E.M. nº 77 Mayo-Agosto 2024

UN ANÁLISIS JURÍDICO-ECONÓMICO DE ESTAFAS EN ENTIDADES DE CRÉDITO

Cristina González Cáceres
Graduada en Economía y en Derecho por la URJC. Colaboradora de GESCE-URJC.

RESUMEN

El objetivo de este análisis es examinar las implicaciones jurídico-económicas de las estafas realizadas mediante la apertura de financiaciones fraudulentas en entidades de crédito a particulares. A medida que la digitalización de los servicios financieros aumenta, también lo hace la prevalencia de los delitos cibernéticos que buscan explotar las vulnerabilidades del ser humano y de un sistema bancario, cada vez más digitalizado que interpone procesos de adquisición semi-inmediata de créditos a disposición de los clientes. Este estudio se justifica por la necesidad de adaptar las respuestas legales a los nuevos métodos de fraude y proporcionar un marco que pueda servir para prevenir futuras vulnerabilidades en el sector.

1. INTRODUCCIÓN

La digitalización de los servicios financieros y sus instrumentos (Sánchez-Bayón y García-Ramos, 2021) ha transformado la forma en que interactuamos con el dinero, facilitando transacciones más rápidas y accesibles a escala global, cambiando nuestro paradigma financiero (Sánchez-Bayón, 2020a-b y 2021). Sin embargo, este avance ha venido acompañado de un incremento en los delitos cibernéticos, exponiendo tanto a consumidores como a instituciones financieras a nuevos riesgos y vulnerabilidades. La sofisticación y prevalencia de estos delitos han evolucionado, desafiando las medidas de seguridad existentes y demandando enfoques legales innovadores para su control y mitigación. Según la empresa de seguridad Avast, el 33% de los españoles ha experimentado al menos una vez algún tipo de estafa informática (penada en el art. 248.2 del Código Penal). Esto incluye, por ejemplo, recibir un SMS o correo electrónico sospechoso, sufrir el robo de una tarjeta de crédito cuyos detalles se han utilizado posteriormente, o ser víctima de suplantación de identidad, entre otros incidentes fraudulentos. El fraude en el derecho penal español abarca comportamientos que buscan engañar a la víctima para obtener un beneficio patrimonial, resultando en un perjuicio para el sujeto pasivo.

Con el desarrollo de las nuevas tecnologías, especialmente Internet, los delitos de fraude informático han aumentado significativamente. Por ello, impulsaron a la reforma del artículo 248 del Código Penal, ya que el fraude tradicionalmente requiere un engaño, pero un ordenador, como máquina que es, no puede ser engañado en el sentido convencional. Esta paradoja llevó a la necesidad de adaptar la legislación para abordar la realidad de los fraudes informáticos, que operan de manera diferente a los fraudes tradicionales. En respuesta, el legislador español introdujo el fraude informático en el artículo 248.2.a) del Código Penal en 1995, reconociendo la necesidad de una figura legal que se ajustara a los nuevos contextos tecnológicos donde el engaño convencional no es un componente. En los fraudes informáticos, el daño ocurre en el momento en que el sistema es manipulado por el autor, y no hay un proceso de engaño a una persona, sino una alteración directa del sistema informático.

El problema central que aborda esta investigación es la eficacia de la legislación actual para enfrentar y mitigar los delitos cibernéticos en el sector financiero. Por ejemplo, se analiza cómo las leyes

actuales pueden estar desactualizadas frente a las técnicas modernas de fraude y estafa online, y qué modificaciones serían necesarias para fortalecer el marco legal y proteger mejor tanto a los consumidores como al sistema financiero, centrándonos en los cargos fraudulentos en tarjetas y líneas de crédito y la apertura de financiaciones fraudulentas. A su vez, se analizarán los modos que tienen las víctimas de reclamar a las entidades de crédito, así como el amparo que les brinda el Banco de España.

Este estudio es fundamental en el contexto actual dado que la seguridad financiera y la protección de datos personales son de máxima prioridad para garantizar la confianza en el sistema financiero digital. Una legislación robusta y actualizada no solo ayudará a prevenir el fraude y la estafa, sino que también asegurará la estabilidad y la integridad de los mercados financieros, promoviendo un entorno seguro para la innovación y el crecimiento económico.

La metodología empleada para realizar este análisis jurídico-económico incluye una revisión exhaustiva de la legislación actual, estudios de casos de estafas informáticas recientes y un análisis de las Memorias de Reclamaciones de Banco de España más recientes, para comparar el incremento experimentado en la actualidad de reclamaciones de dicha tipología. Además, se realizará un análisis comparativo de enfoques legislativos en diferentes jurisdicciones para identificar mejores prácticas y recomendaciones efectivas que puedan ser adaptadas al contexto nacional. Este enfoque multidisciplinario garantiza una comprensión profunda de los desafíos y soluciones posibles en la materia.

2. MARCOS TEÓRICOS Y METODOLÓGICOS

Este estudio parte de una revisión de bases científico-académicas (v.g. Scopus, Dialnet, Academia, ResearchGate), literatura gris o profesional (de consultoras, entidades financieras y banca central, sobre todo), más el programa de investigación desarrollado por el grupo de investigación GESCE-URJC[1].

Es necesario comenzar definiendo los siguientes conceptos teóricos. En primer término hemos de especificar que es un delito: toda acción típica, antijurídica y culpable. Hablamos de acción haciendo referencia a toda conducta antijurídica, humana, voluntaria y externa. El carácter de típico se lo da el hecho de estar penada en una norma.

Concretamente, la estafa informática, es aquella que a través de medios informáticos, vulnera algún bien jurídico protegido (patrimonio).

El Dr. Terragni ha definido al delito informático como "toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor, aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la ley, que se realiza en el entorno informático y esté sancionado con una pena".

En el caso concreto de las estafas informáticas son una modalidad del tipo básico de estafa (art. 248 CP). Se produce el tipo básico cuando el que "con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno." Pese a que autores como SUÁREZ GONZÁLEZ indican que la relación entre ambas estafas es mínima, indica que lo correcto hubiera sido establecer una figura autónoma en lugar de incluirlo como un subtipo. En la legislación actual la estafa informática aparece tipificada en el art. 249.1 CP, incluyendo por tanto los casos en que, a) "los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática

[1] Grupo de investigación consolidado para el Estudio y seguimiento del ciclo económico de la Universidad Rey Juan Carlos (https://gestion2.urjc.es/pdi/grupos-investigacion/gesce).

o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) "Los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero."

