Instrucciones para el uso de los servicios bancarios

Cashper.es • Cashperplus.es • Fidinda.es

Versión: 1.0 20-11-2026

1. Objeto de este documento

Bank DiMare Limited (el «Banco»), con número de registro C46997, presta servicios de crédito a través de Cashper.es, Cashperplus.es y Fidinda.es.

Esta guía explica cómo puede solicitar, acceder a, utilizar y dejar de utilizar los servicios a distancia asociados a [Cashper.es o CashperPlus.es o Fidinda.es], y facilita información sobre atención al cliente, datos de contacto, medidas de seguridad, procedimientos de comunicación de fraude y protección de datos.

Estos servicios sirven de apoyo a su producto de crédito; no constituyen una cuenta de pago de uso general ni un servicio de banca telefónica transaccional sin restricciones. Lea esta guía junto con su contrato de préstamo, los términos y condiciones aplicables y la política de privacidad. Sus derechos legales no se ven afectados.

2. Canales oficiales, contactos y horario de atención

Los clientes disponen de los siguientes servicios:

Servicio	Disponible
Área de clientes online / servicio a través de internet	Sí
Sitio web adaptado a móviles	Sí
Aplicación móvil de banca específica	No
Banca telefónica	No
Atención por correo electrónico	Sí
Centro de atención al cliente	Sí

Marca y sitio web	Contacto telefónico y por escrito	Horario de atención al cliente

Cashper **Sitio web oficial** **Seleccione «Acceso clientes» para iniciar sesión.**	910 052 004 (llamada con tarifa estándar) 900 525 278 (gratuito, de lunes a viernes) clientes@cashper.es SMS: 638 444 218	Lunes a viernes: 09:30–18:30 Sábados: 09:00–14:00, solo clientes existentes Domingos y festivos: cerrado
Cashperplus **Sitio web oficial** **Seleccione «Acceso clientes» para iniciar sesión.**	900 525 288 (gratuito) 910 059 460 plazos@cashper.es SMS: 638 444 218	Lunes a viernes: 09:30–18:30 Sábados: 09:00–14:00 Domingos y festivos: cerrado
Fidinda **Sitio web oficial** **Seleccione «Acceso clientes» para iniciar sesión.**	900 525 296 (gratuito) 912 582 987 info@fidinda.es	Lunes a viernes: 08:30–16:00 Sábados, domingos y festivos: cerrado

Ayuda fuera del horario de atención al cliente: La atención personal está disponible en el horario indicado arriba, y no las 24 horas del día. Fuera de ese horario, envíe su consulta a la dirección de correo electrónico de su marca. El envío de un correo electrónico o SMS no implica que vaya a revisarse ni tramitarse de inmediato. En caso de sospecha de fraude o actividad no autorizada, siga lo indicado en el apartado 7. Las llamadas y los SMS con tarifa estándar pueden conllevar cargos de su operador. **Dirección postal:** Bank DiMare Limited, The Emporium, C De Brocktorff Street, Msida, MSD 1421, Malta.

Domicilio en España a efectos de notificaciones: C/ Zurbano 45, 1ª planta, 28010 Madrid.

3. Servicios disponibles y acceso 24/7

Acceda al sitio web de su marca con un navegador compatible y conexión a internet. Para acceder desde un smartphone o una tableta, utilice el sitio web a través del navegador de su dispositivo. El acceso mediante el navegador del móvil es distinto de una aplicación bancaria descargable. No se ofrece aplicación para teléfono móvil. La asistencia telefónica está disponible en el horario de atención al cliente indicado en el apartado 2. Cashper también ofrece la posibilidad de solicitar préstamos con asistencia telefónica. Para recibir asistencia sobre Cashperplus o Fidinda, póngase en contacto con el equipo de atención al cliente correspondiente.

Funcionalidad — las tres marcas salvo que se indique otra cosa	**¿Disponible las 24 horas del día, todos los días del año?**

Consultar información, usar un simulador y acceder a un formulario de solicitud online	Sí
Iniciar sesión en el área de clientes y utilizar las funciones de gestión del préstamo habilitadas	Sí
Acceso desde el navegador del móvil	Sí
Aprobación, verificación que requiera la intervención de un agente, desembolso y registro de pagos	Enviar una solicitud o instrucción online no garantiza la aprobación inmediata, la tramitación del pago ni la recepción de los fondos.
Asistencia telefónica e instrucciones gestionadas por un agente	No. La atención personal está disponible en el horario de atención al cliente indicado en el apartado 2.
Correo electrónico y SMS	Los mensajes no constituyen asistencia en tiempo real ni confirman que una instrucción se haya tramitado. La atención personal está disponible en el horario de atención al cliente indicado en el apartado 2.

