

PRIVAT BANK DEGROOF
932 535 400
atencion.cliente@privatbank.es

EBN BANCO DE NEGOCIOS
atencioncliente@ebnbanco.com

TARGOBANK
atencionaclientes@targobank.es

BANQUE MAROCAINE DU COMMERCE EXTERIEUR INTERNATIONAL
915 756 800
atencion-al-cliente@bmce-intl.com

ANEXOS

BANCO FINANTIA SOFINLOC

atencionalcliente@finantia.com

SANTANDER CONSUMER FINANCE

912 573 080

atenclie@gruposantander.com

BANCO CETELEM

serviciodereclamaciones@cetelem.es

UBS BANK

departamento.atencion-cliente@ubs.com

DEXIA SABADELL

reclamaciones@dexiasabadell.com

BANCO INVERDIS

reclamaciones@inverdis.com

BANCO CAMINOS

913 193 448

atencionalcliente@bancocaminos.es

BANCO PICHINCHA ESPAÑA

atencionalcliente@bancopichincha.es

CAJASUR BANCO

atencion.cliente@kutxabank.es

EVO BANCO

atencioncliente@evobanco.com

BANCO DE CREDITO SOCIAL COOPERATIVO

CAJA DE CREDITO DE PETREL

CAIXA RURAL ALTEA

CAJAS RURALES UNIDAS

CAJA RURAL SAN ROQUE DE ALMENARA

CAIXA RURAL SANT VICENT FERRER DE LA VALL D'UIXO

CAIXA RURAL DE CALLOSA D'EN SARRIA

CAJA RURAL CATOLICO AGRARIA

CAJA RURAL SAN JOSE DE BURRIANA

CAIXA RURAL TORRENT

CAJA RURAL SAN JAIME DE ALQUERIAS NIÑO PERDIDO

CAJA RURAL DE CHESTE

CAIXA RURAL DE TURIS

CAJA RURAL SAN JOSE DE NULES

CAJA RURAL DE VILLAR

CAJA RURAL LA JUNQUERA DE CHILCHES

CAIXA RURAL SANT JOSEP DE VILAVELLA

CAJA RURAL DE ALGINET

CAIXA RURAL ALBALAT DELS SORELLS

servicioatencioncliente@grupocooperativocajamar.es

BANCO MARE NOSTRUM

quejasyreclamaciones@grupobmn.com

SELF TRADE BANK

902 888 777

reclamaciones@selfbank.es

ANDBANK ESPAÑA

cumplimiento.esp@andbank.com

ANEXOS

CECABANK
915 965 519
servicioatencionalcliente@ceca.es

CATALUNYA BANC
atencioncliente@catalunyacaixa.com

BANKIA
913 792 590
atencionalcliente@bankia.com

LIBERBANK
942 204 533
atencionalcliente@liberbank.es

ABANCA CORPORACION BANCARIA
atencioncliente@abanca.com

IBERCAJA BANCO
976 767 643
976 767 693
atencioncliente@ibercaja.es

KUTXABANK
944 017 124
atencion.cliente@kutxabank.es

UNICAJA BANCO
952 138 016
atencion.al.cliente@unicaja.es

BANCO DE CAJA ESPAÑA DE INVERSIONES
atencion.cliente@cajaespana.es

CAJA DE AHORROS Y MONTE DE PIEDAD DE ONTINYENT
962 919 113
defensor.clientes@caixaontinyent.es