Los requisitos principales para que este se produzca serán el ánimo de lucro del sujeto activo, el engaño bastante al sujeto pasivo a través de la manipulación informática, el acto de disposición realizado por el sujeto pasivo y el detrimento patrimonial como resultado de la acción. Esta nueva categoría fue introducida por razones político-criminales para paliar un vacío legal presente cuando mediaba la manipulación informática. Anteriormente, la defraudación de este tipo no encajaba dentro de las categorías de estafa, ni podía clasificarse como hurto o apropiación indebida. Adicionalmente, la Ley Orgánica 15/2003, del 25 de noviembre, añadió un tercer párrafo que aborda directamente el fraude informático, regulando los actos preparatorios relacionados. En lo que respecta al fraude informático, resulta excesivo atribuir a esta categoría cualquier perjuicio patrimonial que involucre manipulación informática, limitando su aplicación a las defraudaciones patrimoniales realizadas mediante medios informáticos. Estas se presentan principalmente de dos maneras: estafas realizadas a través de manipulaciones informáticas y conductas ilícitas o abusivas con tarjetas utilizadas en cajeros automáticos.

La manipulación informática puede entrar en concurso con el delito de daños según el artículo 264.2 del Código Penal español, especialmente en situaciones donde se destruyen o alteran datos dentro de un sistema informático. Además, en circunstancias de falsedad documental, el fraude informático puede entrar en concurso ideal con este delito, dado que el artículo 26 del Código Penal equipara el soporte material que contiene datos a un documento.

Por otro lado, en el caso del empleo y la utilización de información sensible por parte de terceros pueden entrar en conflicto el Reglamento General de Protección de Datos (GDPR) a nivel de la UE, y concretamente a nivel de España la Ley Orgánica 3/2018, de Protección de Datos y garantía de los derechos digitales (LOPDGDD). España, impone requisitos estrictos sobre consentimiento, transparencia, y la seguridad de los datos personales, asegurando que los individuos tengan control sobre sus datos personales. Además, la ley establece sanciones significativas para las violaciones, lo que refuerza la importancia de cumplir con las normativas de protección de datos.

En el contexto de las estafas informáticas y fraudes, cualquier acceso no autorizado o uso indebido de datos personales que contravenga estas normas puede llevar a acciones legales contra las entidades o sujetos responsables.

A su vez, en el caso de estafas que impliquen transacciones financieras fraudulentas, pueden intervenir otras normativas como la Ley 16/2009, de Servicios de Pago, que regula los servicios de pago y la realización de transferencias dentro del sistema financiero español. Esta ley se ocupa de establecer un marco para la seguridad y la eficacia de los pagos, incluyendo disposiciones específicas sobre la autorización y ejecución de transacciones, así como la protección frente a operaciones no autorizadas.

A través de las leyes vigentes en España, el análisis de la jurisprudencia y el análisis de las conductas y precauciones que toman las entidades de crédito en la actualidad, se evaluarán en cuanto a eficacia, y por otro lado, se examinará a nivel de responsabilidad, cuando la toman los bancos y cuando los usuarios afectados, que incurran en negligencia grave.

3. ANÁLISIS JURÍDICO-ECONÓMICO

Se aplica aquí el análisis jurídico tradicional (de estudio regulatorio) y neoinstitucional (de Análisis Económico del Derecho, Elección Pública, Economía Constitucional, etc., Sánchez-Bayón, 2022a-b). Se ha tomado como referencia las herramientas combinadas para el análisis de fenómenos y

figuras sociales usadas por GESCE-URJC (Sánchez-Bayón, 2023a-c y 2024; Sánchez-Bayón et al, 2023).

3.1. Tipología de las estafas por financiaciones fraudulentas y métodos de comisión del fraude

Las estafas en financiaciones fraudulentas pueden clasificarse en función de cómo se obtiene y se utiliza la información personal de la víctima y el método específico empleado en el fraude.

El hackeo de bases de datos es una técnica común donde los atacantes acceden ilegalmente a sistemas de entidades financieras y otras organizaciones para robar datos personales. Esta información robada puede incluir cuentas bancarias, contraseñas, números de identificación, entre otros, que luego se utilizan para cometer fraudes. Otra técnica prevalente es el phishing, que utiliza correos electrónicos fraudulentos para redirigir a sitios web falsos que recopilan información personal. Una variante es el smishing, donde los ataques se realizan mediante mensajes SMS engañosos que aparentan ser de fuentes legítimas y contienen enlaces a páginas fraudulentas.

El vishing se basa en engaños telefónicos para obtener información confidencial, donde los estafadores se hacen pasar por representantes de instituciones legítimas. Los ataques "Man in the middle" (MitM) implican la intercepción de comunicaciones entre dos partes sin que estas lo sepan, permitiendo al atacante robar o alterar datos. El malware y el spyware son programas maliciosos diseñados para infiltrarse en sistemas y robar información. El keylogging es una técnica que registra las pulsaciones de teclado para capturar datos ingresados por el usuario, como contraseñas y datos de tarjetas de crédito.

La ingeniería social implica la manipulación psicológica para engañar a las personas y obtener acceso a información confidencial o sistemas protegidos. En el sector financiero, este método puede incluir estafas en portales de alquiler y compraventa de pisos, donde los delincuentes publican anuncios falsos para obtener datos sensibles de las víctimas.

En la era digital, la obtención de préstamos y financiaciones se ha vuelto más accesible, permitiendo a los delincuentes aprovechar esta facilidad para cometer fraudes. Las estafas pueden involucrar la creación de identidades falsas o el uso de documentos robados para abrir préstamos. Un método común es la usurpación de identidad, donde los estafadores utilizan los datos personales de una víctima, obtenidos a través de engaños, para solicitar préstamos a su nombre. Las estafas de manipulación de solicitudes implican la alteración de información en las solicitudes de crédito para obtener mejores condiciones o cantidades de crédito más altas.

Las estafas de insolvencia planificada se producen cuando un solicitante de crédito tiene la intención de declararse insolvente poco después de recibir el préstamo, acumulando deudas que luego no pagará. Estas acciones son favorecidas por la Ley de la Segunda Oportunidad de 2015, que permite la cancelación de deudas impagables bajo ciertas condiciones. También existen estafas de complicidad interna, donde empleados corruptos dentro de instituciones financieras facilitan la aprobación de créditos fraudulentos a cambio de una cuantía económica.