Interrupciones del servicio: las tareas de mantenimiento programado y/o de emergencia, las incidencias técnicas, las restricciones de seguridad, los problemas de conectividad, las medidas de ciberseguridad y los servicios bancarios o de verificación de terceros pueden afectar al acceso o a la realización de una operación. El acceso a un servicio online no garantiza un servicio ininterrumpido ni una tramitación inmediata. Consulte el apartado 8 para saber qué hacer si un servicio no está disponible.

4. Cómo solicitar un servicio y empezar a utilizarlo

1. **Acceda al sitio web – [sitio web]** Revise la información del producto, los costes, las fechas de reembolso y la información precontractual antes de decidir si presenta la solicitud.
2. **Complete la solicitud online.** Seleccione el importe y el plazo que desea solicitar y siga el formulario de solicitud. Facilite de forma exacta los datos de identidad, contacto, cuenta bancaria e información financiera que se le pidan para su solicitud.
3. **Si procede, complete la verificación.** Siga los pasos de verificación de identidad y financiera de su solicitud, incluida la verificación mediante Tink cuando se ofrezca. Cualquier vía alternativa de documentación dependerá de su solicitud y de sus circunstancias. Lea la información correspondiente al servicio del tercero antes de autorizar el acceso. No envíe por correo electrónico contraseñas bancarias ni códigos de seguridad.

4. **Si se aprueba, revise y, si está de acuerdo, acepte toda la documentación.** Lea y conserve la información precontractual y el contrato. Complete los pasos de aceptación y activación de la cuenta que se le presenten. El envío de la solicitud no implica por sí mismo que el préstamo haya sido aprobado. Siempre es necesaria una evaluación de la solvencia.
5. **Acceda a su área de clientes.** Seleccione «Acceso clientes» en [sitio web] e introduzca las credenciales solicitadas. Utilice «He olvidado mi contraseña» si necesita recuperar el acceso, o póngase en contacto con su marca si ha cambiado su número de teléfono registrado.
   Asegúrese de mantener la confidencialidad de sus contraseñas; utilizar contraseñas seguras; no compartir sus credenciales de acceso; proteger adecuadamente sus dispositivos; y avisar inmediatamente a Cashper si sospecha de cualquier actividad no autorizada.
6. **Asistencia telefónica.** Utilice los contactos del apartado 2. Pregunte al equipo de atención al cliente qué operaciones pueden realizarse por teléfono.

5. Cómo utilizar los servicios

Sitio web o navegador del móvil: Inicie sesión a través del sitio web. Revise la información del préstamo y las operaciones efectivamente habilitadas para su cuenta. Cuando estén disponibles, siga los pasos indicados en pantalla para revisar documentos, facilitar la información solicitada o iniciar un pago. Compruebe el importe, la referencia y los datos del destinatario con su contrato o con instrucciones verificadas de forma independiente. Conserve los justificantes y cierre la sesión después de usarla.

Teléfono, correo electrónico y SMS: Utilice los contactos indicados en el apartado 2 para consultas sobre solicitudes, acceso, documentos, reembolsos, incidencias técnicas y otras cuestiones relativas al producto. Es posible que el Banco tenga que verificar su identidad antes de facilitarle información o atender una instrucción. Pregunte qué operaciones pueden realizarse por ese canal y solicite confirmación de cualquier instrucción acordada.

6. Cómo dejar de utilizar un servicio

Los clientes que deseen dejar de utilizar un servicio pueden:

- ponerse en contacto con Atención al Cliente a través de los datos indicados en el apartado 2 e indicar si desean dejar de utilizar el acceso web/desde el navegador del móvil, un servicio de SMS habilitado u otro servicio a distancia;
- solicitar el cierre de la cuenta cuando la ley lo permita; o
- dejar de utilizar el servicio una vez cumplidas todas las obligaciones contractuales.

Cashper podrá conservar determinada información cuando así lo exija la ley, incluidos los requisitos en materia de prevención del blanqueamiento de capitales, contabilidad, protección del consumidor o normativa regulatoria.

Desactivar el acceso o dejar de utilizar un canal no cancela por sí mismo un préstamo ni elimina las obligaciones contractuales de reembolso. Si desea desistir de un contrato, realizar un reembolso anticipado o resolver una línea de crédito, solicite el procedimiento específico aplicable y consulte su contrato de préstamo y/o los términos y condiciones.

