PROTECCIÓN DEL CONSUMIDOR Y SEGURIDAD FINANCIERA

Daniel Martín Garrote

Grado en Administración y Dirección de Empresas en la Universidad de Málaga

Marco legal y derechos del consumidor

¿Qué es la protección del consumidor financiero y quién la garantiza?

Según la Ley 10/2014, de 26 junio, de ordenación, supervisión y solvencia de entidades de crédito, la protección del consumidor financiero consiste en el conjunto de normas que aseguran la transparencia y la equidad en la relación entre clientes y los distintos agentes financieros, tales como entidades de crédito, de inversión o aseguradoras. En España, quienes se encargan de supervisar, regular y velar por su cumplimiento son, principalmente, el Banco de España, la Comisión Nacional de Mercado de Valores (CNMV) y la Dirección General de Seguros y Fondo de Pensiones (DGSFP).

¿Qué es el Servicio de Atención al Cliente (SAC)?

El SAC es el departamento interno y obligatorio que las entidades financieras ponen a disposición del consumidor para resolver de forma gratuita sus quejas y reclamaciones. Una vez realizada la reclamación, constituye el primer paso legal e indispensable antes de poder acudir a los supervisores públicos. Además, según el Real Decreto-ley 19/2018 de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, la entidad está obligada por ley a emitir una contestación oficial en un plazo máximo de quince días hábiles para servicios de pago o de un mes para el resto de los productos financieros.

¿Qué papel juegan las hojas de reclamaciones en el sector financiero?

En el sector financiero, las hojas de reclamaciones son instrumentos oficiales que permiten al consumidor dejar constancia formal de una disconformidad, siendo obligatorias tanto en sucursales físicas como en canales digitales. Sirve como prueba vinculante de que el cliente intentó solucionar la controversia directamente con la entidad antes de poder elevar el caso ante los organismos supervisores del Estado.

¿Qué información debe facilitar la entidad antes de contratar un producto?

Antes de la contratación de un producto financiero, las entidades deben entregar documentación precontractual obligatoria para garantizar el principio de transparencia y un consentimiento informado. En el ámbito del crédito se exige la Ficha de Información Precontractual regulada en la Orden EHA/2899/2011, de 28 de octubre, de transparencia y protección del cliente de servicios bancarios; o la Ficha Europea de Información Normalizada, establecida en la Ley 5/2019, 2de 15 de marzo, reguladora de los contratos de crédito inmobiliario en hipotecas, donde se detalla el coste total y la Tasa Anual Equivalente.

Por otro lado, en inversiones es preceptivo el documento de Datos Fundamentales para el Inversor o el *Key Information Document*, regulado en el Reglamento (UE) n.º 1286/2014 del Parlamento Europeo y del Consejo, de 26 de noviembre, sobre los documentos de datos fundamentales relativos a los productos de inversión minorista vinculados y los productos de inversión basados en seguros, para desglosar los riesgos, comisiones y escenarios de rentabilidad.

Esta entrega previa constituye un requisito legal imprescindible para evaluar los costes y comparar ofertas antes de la contratación.

¿Cuándo se puede acudir, desde el punto de vista del consumidor, a los supervisores públicos como el Banco de España o la CNMV?

El consumidor puede acudir de forma gratuita a los supervisores públicos (Banco de España, CNMV o DGSFP) únicamente tras haber agotado la vía previa de reclamación directa ante el Servicio de Atención al Cliente (SAC) de la entidad financiera. Este paso es un requisito legal obligatorio que se habilita una vez que el SAC deniega la queja o cuando transcurre el plazo legal de resolución sin que el usuario haya recibido una contestación oficial.

Seguridad financiera y prevención del fraude

¿Qué entendemos por seguridad financiera en el entorno actual?

En el entorno digitalizado actual, la seguridad financiera se entiende como el conjunto de medidas, hábitos y herramientas que el consumidor adopta para proteger tanto sus fondos como datos personales frente a accesos no autorizados y ciberamenazas. Esto implica, más allá de la confianza en los sistemas de autenticación y encriptación de las entidades de crédito, la responsabilidad del usuario en la custodia de sus credenciales y en el desarrollo de una cultura de prevención y escepticismo digital.

¿Cuáles son las estafas digitales más comunes actualmente?