3.2. Análisis de la legislación vigente

A. El tipo básico de estafa

En relación con el tipo penal de estafa, el actual Código Penal mantiene la estructura establecida por la reforma de 1983, definiendo una serie de elementos necesarios para determinar la existencia del delito. La definición más clara y aún vigente sobre la estafa la ofrece Antón Oneca[2], quien describe el delito como "*la conducta engañosa, con ánimo de lucro injusto, propio o ajeno, que, determinando un*

[2] Nueva Enciclopedia Jurídica. Editorial Francisco Seix, Estafa, t. IX, 1958.

error en una o varias personas, les induce a realizar un acto de disposición, a consecuencia del cual se produce un perjuicio en su patrimonio o en el de un tercero". Esta definición se alinea estrechamente con lo estipulado en el artículo 248.1 del Código Penal, que define la estafa como el acto de quienes, con ánimo de lucro, emplean engaño suficiente para provocar error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno. Para que se configure el delito de estafa según nuestro Código Penal, deben concurrir una serie de elementos esenciales, establecidos por el Tribunal Supremo en reiterada jurisprudencia, siendo muy ilustrativa la Sentencia núm. 187/2002 de 8 de febrero de la Sala Segunda de lo Penal[3].

Esta jurisprudencia enumera los siguientes elementos configuradores del delito de estafa: un engaño previo o concurrente que actúe como esencia de la estafa, suficiente y proporcional para conseguir los fines propuestos; un error esencial inducido en el sujeto pasivo que actúe bajo falsas premisas; un acto de disposición patrimonial que resulte en un perjuicio económico, ya sea por entrega directa de bienes o por movimientos contables que impacten negativamente en el patrimonio; un ánimo de lucro que motive al estafador a obtener un beneficio económico correlativo al perjuicio causado; y un nexo causal claro entre el engaño y el perjuicio, donde el engaño motive el error que a su vez cause el perjuicio patrimonial en la víctima. Estos componentes son fundamentales para la adjudicación de responsabilidades y la aplicación de las sanciones correspondientes dentro del marco legal español.

B. Las estafas informáticas y sus elementos

Las estafas informáticas son una variante del delito de estafa básico recogido en el artículo 248 del Código Penal, surgidas por la necesidad de adaptación a las nuevas tecnologías, así como el surgimiento de nuevos tipos y variantes de delitos. Estas están recogidas en el artículo 249 del Código Penal y se definen por el uso de tecnologías de la información y su regulación legal responde a la necesidad de los legisladores de gestionar los riesgos que las nuevas tecnologías plantean en la comisión de delitos. Las tecnologías modernas proporcionan un mayor anonimato a los delincuentes y les permiten acceder a un gran número de víctimas potenciales. Recientemente, han sido objeto de una actualización legislativa mediante la Ley Orgánica 14/2022, que entró en vigor el 12 de enero de 2023, siguiendo una reforma significativa previa realizada por la Ley Orgánica 1/2015.

En otros de los casos anteriormente mencionados podríamos hallarnos ante un concurso de delitos entre el de estafa informática y el de falsificación de documentos (artículos 390 y 392 del Código Penal) cuando en el proceso de solicitar financiación se utilizan documentos falsificados, como una nómina o una factura de luz alterada, o con el delito de descubrimiento y revelación de secretos (artículo 197 del Código Penal). Este, podría considerarse si se accede ilegalmente a información personal como DNI y nóminas sin autorización.

[3] La *Sentencia 187/2002 de 8 de febrero de la Sala Segunda de lo Penal*, establece de manera detallada los elementos que configuran el delito de estafa, señalando como esencial el engaño previo o concurrente que actúa como columna vertebral y elemento central del delito, originado del ingenio engañoso destinado a aprovecharse del patrimonio de otros. Este engaño debe ser significativo, es decir, debe poseer la suficiencia y proporcionalidad necesarias para alcanzar los objetivos deseados, manifestándose en diversas formas que deben ser lo suficientemente serias y convincentes para funcionar como un estímulo efectivo para el traspaso de propiedad en el ámbito social. Este análisis debe considerar tanto criterios objetivos como las circunstancias particulares del individuo afectado y las del caso específico. Además, el engaño debe inducir un error crítico en la víctima, quien actúa bajo una falsa comprensión de la realidad, llevando a una decisión viciada que resulta en una disposición patrimonial. Tal acto de disposición debe llevar directamente a un perjuicio económico para la persona que lo realiza, no siendo necesario que la víctima del engaño y la persona perjudicada sean la misma. El ánimo de lucro se identifica como un elemento subjetivo crucial del delito, definido actualmente en el artículo 248 del Código Penal como la intención del infractor de lograr un beneficio económico que se corresponda, aunque no necesariamente de manera equivalente, con el daño causado, descartando la responsabilidad por imprudencia. Por último, debe existir un nexo causal directo entre el engaño perpetrado y el daño resultante, mostrando que el fraude diseñado precede o acompaña la dinámica defraudatoria, con el agente consciente de las consecuencias de su conducta engañosa, lo que estimula la transferencia de bienes como resultado directo del error inducido, culminando en el perjuicio patrimonial de la víctima.

Respecto a la cuestión concreta ocupada por esta investigación, en concreto el supuesto en que el delincuente realiza la usurpación de los datos personales de la víctima para solicitar una financiación a nombre de este y percibir un aumento patrimonial y un beneficio económico. Esto estaría penado como un delito de estafa informática recogido en el artículo 249 del Código Penal, donde además nos encontraríamos con el delito de usurpación de identidad de la víctima recogido en el artículo 401 del Código Penal, cometido cuando una persona usurpa la identidad de otra para realizar actos en su nombre sin su consentimiento. Deben existir unos elementos para que este concurra, declarados por la Sala Penal del Tribunal Supremo (art. 248.2 CP: el ánimo de lucro, la manipulación informática, el acto de disposición y el engaño bastante) (STS (Penal), sec. 1ª, nº 379/2019, de 23 de julio de 2019).