Además, debería:

1. **Cerrar la sesión:** Cierre la sesión y la ventana del navegador, especialmente en un dispositivo compartido. Elimine las credenciales guardadas de cualquier dispositivo que ya no controle.
2. **Acordar cómo recibirá la información esencial:** Antes de que se desactive el acceso, conserve sus documentos y pregunte cómo recibirá los extractos, las notificaciones y las instrucciones de pago, y cómo podrá seguir contactando con el Banco.
3. **Solicitudes sobre marketing y privacidad:** Utilice la opción para darse de baja incluida en las comunicaciones comerciales o póngase en contacto con [Cashper/CashperPlus/Fidinda] para dejar de recibirlas. Podrán seguir enviándose las comunicaciones contractuales o legales necesarias. Póngase en contacto con el DPD (más información en el apartado 9) para solicitar la supresión de sus datos o ejercer otros derechos de privacidad; el cierre de un canal no obliga automáticamente a eliminar los registros que deban conservarse legalmente.

7. Seguridad, sospecha de fraude y actividad no autorizada

Proteja su acceso.

- Utilice un dispositivo y un navegador actualizados, una conexión a internet segura y una contraseña exclusiva.
- Mantenga su dispositivo bloqueado y sus credenciales en secreto.
- Compruebe la dirección exacta del sitio web y la conexión HTTPS; el HTTPS por sí solo no demuestra que un sitio web sea auténtico.
- No revele contraseñas ni códigos de autenticación de un solo uso a nadie que le llame, ni por SMS ni por correo electrónico, y no apruebe solicitudes de verificación inesperadas.
- Desconfíe de enlaces, archivos adjuntos o solicitudes de acceso remoto no solicitados, así como de peticiones para transferir dinero a una «cuenta segura».

1. **Interrumpa cualquier interacción sospechosa.** No abra más enlaces, no facilite más información ni apruebe instrucciones que no reconozca. Si su dispositivo pudiera estar comprometido, utilice otro dispositivo de confianza para ponerse en contacto con el Banco.
2. **Comuníquelo sin demora.** Llame al Banco a través de los datos indicados en el apartado 2 durante el horario de atención al cliente y explique que sospecha de un fraude, un uso indebido de su identidad, credenciales comprometidas o una actividad no autorizada.
   Solicite que se adopten medidas de protección sobre el acceso a distancia afectado y la confirmación de su comunicación. Fuera de ese horario, envíe sin demora un correo electrónico a su marca con el asunto «URGENTE — sospecha de fraude / actividad no autorizada» y llame cuando el servicio vuelva a estar disponible. El envío de un correo electrónico no implica que se hayan adoptado medidas de protección inmediatas.
   Facilite datos útiles, no claves de seguridad. Indique su nombre, una forma segura de devolverle la llamada, la referencia de la solicitud o del préstamo correspondiente, la hora del suceso y una descripción. Conserve los mensajes sospechosos y las capturas de pantalla. No envíe contraseñas, códigos de autenticación, datos completos de la tarjeta ni documentos de identidad innecesarios.
3. **Proteja otros servicios afectados.** Desde un dispositivo de confianza, cambie las contraseñas comprometidas cuando sea seguro hacerlo. Si se ven afectados otra cuenta bancaria, una tarjeta de pago, una cuenta de correo electrónico o una tarjeta SIM, póngase en contacto sin demora con los proveedores correspondientes a través de un canal verificado de forma independiente.
4. **Denuncie cualquier posible delito ante la autoridad policial competente cuando proceda.**
5. **Comunique cualquier posible violación de datos personales al DPD** utilizando los datos indicados en el apartado 9, además de comunicar el fraude. No espere a reunir todas las pruebas para trasladar su inquietud.

Cómo gestiona el Banco su comunicación: El Banco registra su comunicación, verifica su identidad por una vía adecuada, evalúa el riesgo y traslada el asunto a los equipos correspondientes. Entre las medidas de protección pueden incluirse la restricción del acceso afectado, la investigación de la actividad controvertida y la exigencia de una recuperación segura de las credenciales. El Banco evalúa sus obligaciones de notificación y le comunica los siguientes pasos pertinentes a través de un canal de contacto verificado. Las medidas adoptadas dependen de las circunstancias; comunicar una incidencia no garantiza por sí mismo un bloqueo inmediato, un resultado concreto de la investigación ni un reembolso automático. Sus derechos legales y contractuales aplicables no se ven afectados.