IBM (s.f.), INCIBE (s.f.-d) y Muñoz (2022) coinciden en señalar que las amenazas más frecuentes se basan en la ingeniería social, es decir, en técnicas de manipulación psicológica para que la víctima facilite voluntariamente sus claves. Entre ellas, destacan el *phishing* (correos electrónicos que suplantan identidades), el *smishing* (SMS fraudulentos con enlaces maliciosos) y el *vishing* (llamadas telefónicas engañosas). A estas se le suma el *qrishing*, que utiliza códigos QR manipulados para redirigir al usuario a webs fraudulentos con el objetivo de capturar sus datos de acceso.

¿En qué consiste la Autenticación de Doble Factor (2FA)?

La autenticación de Doble Factor es una medida de seguridad obligatoria en la banca digital que exige al consumidor aportar dos formas independientes de identificación para validar un acceso o una operación financiera. De acuerdo con el INCIBE (s.f.-a), este sistema combina tres posibles elementos: información secreta (como una contraseña), un objeto personal (como su teléfono móvil para recibir un código) o una característica física (su huella dactilar o reconocimiento facial).

¿Qué prácticas de "higiene digital" mejoran nuestra seguridad?

La higiene digital en finanzas comprende los hábitos preventivos para reducir la exposición a ciberriesgos económicos. Destaca el uso de aplicaciones oficiales y protocolos seguros (*https*), evitar operar o realizar compras en redes WiFi-públicas, y el empleo de contraseñas robustas y exclusivas guardadas en gestores. Estas pautas actúan como un cortafuegos para minimizar el impacto financiero ante cualquier brecha de seguridad.

¿Qué pasos se deben seguir tras detectar una estafa financiera?

Ante un fraude, el consumidor debe activar un protocolo inmediato: primero, bloquear tarjetas y accesos a la banca digital. Acto seguido, se deben recopilar todas las evidencias (capturas de pantalla y mensajes) e interponer una denuncia formal ante la Policía o la Guardia Civil. Finalmente, se debe presentar dicha denuncia ante el banco para iniciar la reclamación de los fondos sustraídos bajo el amparo legal (Banco de España, s.f.).

Seguridad en el uso de tarjetas y cajeros

¿Qué responsabilidad tiene el usuario ante cargos no autorizados?

Según el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, en caso de pérdida o robo de un instrumento de pago, la responsabilidad del usuario se limita a un máximo de 50€ para las operaciones no autorizadas realizadas antes de notificar el suceso, salvo cuando al usuario no le resultara posible detectar la pérdida o esta fuera imputable a actuaciones de la propia entidad o sus agentes.

Una vez que el usuario comunica la pérdida o uso indebido, deja de soportar pérdidas derivadas de operaciones posteriores, quedando el proveedor de servicios de pago obligado a reembolsar sin demora el importe de las operaciones no autorizadas.

¿Existen excepciones donde el cliente no asuma ningún coste o deba pagar la totalidad del fraude?

Según el Real Decreto-ley 19/2018, de 23 de noviembre, existen determinadas excepciones en las que el usuario no soporta pérdidas. En particular, no asumirá ningún coste si el proveedor de servicios de pago no aplicó la autenticación reforzada del cliente o no puso a su disposición medios adecuados para notificar la pérdida o bloquear el instrumento de pago, siempre que el usuario no haya actuado de forma fraudulenta o con negligencia grave.

Por el contrario, el usuario responderá de la totalidad de las pérdidas cuando haya actuado con fraude o negligencia grave, por ejemplo, al facilitar voluntariamente sus credenciales de seguridad a un tercero.

¿Qué es el skimming y cómo evitarlo en los cajeros?

Según lo establecido por Santander (2023), el *skimming* constituye una práctica delictiva orientada a la captación ilícita de los datos contenidos en una tarjeta bancaria, con el objetivo de reproducirlos en soportes fraudulentos o de realizar operaciones no autorizadas. Para mitigar este riesgo, se recomienda que el usuario adopte conductas preventivas como no perder de vista la tarjeta durante su uso, verificar el estado de los dispositivos o evitar la utilización de cajeros en entornos poco iluminados, donde resulta más difícil detectar la presencia de mecanismos externos de captura. No obstante, la estrategia de prevención más eficaz consiste en priorizar el empleo de tecnologías *contactless* o la retirada de efectivo mediante códigos generados en aplicaciones

móviles, reduciendo así la necesidad de introducir físicamente la tarjeta en terminales potencialmente comprometidos.