En primer lugar, debe existir el engaño antecedente, que se refiere al uso de maquinaciones, ardides o fraudes que el sujeto activo emplea para inducir a error "bastante" o suficiente en la víctima. En este caso, el engaño puede consistir en la presentación de documentos robados o falsificados que parecen legítimos, lo que lleva a la entidad financiera a creer que están tratando con el verdadero titular de los documentos. O por ejemplo, uno de los casos más vistos actualmente en el sector, es el robo de los datos personales a través de portales de alquiler de vivienda, como *Idealista*, donde dichos estafadores solicitan a las víctimas que les envíen datos personales como el DNI, la nómina y alguna factura, para ficticiamente comparar su solvencia y que les sirva de señal, falseando que están muy ocupados para enseñar el piso y que si quieren visitarlo deben aportarles dicha documentación para mostrar interés y seriedad. Jugando con la urgencia de las víctimas y aparentando ser real bajo imágenes de pisos originales, a precios razonables y hablando por teléfono con personas humanas, realizan creíble su estrategia para obtener documentación de las víctimas.

De ese modo se produce el error inducido de la víctima quien creyendo que ofrece dicha documentación para poder visitar el piso o reservar, en realidad es para su utilización ilícita y el piso ni siquiera existe. Esta usurpación también puede producirse a través de otros métodos, como filtraciones por internet, hackeos a las bases de datos de entidades u organismos*, phishing…* La Sala Penal del Tribunal Supremo afirma que "no debe desplazarse indebidamente sobre los perjudicados la responsabilidad de comportamientos en los que la intención de engañar es manifiesta, y el autor ha conseguido su objetivo, lucrándose en perjuicio de su víctima" porque "el engaño no tiene que quedar neutralizado por una diligente actividad de la víctima" (STS (Penal), sec. 1ª, nº 51/2020, de 17 de febrero de 2020). Además, esa suplantación de identidad supera el "burdo engaño" porque, como dice la SAP Madrid, sec. 9ª, S 04-05-2015, nº 178/2015, rec. 661/2013, en el "phishing se utilizan técnicas de engaño, a través de las cuales el phisher utiliza contra la víctima el propio código de programa del banco o servicio similar, adquiriendo la página Web la verdadera apariencia de la entidad bancaria".

Para poder aceptar estas operaciones, llega un código *OTP (one-time password)* al móvil de la víctima, para confirmar la financiación o la utilización fraudulenta. Aquí comienza la segunda parte, donde se produce un error inducido en la víctima. Jugando con la desesperación y la urgencia del perjudicado, le vician su voluntad. En la mayoría de los casos el estafador llama a la víctima, haciéndose pasar por la entidad bancaria, y le comunican que se ha realizado una operación fraudulenta con sus datos y que le han abierto una financiación a su nombre o le han realizado cargos en su línea de crédito. Buscando generarle urgencia a la víctima, le dicen que para cancelar dicha operación y poder rechazar y subsanar el fraude, debe darle el código *OTP* recibido en su teléfono móvil, viéndose viciada su voluntad, ofreciéndole al estafador el propio código para aceptar y confirmar la apertura de la financiación. Ahí es cuando a consecuencia del engaño, la víctima realiza el propio acto de disposición patrimonial, como resultado del engaño y el error inducido. De ese modo, realiza un acto de disposición al aprobar la financiación (sin voluntad) realizándose en detrimento de su propio patrimonio o del de terceros, como podría ser el titular legítimo de la información robada.

El resultado directo del acto de disposición es el perjuicio patrimonial, que afecta al titular de la información personal, quien puede verse confrontado con obligaciones financieras no consentidas. Así el estafador a consecuencia de su acción obtiene un beneficio patrimonial, como es el objeto financiado o la disposición de efectivo de la línea de crédito.

Otro de los elementos necesarios en el delito de estafa, es el nexo causal. Es necesario establecer una cadena causal clara, donde el engaño provoca el error, el error conduce al acto de disposición, y este acto resulta en un perjuicio patrimonial. Esta relación de causalidad debe ser demostrable para atribuir la responsabilidad penal adecuadamente.

Finalmente, para que se configure el delito de estafa, debe existir un claro ánimo de lucro por parte del defraudador, quien actúa con la intención de obtener un beneficio económico a través del engaño y el fraude.

4. RESPONSABILIDAD DE LAS ENTIDADES DE CRÉDITO

Según el artículo 1766 del Código Civil, entre las obligaciones de los proveedores de servicios de pago, tanto como depositarios de los fondos de sus clientes, como facilitadores de crédito, está la de guardar la cosa con la diligencia de un ordenado empresario.

Las Memorias de Reclamaciones del Banco de España indican que, desde el año 2019, ha habido un aumento significativo en las reclamaciones contra los proveedores de servicios de pago debido a los delitos de estafas de phishing sufridas por los usuarios. A su vez, las estadísticas del Ministerio del Interior también muestran un crecimiento notable en el volumen de fraudes informáticos, aumentando de 94,792 delitos en 2017 a 267,011 delitos informáticos en 2021. Si observamos el tipo de delito, las estafas bancarias, con tarjeta e informáticas han aumentado de 28,246 delitos en 2017 a 100,461 delitos en 2021, según las estadísticas del Ministerio del Interior.

La Ley de Servicios de Pago (LSP) establece que, en caso de ejecución de una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devolverá inmediatamente el importe de la operación no autorizada, restituyendo la cuenta de pago al estado en que se habría encontrado de no haberse efectuado la operación no autorizada (Art. 45). La única excepción a esta norma es que el usuario haya actuado de manera fraudulenta o por haber incumplido deliberadamente o por negligencia grave una o varias de las obligaciones que establece el artículo 41 (Art. 46), es decir, que haya incumplido la obligación de custodiar las claves personales con “todas las medidas razonables” (Art. 41.a). El Real Decreto-ley 19/2008, de 23 de noviembre, que regula los servicios de pago, exige a las entidades financieras asegurar la confidencialidad de la identidad de los clientes y la validez de las transacciones. De este modo, los bancos son responsables de prevenir el phishing. Para cumplir con esta normativa, las entidades financieras deben educar a sus clientes sobre las prácticas de seguridad adecuadas, siendo responsabilidad de los clientes atender y seguir dichas recomendaciones, de modo que si no lo hace estaría cayendo en negligencia grave.

La práctica general de las entidades es la desestimación de las reclamaciones con el argumento de que el usuario ha incurrido en negligencia grave por haber incumplido la obligación de custodiar sus claves personales, al haberlas cedido al estafador como consecuencia del engaño. Ahora bien, ¿se puede considerar que el usuario ha incurrido en negligencia grave por el hecho de haber sido víctima de una estafa punible de phishing? Aunque la jurisprudencia no es uniforme, la mayoría de los tribunales se inclinan por excluir la negligencia grave del usuario.