8. Resiliencia operativa y de seguridad

El Banco mantiene sistemas de supervisión de la seguridad, protecciones de red y de aplicaciones, actualizaciones de seguridad, mecanismos de gestión de incidentes y planes de continuidad de negocio y de recuperación ante desastres. Los mecanismos de recuperación incluyen copias de

seguridad y sistemas replicados, infraestructura alternativa y medidas para mantener las operaciones esenciales. Estas medidas están diseñadas para reducir la probabilidad y el impacto de las interrupciones y facilitar el restablecimiento seguro del servicio. No pueden eliminar todos los riesgos cibernéticos ni garantizar un acceso ininterrumpido.

Si un servicio no está disponible: Consulte el sitio web de Cashper/CashperPlus/Fidinda para ver actualizaciones sobre el servicio, evite enviar repetidamente la misma solicitud o el mismo pago y anote la fecha, la hora y los detalles del error sin revelar sus credenciales. Póngase en contacto con su marca a través de otro canal oficial, si está disponible. Si se acerca una fecha límite de reembolso, contacte sin demora con el Banco para obtener instrucciones de pago verificadas y explique el problema de acceso. Una incidencia técnica no modifica por sí misma su contrato ni su fecha de pago. Mecanismos de actualización del servicio y de acceso alternativo: [insertar detalles].

9. Datos personales, RGPD y Delegado de Protección de Datos

El Banco trata los datos personales de conformidad con el Reglamento General de Protección de Datos (UE) 2016/679 y la normativa de protección de datos aplicable. La política de privacidad de Cashper/CashperPlus/Fidinda explica las categorías de datos recogidos, las finalidades y bases jurídicas, los destinatarios, las transferencias internacionales, la conservación, las medidas de seguridad y sus derechos. En función del tratamiento de que se trate, las bases jurídicas pueden incluir la aplicación de medidas precontractuales a petición del interesado, la ejecución de un contrato, el cumplimiento de obligaciones legales, el interés legítimo o el consentimiento, cuando proceda. No todo tratamiento se basa en el consentimiento. El Banco trata los datos personales de forma lícita, leal y transparente, limita su recogida a lo necesario, mantiene su exactitud, conserva la información solo durante el tiempo justificado y aplica medidas técnicas y organizativas adecuadas.

Puede consultar la política de privacidad de Cashper/CashperPlus/Fidinda en [Política de privacidad de Cashper; Política de privacidad de Cashperplus; Política de privacidad de Fidinda]

En las condiciones previstas en el RGPD, puede solicitar el acceso, la rectificación, la supresión, la limitación o la portabilidad de sus datos, oponerse al tratamiento correspondiente, retirar su consentimiento cuando este sea la base del tratamiento y ejercer los derechos aplicables en relación con las decisiones basadas únicamente en un tratamiento automatizado. Puede presentar una reclamación ante una autoridad de control competente. Las solicitudes de ejercicio de derechos deben atenderse sin dilación indebida y, por lo general, en el plazo de un mes; las prórrogas permitidas deben notificarse dentro de ese primer mes. El derecho de supresión no es absoluto, en particular cuando la conservación de los datos siga siendo legalmente obligatoria.

Si tiene alguna pregunta o comentario sobre protección de datos o desea ejercer sus derechos individuales, póngase en contacto con nosotros en la siguiente dirección: data.officer@cashper.es,

o bien diríjase por escrito a Bank DiMare Limited (Bank DiMare Limited, The Emporium, C De Brocktorff Street, Msida, MSD 1421, Malta), por teléfono al +49 69- 120066650 (en horario laboral habitual) o a nuestro Delegado de Protección de Datos.

El Delegado de Protección de Datos de Bank DiMare es Vincent Valletta, con quien puede contactar directamente en data.officer@cashper.es.

Cómo comunicar una posible violación de datos personales o una ya detectada:

- Envíe un correo electrónico al contacto del DPD correspondiente con el asunto «Posible violación de datos personales — [marca]».
- Describa qué ha ocurrido, cuándo sucedió o se descubrió, qué información puede verse afectada y una forma segura de contactar con usted.
- Comparta únicamente la información necesaria y solicite un método seguro si se requieren pruebas sensibles.
- Si el buzón no funciona, póngase en contacto con Cashper/CashperPlus/Fidinda a través de los datos de contacto indicados en el apartado 2 y solicite que le remitan al DPD.
- No confíe en el correo electrónico para obtener una respuesta inmediata. En su caso, comunique la sospecha de fraude por separado conforme al apartado 7.