Fundación Telefónica

GUÍA DEL ALUMNO

Descubre el mundo de la banca digital

Nombre:

Gracias por acudir a nuestro taller de formación. Esperamos que te haya sido útil, además de pasar un buen rato.

Con esta breve guía **queremos que tengas en casa temas explicados, cosas aprendidas** y alguna más que quizá se haya quedado en el tintero.

A lo largo de las páginas encontrarás un resumen de los siguientes bloques temáticos, que te resultarán ya familiares:

1. **Introducción a la banca digital**
2. **Ventajas e inconvenientes**
3. **Usos de la banca digital**
4. **Sistemas de protección de datos**
5. **Prácticas de seguridad**
6. **Funcionamiento de la banca digital**

Esta guía pretende proporcionarte algunas indicaciones para tener en cuenta a la hora de desarrollar la formación en cada uno de los bloques.

Esperamos que te sirva de apoyo.

Fundación Telefónica

1

Introducción a la banca digital

1. Introducción

¿Qué es la banca digital?

La **banca digital** es el traslado de servicios bancarios tradicionales al **entorno de internet**, donde podemos realizar transacciones y consultas o contratar productos.

Se puede operar a través de la **página web** del banco o de una **aplicación** en el teléfono móvil.

Fundación Telefónica

2

VENTAJAS E INCONVENIENTES

2. Ventajas e inconvenientes

Ventajas

- Tus cuentas bancarias **disponibles** las **24 horas**, los **365 días** del año.
- **Acceso** a tu banco **a través de internet**, sin importar dónde estés.
- Sin **desplazamientos** ni **esperas**.
- **Ahorro de costes**; suele haber menos comisiones o son mucho menores.
- **Control** de movimientos bancarios.
- **Seguridad** muy alta.

Puedes respirar con tranquilidad, ya que existen sistemas muy avanzados como la encriptación, que permite que tus datos estén seguros.

2. Ventajas e inconvenientes

Inconvenientes

1. Es necesario un **aprendizaje** inicial.
2. **Falta de atención personalizada**, aunque los bancos disponen de un teléfono para dudas.
3. Posibles **problemas de conectividad**, errores puntuales de acceso o de funcionamiento.
4. **Mayor riesgo** al contratar productos financieros, pues no existe el asesoramiento de una persona experta.
5. Miedo al **fraude**.

Fundación Telefónica

3

USOS DE LA BANCA DIGITAL

3. Usos de la banca digital

A través de la banca digital tienes las **mismas opciones** de uso del banco tradicional, pero sin esperas ni desplazamientos.

3.1. Operaciones comunes

Estas son las operaciones más habituales que puedes realizar:

- Consultar movimientos

Consultar **movimientos**, así como **gastos** e **ingresos**: las aplicaciones suelen permitir desde la página de entrada ver el **saldo** del que se dispone, así como acceder a las **cuentas** para poder comprobar el extracto de cada una de ellas.

- Transferencias

  - **Realizar transferencias y programarlas** (si son pagos recurrentes).
  - Desde estas aplicaciones se pueden realizar transferencias **sin necesidad de desplazarnos físicamente** a una sucursal.
  - En caso de hacer un pago con la misma cuantía todos los meses, o cada dos meses, por ejemplo, se puede **programar** para que se haga **automáticamente**, sin necesidad de estar pendientes o de entrar en la aplicación para dar la orden.

- Bizum

Puedes usar **Bizum**, que es un sistema que permite **enviar y recibir dinero** de manera instantánea, sin comisiones.
Límites para enviar: entre 0,5 y 1.000 €. **Límite diario de envío:** ilimitadas operaciones, máximo 2.000 €. **Límite mensual de envío:** 5.000 €. **Límites para recibir:** 60 recepciones al mes, 2.000 € diarios.

- Control de tarjetas

Los **movimientos** de las tarjetas se presentan en un **espacio específico** para estas, pudiendo ver qué se ha pagado con ellas, así como el dinero que está retenido para un pago, si se trata de una **tarjeta Visa**.