Debemos valorar la implicación de la entidad respecto a sus medidas de seguridad internas, la educación al usuario que implemente y los protocolos de actuación que se suelan llevar a cabo ante movimientos sospechosos. A su vez, también se debe valorar el grado de negligencia del usuario que ha resultado perjudicado, así como el resto de los elementos de la estafa informática.

Se consideran deberes de las entidades bancarias rastrear las páginas web que suplantan su identidad y realizar un análisis de riesgo de las operaciones para implementar medidas de seguridad acorde a los riesgos presentes.

En base a la Sentencia de 16 de septiembre de 2022 del Juzgado de 1ª Instancia nº 3 de Santander "*los bancos deberían incorporar sus propios "detectores de humo" para anticipar cuando puede estar teniendo lugar una estafa e intervenir*", afirmación que guarda relación con la obligación que impone el Reglamento Delegado 2018/389 de realizar un análisis de riesgos en tiempo real para detectar cuándo una orden de pago es fraudulenta, para poder evitar dichas operaciones. Muchas entidades bancarias han venido usando un sistema de autenticación reforzada basado en sistemas 2FA, esto es, en el envío de claves de un solo uso (OTP) a través de SMS al teléfono móvil del usuario vinculado a la banca digital. Sin embargo, la industria de ciberseguridad recomienda evitar el uso del 2FA porque no acaba siendo del todo seguro. Como alternativa al sistema 2FA existen métodos de seguridad más robustos, como el acceso a la banca digital mediante llaves de seguridad USO y NFC o el acceso a la banca digital mediante un certificado digital o firma electrónica cualificada. Desde la Sentencia la SAP de Alicante, Sec. 8ª, nº 107/2018, de 12/3/2018 se viene considerando que la responsabilidad de la Entidad Bancaria es de "naturaleza cuasi-objetiva o de riesgo por razón legal". Esta declaración se reitera, entre otras, en la SAP de Zaragoza, Sec. 5ª, S. 01-07-2022, nº 804/2022, rec. 1130/2021.

Sin embargo, teniendo en cuenta, por un lado el incremento de este tipo de fraudes, cuyas cifras de criminalidad rebasan las de otros sectores de actividades peligrosas; la finalidad de la DSP2, según la cual los usuarios deben gozar de la debida protección frente a los riesgos inherentes a los medios de pago digitales; y que la doctrina jurisprudencial establece que quien tiene las ventajas de un negocio por el que obtiene un lucro, debe soportar los inconvenientes de ese negocio como contraprestación por el lucro obtenido (STS, Sala 1ª, S. 3-6-2006, nº 328/2006, rec. 281/1999), se debería tender a un juicio de responsabilidad objetiva, siempre analizando los elementos de concurrencia del tipo penal en consonancia con las brechas y barreras de seguridad de las entidades bancarias.

5. PROCESO DE RECLAMACIÓN DEL FRAUDE

A. Reclamación a la entidad bancaria

El proceso de reclamación comienza cuando el perjudicado notifica a la entidad bancaria lo ocurrido. Según la Orden ECO/734/2004, todas las entidades de crédito deben disponer de un Servicio de Atención al Cliente al que se debe acudir primero. La reclamación debe realizarse por escrito, ya sea por correo postal o electrónico, explicando el fraude y enviándola por correo certificado, con acuse de recibo, o burofax a la entidad. Es recomendable dirigirla al Servicio de Atención al Cliente (SAC) o al Defensor del Cliente, adjuntando la documentación necesaria, como el DNI y, si se ha interpuesto una denuncia, incluirla. El plazo de respuesta es de 15 días para fraudes relacionados con servicios de pago, un mes para otros fraudes (consumidores) y dos meses para no consumidores.

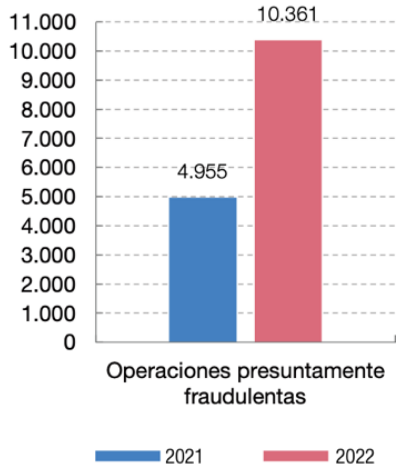
B. Reclamación al Banco de España

Si la entidad no responde en el plazo mencionado o si la resolución es insatisfactoria, el perjudicado puede dirigirse al Banco de España. La reclamación puede presentarse por vía telemática, por escrito, directamente en el Registro General del Banco de España, por correo postal a: Banco de España. Departamento de Conducta de Entidades. C/Alcalá, 48, 28014 Madrid, o a través de sus sucursales. El solicitante debe identificarse proporcionando nombre, apellidos, domicilio para notificaciones, DNI, y, si aplica, la documentación que acredite su representación legal. Debe especificar la entidad contra la cual se dirige la reclamación y la oficina implicada. Es imprescindible acreditar que se ha cumplido con el trámite previo ante los Servicios de Atención al Cliente de la entidad correspondiente. La reclamación debe incluir lugar, fecha y firma original del solicitante, junto con una fotocopia de la documentación que sustenta los hechos reclamados.

Las reclamaciones de consumidores serán inadmitidas si ha pasado más de un año desde la presentación de la reclamación ante la entidad, conforme al artículo 18.1.e de la Ley 7/2017. Además, no se admitirá una reclamación si han pasado más de cinco años desde los hechos sin que se haya presentado una reclamación ante la entidad.

En la Memoria de Banco de España de 2022, se informó que las reclamaciones por operaciones presuntamente fraudulentas fueron 10.361, un 30,3% del total recibido. Estos casos involucran a ciudadanos que no reconocen haber autorizado ciertas operaciones o que afirman haber sido engañados. De estas, el 86.1% corresponde a operaciones con tarjetas y el 13.9% a transferencias por Internet.