¿Por qué es recomendable utilizar tarjetas virtuales para compras online?

Las tarjetas virtuales aportan un extra de seguridad al actuar como un escudo de confidencialidad, manteniendo los datos bancarios reales y de las cuentas corrientes al margen de las compras por Internet. Al crear una, el usuario dispone de un número de tarjeta, fecha de caducidad y de un Código Valor de Verificación que no corresponden a sus datos ordinarios, por lo que nunca le podrán sustraer su información real. Además, ofrecen un control total: el usuario decide la fecha de caducidad y puede limitar el saldo al importe exacto de la compra, permitiendo crear una tarjeta distinta para cada operación o anularla al instante desde la banca electrónica si sospecha de cualquier peligro (Rubio Jiménez, 2024).

¿Qué precauciones esenciales se deben adoptar al retirar efectivo en un cajero automático?

Según lo establecido por Álvarez Avello (s.f.), la retirada de efectivo en cajeros automáticos exige la adopción de determinadas medidas de seguridad orientadas a prevenir el fraude y proteger la información personal. Entre ellas, resulta fundamental ocultar el teclado durante la introducción del PIN, con el fin de impedir su captación mediante microcámaras ocultas o técnicas de observación directa, reduciendo así el riesgo de clonación de la tarjeta. Asimismo, es recomendable realizar una inspección previa del terminal para detectar posibles anomalías o dispositivos añadidos, comprobar que el cajero se encuentra en su estado operativo habitual y priorizar aquellos ubicados en entornos concurridos y adecuadamente iluminados. Igualmente, debe mantenerse una distancia prudencial respecto a terceros durante la operación, evitando la intervención o la proximidad de desconocidos. Finalmente, se aconseja prescindir del recibo impreso o, en su caso, custodiarlo adecuadamente, optando preferentemente por la consulta digital de los movimientos para minimizar la exposición de información sensible.

Seguridad en la banca digital y aplicaciones móviles

¿Cómo afecta el entorno digital a nuestra seguridad financiera?

Como señalan los autores Toloba y del Río (2020), la digitalización bancaria ha dado lugar a nuevas oportunidades como la mejora de la eficiencia y la eficacia, la reducción de costes o la mejora de la experiencia del cliente. No obstante, también ha facilitado la introducción de riesgos cibernéticos como el phishing y el *ransomware*, amenazando la confidencialidad de los datos.

Asimismo, la falta de verificaciones exhaustivas y el uso de *deepfakes* (contenido audiovisual o de audio que crea, a partir de la IA, imágenes, vídeos o voces falsas) facilitan el fraude y la suplantación de identidad con información robada. Desde la perspectiva de las entidades bancarias, a nivel operativo, los errores de configuración de *software* generan brechas críticas, mientras que la gestión deficiente de los datos personales acarrea sanciones y pérdidas reputacionales. Por ello, el marco regulatorio exige auditorías automatizadas y una estricta trazabilidad, obligando a las entidades a capacitar a su personal e implementar estrategias de mitigación efectivas (EsF, 2023).

¿Qué importancia tienen las actualizaciones de la aplicación bancaria?

La actualización periódica de la aplicación de banca móvil es indispensable para mitigar los riesgos de fraude electrónico, ya que permite parchear vulnerabilidades y corregir errores de la aplicación que los ciberdelincuentes podrían explotar para interceptar datos financieros. Asimismo, este proceso garantiza el acceso inmediato a nuevas herramientas de control y mejoras de seguridad desarrolladas por la entidad. Para mantener esta protección de forma continua, se recomienda activar las actualizaciones automáticas y utilizar únicamente las tiendas oficiales de aplicaciones (FasterCapital, 2025).

¿Cómo verificar que una página web bancaria es auténtica?