COLONYA
902 104 293
sac@colonya.es

CAJA RURAL DE ALMENDRALEJO
924 670 371
atencioncliente@cajalمندralejo.com

CAJA RURAL CENTRAL
966 747 851
atencionclientes@ruralcentral.es

CAJA RURAL DE GIJON
985 180 400
atencion_cliente_crgijon@cajarural.com

CAJA RURAL DE NAVARRA
buzon.crnavaarra@cajarural.com

CAJA RURAL DE EXTREMADURA
924 207 474
atencioncliente_crext@cajarural.com

ANEXOS

CAJA RURAL DE SALAMANCA

923 128 609

atencionalcliente.3016@cajarural.com

CAJA RURAL DE SORIA

975 212 840

atencioncliente.soria@cajarural.com

CAJA RURAL REGIONAL SAN AGUSTIN FUENTE ALAMO MURCIA

968 597 211

atencioncliente@ruralregional.com

CAJA RURAL DE UTRERA

clientes.utrera@cajarural.com

CAJA RURAL DE GRANADA

atencioncliente.crg@cajarural.com

CAIXA DE CREDIT DELS ENGINYERS

900 302 514

serviciosocio@caja-ingenieros.es

CAJA LABORAL POPULAR

servicio.de.atencion.al.cliente@laboralkutxa.com

CAJA RURAL DE ASTURIAS

985 984 542

departamentoatencioncliente_crasturias@cajarural.com

CAJA RURAL DE BURGOS

atencioncliente_3060@cajarural.com

CAJA RURAL DE JAEN

900 103 180

attcliente.jaen@cajarural.com

CAIXA RURAL GALEGA

caixa.ruralgalega@cajarural.com

CAJASIETE

922 243 156

cajasiete_sac@cajasiete.com

RURAL TERUEL

978 617 100

crteruel_defensa_cliente@cajarural.com

CAJA RURAL DE CASTILLA-LA MANCHA

atencionalcliente@cajaruralclm.es

CAJA RURAL DE ZAMORA

980 532 671

atcliente.zamora@cajarural.com

CAJA RURAL DE BAENA NTRA. SRA. DE GUADALUPE

957 670 637

baena@cajarural.com

CAIXA RURAL DE L'ALCUDIA

962 540 166

cliente_cralcudia@cajarural.com

ANEXOS

CAJA RURAL NTRA. SRA. DEL ROSARIO
957 678 228
nuevacarteya@cajarural.com

CAJA RURAL DE CANETE DE LAS TORRES NTRA.SRA.DEL CAMPO
957 183 031
canetedelastorres@cajarural.com

CAIXA RURAL LA VALL 'SAN ISIDRO'
atencioncliente.3111@caixalavall.com

CAJA RURAL SAN JOSE DE ALCORA
964 360 976
sac.alcora@cajarural.com

CAJA RURAL 'NUESTRA MADRE DEL SOL'
957 166 028
madresol@cajarural.com

CAIXA RURAL D'ALGEMESI
962 488 030
atencioncliente.3117@cajarural.com

CAJA RURAL DE CASAS IBÁÑEZ
967 460 312
casaibanez.3127@cajarural.com

CAJA RURAL SAN JOSE DE ALMASSORA
964 560 003
jreball@caixalmassora.es

CAJA RURAL NUESTRA SEÑORA DE LA ESPERANZA DE ONDA
964 776 677
sac@caixaonda.com

CAJA RURAL DE BETXI
964 623 003
sac.betxi@cajarural.com

CAJA RURAL DE GUISSONA
973 551 200
atencio.client.caixaguissona@cag.es

CAJA RURAL DE VILLAMALEA
967 483 026
villamalea@cajarural.com

CAJA DE CREDITO COOPERATIVO
916 926 153
sac@novanca.com

CAJA RURAL DE ALBAL
961 260 075
atencion_cliente.albal@cajarural.com

CAIXA POPULAR-CAIXA RURAL
961 318 282
atencion-al-cliente-de-caixapopular@cajarural.com

CAIXA RURAL LES COVES DE VINROMA
964 426 050
atencióncliente@caixacoves.es

ANEXOS

CAIXA RURAL VINAROS

964 407 280

aredo.vinaros@cajarural.com

CAJA DE ARQUITECTOS

934 826 810

atencionalcliente@arquia.es

CAJA RURAL DEL SUR

atencionalcliente_crsur@cajarural.com

CAJA RURAL DE ALBACETE

967 228 217

servicioatencioncliente@globalcaja.es

CAJA RURAL DE ARAGON

976 763 300

atencionalcliente@nuevacajaragon.es

E. KUANTIA EDE

sac@ekuantia.es

MOMOPOCKET

902 730 506

atencionalcliente@momopocket.com

[illegible]

[illegible]

0101Proyecto implementado conjuntamente por:111101010101010101000010101001010101



**PÄRNU CENTRE
FOR GENDER
BASED VIOLENCE**



 Procuradoria-Geral da República

```

0101> Associação Portuguesa de Apoio à Vítima101010101010000101010010101010010101
1010 [Portuguese Association for Victim Support]00000101010101010001111101010101
1111> Fiscalía General del Estado de España - Unidad Especializada contra la10100
0101 criminalidad informática111110101010101010100001010100101010100101010010000
1010 [Spanish General Prosecutor's Office - Cybercrime Specialized Unit]010101010
1010> Politia Romana00101010100101010010000110010101101010101001010101000000101
1010 [General Inspectorate of the Romanian Police]101010101001010100100001100101
1000> Pärnu Lähisuhtevägivalla Ennetuskeskus- Varjupaik10101001010100100001101010
0101 [Pärnu's Centre of Gender Based Violence - Estonia]10101010000001010101010
0010> Polícia Judiciária00101010101010001111101010101010100001010100101010101
0010 [Portuguese Judiciary Police]101101010101001010101010101010101000010101001010
0101> Procuradoria Geral da República110101010100101010101000000101010101000111
0101 [Portuguese General Prosecutor's Office]010101010010000110010101101010101001

```

ISBN 978-972-8852-71-9

Sólo está permitida la cita y /o reproducción total o parcial de la presente obra con fines exclusivamente informativos y con cita expresa de la fuente. Esta publicación es responsabilidad exclusiva de su autor y la Comisión Europea no se hace responsable del uso que pueda hacerse de la información contenida en el mismo.

Proyecto promovido por la Asociación Portuguesa de Apoyo a las Víctimas y co-financiado por la Prevención y Lucha contra el Crimen. Programa de la Unión Europea.