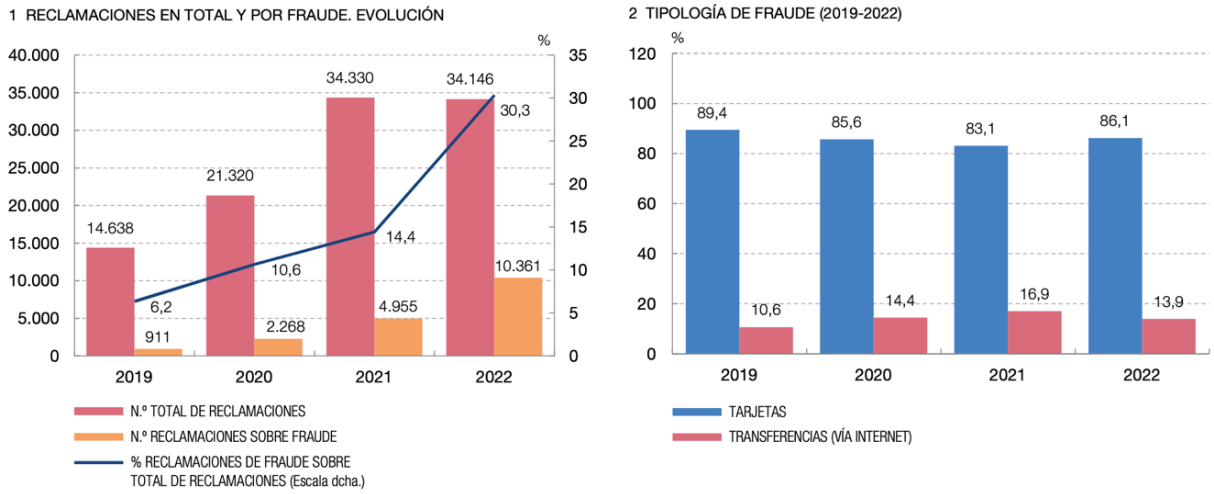
Gráfico 1. Comparativa de 2021 y 2022 de operaciones supuestamente fraudulentas.



Fuente: Banco de España

El gráfico 2 ilustra la evolución del volumen de reclamaciones recibidas en los últimos cuatro años en comparación con el total de reclamaciones y desglosado por tipología del producto afectado por el fraude. Las discrepancias entre los usuarios de servicios de pago y las entidades financieras son una de las principales razones del aumento de reclamaciones ante el Banco de España en los últimos años. En 2022, el volumen de reclamaciones relacionadas con fraudes se duplicó respecto a 2021, representando más del 30% del total de reclamaciones. La mayoría de las operaciones fraudulentas se realizaron con tarjeta (86%), mientras que las relacionadas con transferencias alcanzaron casi el 14%. En diciembre de 2022, el número total de tarjetas bancarias emitidas en España era de 102.029.691, y los 8.919 casos de fraude representaron aproximadamente el 0,01% de las tarjetas en circulación. A nivel de la Unión Europea, el fraude en pagos no presenciales con tarjeta disminuyó un 12% en 2021, según el Banco Central Europeo.

Gráfico 2. Reclamaciones por fraude. Evolución y comparación con el total de recibidas



Fuente: Banco de España

6. POLÍTICAS ANTIFRAUDE DE LAS ENTIDADES DE CRÉDITO

Con el incremento de las estafas informáticas, las entidades bancarias han implementado medidas de educación, seguridad interna y control de operaciones. Las entidades conciencian a los usuarios mediante comunicados y secciones en sus páginas web, instándoles a crear contraseñas complejas, instalar antivirus y mantener sus dispositivos actualizados. Aconsejan no responder, descargar ni ejecutar archivos adjuntos de correos que soliciten información personal, ya que suelen ser intentos de phishing. También se recomienda desconfiar de ofertas bancarias en internet que parezcan demasiado buenas para ser verdad y de ofertas de financiación o inversión de entidades de países remotos sin información fiable. Ante correos falsos solicitando datos confidenciales, se debe contactar directamente con el banco para verificar la autenticidad. Es importante ignorar correos que pretendan ser del Banco de España informando sobre productos bancarios no solicitados o transferencias inesperadas.

Los bancos nunca solicitan información sensible por teléfono de manera no solicitada. En caso de recibir una llamada sospechosa, se recomienda colgar y contactar al banco a través de canales oficiales. Los delincuentes suelen hacerse pasar por técnicos informáticos o personal del banco, alertando sobre supuestos problemas en dispositivos o movimientos fraudulentos en cuentas bancarias para obtener datos de la tarjeta bancaria o códigos OTP. Para evitar el "SMS spoofing", se recomienda activar funciones de detección de spam, analizar cuidadosamente los mensajes recibidos y usar aplicaciones que identifiquen la fuente real de las llamadas. Ante la recepción de una clave temporal sin haberla solicitado, es probable que sea un intento de fraude. Es crucial mantener a los usuarios informados para evitar estos fraudes.

El Real Decreto Ley 19/2018, de 23 de noviembre, Ley de Servicios de Pago, establece que las entidades financieras deben asegurar que las credenciales de seguridad del usuario no sean accesibles a terceros y que todas las operaciones se realicen a través de canales seguros. Los bancos están obligados a reembolsar cualquier operación no autorizada al cliente al final del día hábil siguiente a la notificación y deben cumplir estrictamente con los términos del contrato establecido con los clientes. La Directiva (UE) 2015/2366 (DSP2) exige autenticación reforzada de cliente y controles adecuados para gestionar riesgos operativos y de seguridad. El Reglamento Delegado 2018/389 complementa la DSP2, estableciendo la obligación de realizar un análisis de riesgo en tiempo real basado en factores como el importe de las operaciones y patrones de comportamiento anormales.

Los bancos implementan tecnología EDR ("Endpoint Detection and Response") para detectar, investigar y responder a amenazas cibernéticas. Este sistema utiliza inteligencia artificial y Big Data para mejorar la detección y prevención de amenazas complejas. La implementación de EDR incluye integración con la infraestructura existente, configuración personalizada, formación de empleados, pruebas y simulaciones de ataques, y revisión continua. Además, muchas entidades tienen un centro de operaciones de seguridad (SOC) que monitorea la actividad del banco en busca de movimientos sospechosos. El SOC se compone de analistas y técnicos de ciberseguridad especializados, encargados de identificar y responder a incidentes de seguridad. Otras herramientas utilizadas incluyen antivirus, antimalware, firewalls y sistemas de prevención de intrusiones (HIPS).

7. CONCLUSIONES

A través de este estudio, se han identificado y analizado las nuevas tipologías de estafas informáticas que afectan a las entidades bancarias, especialmente las relacionadas con aperturas de financiación y líneas de crédito. Los hallazgos clave indican que estos delitos no solo afectan a los usuarios individuales, sino que también alteran la estabilidad y la integridad del sistema financiero en su conjunto.