De acuerdo con lo indicado por el INCIBE (s.f.-c), para comprobar la autenticidad de un sitio web bancario, se debe verificar que la URL comience estrictamente por *https* y muestre el icono de un candado en la barra de direcciones. Asimismo, resulta fundamental hacer clic sobre dicho candado para constatar que la dirección esté correctamente escrita y no suplante a la entidad. Adicionalmente, se debe evitar el uso de redes wifi-públicas al realizar estos trámites, rechazar cualquier correo electrónico que solicite claves personales y, ante cualquier sospecha, contactar directamente con el banco para solucionar el problema.

¿Qué ventajas ofrece el bloqueo biométrico en el móvil?

El INCIBE (s.f.-b) establece que la biometría destaca por ser una alternativa altamente precisa que emplea rasgos físicos únicos del usuario, como la huella dactilar o el reconocimiento facial, para verificar su identidad. Su principal ventaja radica en que estas características no pueden ser fácilmente replicadas ni falsificadas por terceros. Además, al no depender de combinaciones alfanuméricas, elimina de raíz el riesgo de que el mecanismo de acceso sea olvidado o adivinado, convirtiéndose en una solución sólida, rápida y cómoda para blindar la información sensible del dispositivo.

¿Qué es el pharming y cómo se previene?

De acuerdo con Muñoz (2025), el *pharming* es un fraude cibernético que altera los servidores de Sistema de Nombres de Dominio (DNS, por sus siglas en inglés) o infecta dispositivos para redirigir al usuario a páginas web falsas, incluso si escribe correctamente la dirección oficial, con el fin de robar sus credenciales bancarias. Para prevenirlo, es fundamental mantener actualizados el sistema operativo y el antivirus. Asimismo, se debe verificar minuciosamente la URL bajo protocolo *https*, activar el doble factor de autenticación y acceder siempre tecleando de forma directa la dirección oficial en el navegador.

Protección de datos y privacidad financiera

¿Qué relación hay entre protección de datos y seguridad económica?

Tal y como explica la AEPD (s.f.), la protección de datos es crucial para la seguridad económica, ya que la información financiera y de identidad determina nuestra solvencia patrimonial. De hecho, la ley prohíbe que se utilicen datos de forma ilícita para contratar servicios que el ciudadano no ha solicitado. Un fallo en la privacidad puede derivar en la inclusión indebida del ciudadano en ficheros de morosos, afectando gravemente a su historial de crédito. Por ello, las entidades deben evaluar riesgos y aplicar medidas como el cifrado para blindar tanto los datos como el patrimonio.

¿Qué son los derechos de acceso, rectificación, oposición y supresión?

Los derechos de acceso, rectificación, oposición y supresión constituyen garantías fundamentales en materia de protección de datos personales, reconocidas en el marco normativo supervisado por la Agencia Española de Protección de Datos. El derecho de acceso permite al interesado conocer si sus datos están siendo tratados y obtener copia de los mismos; el de rectificación posibilita la corrección de datos inexactos o incompletos; el de oposición faculta al titular para impedir el tratamiento de sus datos en determinados supuestos, como la utilización con fines comerciales; y el derecho de supresión (también denominado “derecho al olvido”) permite solicitar la eliminación de la información personal cuando ya no resulte necesaria o cuando el tratamiento sea ilícito.

¿Qué riesgos financieros tiene compartir información en redes sociales?

Siguiendo lo establecido por el INCIBE (s.f.-c), la publicación de datos privados provoca una pérdida de control de la información que puede ser utilizada en nuestra contra. Revelar aspectos críticos como contraseñas, datos bancarios expone al usuario a problemas de suplantación o fraudes. Asimismo, todo lo compartido alimenta la reputación digital y queda registrado de forma

permanente en los servidores, permitiendo que terceros desconocidos copien o difundan estos datos con fines delictivos.

¿Por qué es necesario destruir los documentos bancarios físicos?

La destrucción de los soportes no electrónicos es obligatoria cuando la información llega al final de su ciclo de vida y deja de ser necesaria. Desechar estos documentos impresos sin precauciones expone la información confidencial a manos de terceros que pueden utilizarla de forma perjudicial. Por ello, resulta indispensable aplicar el triturado para garantizar que los datos no vuelvan a ser accesibles, cumpliendo así de forma estricta con la legislación y la normativa de privacidad vigentes (INCIBE, 2024).

¿Qué es la "cesión de datos a terceros" y qué peligro financiero tiene?

Según la AEPD (s.f.), la cesión a terceros es la comunicación de datos personales a entidades externas para fines ajenos al contrato principal. El peligro financiero radica en que una brecha de seguridad en dichas bases de datos expone al usuario a contrataciones fraudulentas y altas no solicitadas en servicios financieros o de suministro. Para evitarlo, la normativa ampara el derecho de oposición y obliga a las empresas a incluir casillas visibles para que el ciudadano pueda negarse expresamente a estos tratamientos comerciales.

Referencias

AEPD (s.f.). *Protección de Datos: Guía para el Ciudadano.* Agencia Española de Protección de Datos. https://www.aepd.es/guias/guia-ciudadano.pdf

Álvarez Avello, F. (s.f.). *¿Cómo sacar dinero con la tarjeta de crédito?* BBVA https://www.bbva.es/finanzas-vistazo/ef/tarjetas/sacar-dinero-con-tarjeta-de-credito.html

Banco de España. (s.f.). *Consejos para prevenir el fraude en operaciones bancarias*: *Iniciativa Educativa del Banco de España.* https://www.bde.es/f/webbe/INF/MenuHorizontal/AreasActuacion/conducta/ficheros/Sesion1GuiaConsejosparaprevenirelfraudeenoperacionesbancarias.pdf

EsF (2023). *Desafíos de la digitalización del sistema financiero*. (Dossieres nº 49). Economistas sin Fronteras. https://ecosfron.org/wp-content/uploads/2023/03/Dossieres-EsF-49-Desafios-de-la-digitalizacion-del-sistema-financiero.pdf

FasterCapital (2025). *Banca móvil: mitigar los riesgos de fraude electrónico sobre la marcha.* https://fastercapital.com/es/contenido/Banca-movil--mitigar-los-riesgos-de-fraude-electronico-sobre-la-marcha.html#importancia-de-actualizar-peri-dicamente-las-aplicaciones-de-banca-m-vil

IBM. (s.f.). *¿Qué es la Ingeniería Social?* https://www.ibm.com/es-es/think/topics/social-engineering

INCIBE. (2024). *Borrado seguro y gestión de soportes. Política de seguridad para la PYME* Instituto Nacional de Ciberseguridad. https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/2024/Borrado_seguro_Pol%C3%ADtica%20de%20seguridad_2024.pdf

INCIBE (s.f.-a). *Autenticación de dos factores (2FA).* Instituto Nacional de Ciberseguridad https://www.incibe.es/ciudadania/tematicas/contrasenas-seguras/autenticacion-de-dos-factores

INCIBE (s.f.-b). *Bloqueo de dispositivos: Protege tu información.* https://www.incibe.es/ciudadania/tematicas/dispositivos-moviles/bloqueo-dispositivos

INCIBE (s.f.-c). *Privacidad y seguridad en Internet.* Instituto Nacional de Ciberseguridad y Agencia Española de Protección de Datos. https://www.incibe.es/sites/default/files/docs/guiaprivacidadseguridadinternet.pdf

INCIBE (s.f.-d). *Vishing.* Instituto Nacional de Ciberseguridad. https://www.incibe.es/ciudadania/tematicas/ingenieria-social-fraudes-online/vishing

Muñoz, I. (2022). *QRishing: Ocultando el phishing en códigos QR*. BBVA. https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/qrishing-phishing-oculto-en-codigos-qr.html

Muñoz, I. (2025). *¿Qué es el pharming y cómo puedes protegerte?* BBVA. https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/que-es-el-pharming-y-como-puedes-evitarlo.html

Rubio Jiménez, B. (2024*). Tarjetas virtuales: qué son y para qué sirven.* Blog Unicaja Banco https://uniblog.unicajabanco.es/tarjetas-virtuales--que-son-y-para-que-sirven

Santander (2023). *"Skimming": ¿qué es y cómo protegerte contra este fraude?* https://www.santander.com/es/stories/skimming

Toloba, C. y del Río, J. M. (2020). La perspectiva de la digitalización de la banca española: riesgos y oportunidades. *Revista de Estabilidad Financiera* (38), 79-97. https://www.bde.es/f/webbde/GAP/Secciones/Publicaciones/InformesBoletinesRevistas/RevistaEstabilidadFinanciera/20/mayo/es/Digitalizacion.pdf