Las técnicas de estafa se han vuelto más sofisticadas, aprovechando las vulnerabilidades del sistema y de los usuarios. Algunas incluyen el uso avanzado de smishing, phishing, vishing y la ingeniería social para obtener acceso ilegítimo a datos personales y financieros de las víctimas. El

desarrollo tecnológico y digital del sector financiero facilita estas acciones, ya que las operaciones financieras se realizan cada vez más a través de medios digitales, a menudo sin medidas de seguridad robustas.

La investigación ha evidenciado una laguna significativa en la legislación actual que dificulta la persecución y sanción efectiva de estos fraudes. A pesar de la existencia del Reglamento General de Protección de Datos (GDPR), la Ley Orgánica de Protección de Datos Personales (LOPDGDD), la modificación del artículo 249 del Código Penal y la Ley de los Servicios de Pago, las estafas siguen causando graves perjuicios, lo que subraya la necesidad de fortalecer la legislación y los instrumentos de cumplimiento y supervisión.

El gobierno de España y la Unión Europea proponen más medidas de apoyo para erradicar estos fraudes, incluyendo campañas de concienciación e información sobre prácticas ilegítimas. Ruth García Ruiz, técnico de Ciberseguridad para Ciudadanos de Incibe, destaca la importancia de informar a los usuarios sobre estos fraudes para evitar caer en sus engaños. Ante cualquier movimiento, mensaje o llamada sospechosa, se recomienda contactar inmediatamente con el banco o verificar las cuentas a través de la aplicación móvil o web.

Para las entidades, se proponen sistemas de seguridad más robustos con tecnología avanzada como biometría, análisis de datos en tiempo real y equipos de soporte SOC para identificar y eliminar amenazas. Se recomienda el uso de sistemas de doble verificación y reconocimiento facial para acceder a las aplicaciones web y móviles, así como para la confirmación de operaciones y utilizaciones de tarjeta.

Además, se espera una legislación más robusta, con condenas más duras para los delincuentes y más equipos de investigación policial para desmantelar las redes de ciberdelincuentes. La legislación debería también obligar a los portales de compraventa y alquiler de pisos a modificar sus sistemas y establecer intermediaciones entre arrendatarios y arrendadores para evitar usurpaciones de documentación.

A medida que la tecnología avanza, también lo harán las técnicas de los estafadores, lo que requiere una vigilancia continua de la legislación para adaptarla a las nuevas formas de estafa informática. Este análisis establece una base sólida para futuras investigaciones y cambios legislativos en el derecho financiero, permitiendo a las entidades de crédito endurecer sus defensas y contribuir a un entorno financiero más seguro y justo para todos los consumidores.

8. REFERENCIAS

Añover, J. (2001). Echelon y Enfopol nos espían. Recuperado de: http://www.nodo50.org/altavoz/echelon.htm

Banco de España. (2019). Memoria de Reclamaciones 2019. Recuperado de: https://www.bde.es/f/webbde/Secciones/Publicaciones/PublicacionesAnuales/MemoriaServicioReclamaciones/19/Documentocompleto.pdf

Banco de España. (2020). Memoria de Reclamaciones 2020. Recuperado de: https://www.bde.es/f/webbde/Secciones/Publicaciones/PublicacionesAnuales/MemoriaServicioReclamaciones/20/MSR2020.pdf

Banco de España. (2021). Memoria de Reclamaciones 2021. Recuperado de: https://www.bde.es/f/webbde/Secciones/Publicaciones/PublicacionesAnuales/MemoriaServicioReclamaciones/21/MSR2021.pdf

BBVA. (s.f.). ¿Qué medidas de seguridad incluye la banca online de BBVA para particulares? Recuperado de: https://www.bbva.es/finanzas-vistazo/ciberseguridad/como-te-protege-bbva/banca-online-bbva-particulares-que-medidas-de-seguridad-incluye.html

Boletín de Información, número 32. (2009). 21st Century to two new challenges: Cyberwar and Cyberterrorism, Nómadas. Mediterranean Perspectives, número 1, pp. 1-10.

Brookes, P. (2007, Octubre). Contrarrestando el arte de la guerra informática. Grupo de Estudios Estratégicos, número 201. Recuperado de: http://www.gees.org/articulo/4637/

Busón Buesa, C. (2009, Agosto). Control en el ciberespacio. Recuperado de http://www.uned.es/ntedu/espanol/master/segundo/modulos/poder-y-control/poder.htm

Cabanillas, M. (2010, Noviembre). Preparados contra el cibercrimen, PCWorld.

Caro Bejarano, M. J. (2011, Marzo). Nuevo concepto de ciberdefensa de la OTAN. Documento Informativo, número 9, Instituto Español de Estudios Estratégicos (IEEE). Recuperado de: http://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI09_2011ConceptoCiberdefensaOTAN.pdf

Chamorro Palacios, F. N., Guaña Moya, E. J., y Sánchez Paredes, W. I. (2024). Análisis de Memoria de Malware Ofuscado en el Conjunto de Datos CIC- MALMEM-2022. Revista multidisciplinaria de desarrollo agropecuario, tecnológico, empresarial y humanista, 6(1), 5. Recuperado a partir de https://www.dateh.es/index.php/main/article/view/318

Fojón Chamorro, E. y Sanz Villalba, A. F. (2010, Junio). Ciberseguridad en España: una propuesta para su gestión. ARI, número 101, Real Instituto Elcano.

Fuentes, L. F. (2008). Malware, una amenaza de Internet», Revista Digital Universitario, volumen 9, número 4, pp. 1-9.

Domínguez, F. (2022, Junio 23). "La ciberseguridad no se trata sólo de tecnología, sino también de conocimientos que den valor a los clientes". Computerworld Spain, NA. https://link.gale.com/apps/doc/A758623603/IFME?u=anon~b203aadc&sid=googleScholar&xid=66f7bee9

Dupont, B. (2019, Octubre 11). "La ciberresiliencia de las instituciones financieras: importancia y aplicabilidad". Journal of Cybersecurity, Volume 5, Issue 1, 2019. Recuperado de: https://doi.org/10.1093/cybsec/tyz013

Hajgude, J. y Ragha, L. (2012). Phish mail guard: Phishing mail detection technique by using textual and URL analysis. World Congress on Information and Communication Technologies, pp. 297–302.

Hong, J. (2012). The State of Phishing Attacks. Communications of the ACM, 55(1), pp. 74-81.

INCIBE. (s.f) Fuga de información. Recuperado de: https://www.incibe.es/incibe-cert/tags/Fuga%20de%20información?page=3

Kang, A., Dong Lee, J., Min Kang, W., Barolli, L., y Hyuk Park, J. (2014). Security Considerations for Smart Phone Smishing Attacks. Springer-Verlag Berlin Heidelberg}, 1, 467-473. https://doi.org/10.1007%2F978-3-642-41674-3_202

Lemos, R. (2004). A Firm's Place in the Malware Supply Chain. Business Communications Review, pp. 22-28

Martínez Escamilla, M., Martín Lorenzo, M. y Valle Mariscal de Gante, M. (2012). Introducción a la teoría jurídica del delito. I.S.B.N.: 978-84-695-3959-0.

Martínez Santander, C. J., Cruz Gavilanes, Y., Cruz Gavilanes, T., y Álvarez Lozano, M. I. (2018). Seguridad por capas para frenar ataques de Smishing. ISSN-e 2477-8818, Vol. 4, Nº. 1, pp. 115-130.

McKinsey & Company. (2022, Agosto 25). "Creación de un marco de riesgo tecnológico y apetito por el riesgo cibernético". Recuperado de https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/creating-a-technology-risk-and-cyber-risk-appetite-framework

Mitnick, K. D., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley.

Orta Martínez, R. (2005, Mayo). Ciberterrorismo. Revista de Derecho Informático, número 82.

Pachón Ovalle, G. (2004). La red Echelon: privacidad, libertad y criptografía. Virtualidad Real, Programa de Doctorado en SIC, Universitat Oberta de Catalunya. Recuperado de: http://www.virtualidadreal.com/Red%20Echelon.pdf

Rodríguez Bernal, A. (2007, Febrero). Los cibercrímenes en el espacio de libertad, seguridad y justicia. Revista de Derecho Informático, número 103, pp. 1-42.

Rodríguez Pérez, C. (2008). Tecnologías de vigilancia e investigación: el caso Echelon. Informe: tecnologías de vigilancia e investigación, Posgrado Conocimiento, Ciencia y Ciudadanía en la Sociedad de la Información, Universitat de Barcelona. Recuperado de: http://www.ub.es/prometheus21/articulos/obsprometheus/crodr_echelon.pdf

Ruiloba Castilla, J. C. (2006). La actuación policial frente a los déficit de seguridad de Internet. Revista de los Estudios de Derecho y Ciencia Política de la UOC, número 2.

Sánchez-Bayón, A. (2020a). Renovación del pensamiento económico-empresarial tras la globalización: *Talentism & Happiness Economics*, *Bajo Palabra*, 24: 293-318 DOI: https://doi.org/10.15366/bp.2020.24.015

Sánchez-Bayón, A. (2020b). Business and labour culture changes in digital paradigm: rise and fall of human resources and the emergence of talent development. EconStor Open Access Articles and Book Chapters, ZBW - Leibniz Information Centre for Economics, pages 225-243. RePEc:erv:rednma:y:2014-2015:i:31:2

Sánchez-Bayón, A. (2021). Balance de la economía digital ante la singularidad tecnológica: cambios en el bienestar laboral y la cultura empresarial. *Sociología y Tecnociencia*, 11(2). 53-80. DOI: https://doi.org/10.24197/st.Extra_2.2021.53-80

Sánchez-Bayón, A. (2022a). De la Síntesis Neoclásica a la Síntesis Heterodoxa en la economía digital. *Procesos de Mercado, 19*(2): 277-306. https://doi.org/10.52195/pm.v19i2.818

Sánchez-Bayón, A. (2022b). ¿Crisis económica o economía en crisis? Relaciones ortodoxia-heterodoxia en la transición digital. *Semestre Económico*, 11(1): 54–73 doi: http://dx.doi.org/10.26867/se.2022.1.128

Sánchez-Bayón, A. (2023a). Paradoja del género según los neoinstitucionalistas. *Derecho y Religión*, 18: 59-84

Sánchez-Bayón, A. (2023b). Fallos estatales y paradojas sociales por el intervencionismo en cuestión de género. *Procesos de Mercado*. 20(2): 301-342

Sánchez Bayón, A. (2023c). Análisis jurídico-económico de la cuestión de género. *Semestre Económico*, *12*(2), 54–77. https://doi.org/10.26867/se.2023.v12i2.152

Sánchez-Bayón, A. (2024). Revitalización de la disputa del método en economía: revisión científica y docente. *Encuentros Multidisciplinares*, 76: 1-14

Sánchez-Bayón, A., A. Urbina, D., Alonso-Neira, M. Ángel, & Arpi, R. (2023). Problema del conocimiento económico: revitalización de la disputa del método, análisis heterodoxo y claves de innovación docente. *Bajo Palabra*, (34), 117–140. https://doi.org/10.15366/bp2023.34.006

Sánchez-Bayón, A., García-Ramos, M.A. (2021). A win-win case of CSR 3.0 for wellbeing economics: digital currencies as a tool to improve the personnel income, the environmental respect & the general wellness. *Revista de Estudios Cooperativos*-REVESCO, 138, e75564: 1-11. DOI: https://doi.org/10.5209/reve.75564

Sánchez Medero, G. (2008, Marzo). Ciberterrorismo. La guerra del siglo XXI, El Viejo Topo, número 242, pp. 15-23.

Santander. (s.f.). Control interno. Banco Santander. Recuperado de https://www.santander.com/content/dam/santander-com/es/contenido-paginas/landing-pages/gobierno-corporativo-y-política-de-remuneraciones/do-Control%20interno.pdf

Shaikh, A. N., Shabut, A. M. y Hossain, M. A. (2016). A literature review on phishing crime, prevention review and investigation of gaps. 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA), pp. 9–15.

Thomas, Timothy L. (2001, Agosto). Las estrategias electrónicas de China. Military Review, pp. 72-79.

Toffler, A. (1995, Agosto). Onward Cyber-Soldiers, Time Magazine, volumen 146, número 8.

Waston, S. (2007). Científicos usamericanos quieren desembarazarse de la red de Internet. Rebelión. Recuperado de: http://www.rebelion.org/noticia.php?id=49932

Xataka. (2024, Enero). Ni la seguridad del banco es infalible: las cinco técnicas de los ciberdelincuentes para acceder a nuestro dinero. Recuperado de: https://www.xataka.com/legislacion-y-derechos/te-llaman-numero-tu-banco-pierdes-todos-tus-ahorros-estafa-cada-vez-comun-espana

Yu, W. D., Nargundkar, S., y Tiruthani, N. (2008). A phishing vulnerability analysis of web based systems. IEEE Symposium on Computers and Communications, pp. 326–331.