3.2. Servicios

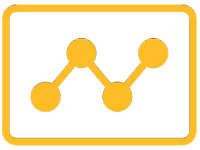
- Herramientas que facilitan el **ahorro**.

Algunos bancos permiten tener una hucha personalizable que se calcula teniendo en cuenta los ingresos o una cantidad que se indique.

- Pago de **impuestos**.

- Localizar **sucursales** cercanas.

- Visualización de **ingresos** y **gastos**.



- Domiciliación de **recibos**.

- Consulta sobre **planes de pensiones**.

- Consulta de **préstamos**.

- Búqueda e información de **productos de inversión**.

Fundación Telefónica

4

SISTEMAS DE PROTECCIÓN DE DATOS

4. Sistemas de protección de datos

Los bancos disponen de sistemas de **protección y verificación** de datos para que puedas usar sus servicios con **seguridad**.

Entrar a la aplicación es como entrar a la oficina del banco. El acceso a la sucursal se hace a través de una **puerta de seguridad**. Debes llamar al timbre o debes superar una doble puerta. En el caso de la aplicación bancaria también hay un acceso seguro con distintas opciones.

Las aplicaciones bancarias, por precaución, se cierran automáticamente después de unos minutos de inactividad, pero esto no quiere decir que no se deba cerrar la aplicación cuando ya no la estemos usando.

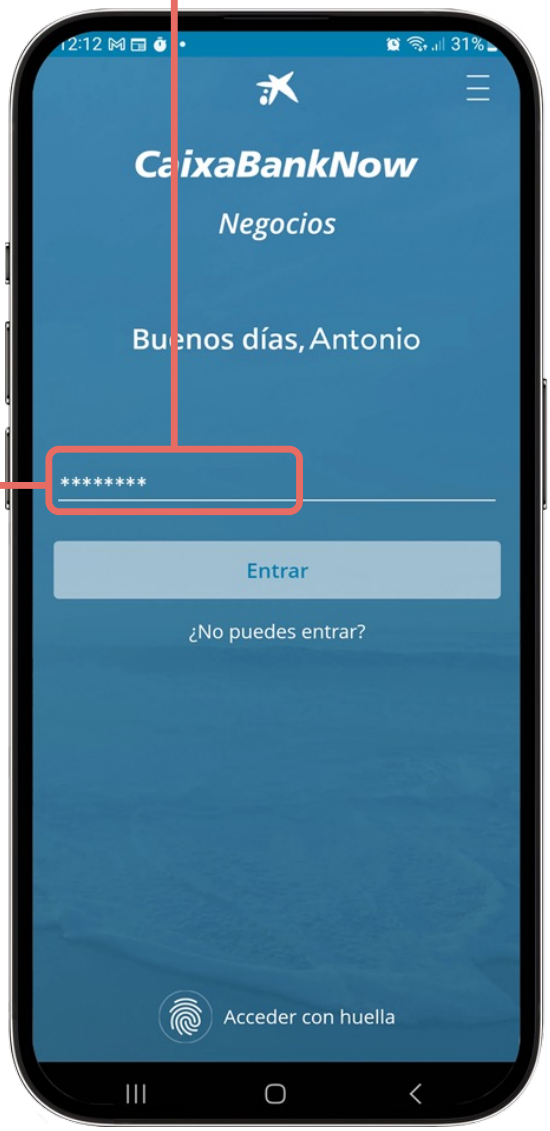
4.1. Sistemas de protección: acceso

- **Identificación a través de número PIN.**

Se trata de la credencial o contraseña compuesta habitualmente por un código de 4 a 8 dígitos.

Si tu PIN o contraseña te lo ha dado el banco, es recomendable cambiarlo la primera vez que accedas a través de la configuración del perfil.

- **Identificación a través de una contraseña alfanumérica.**



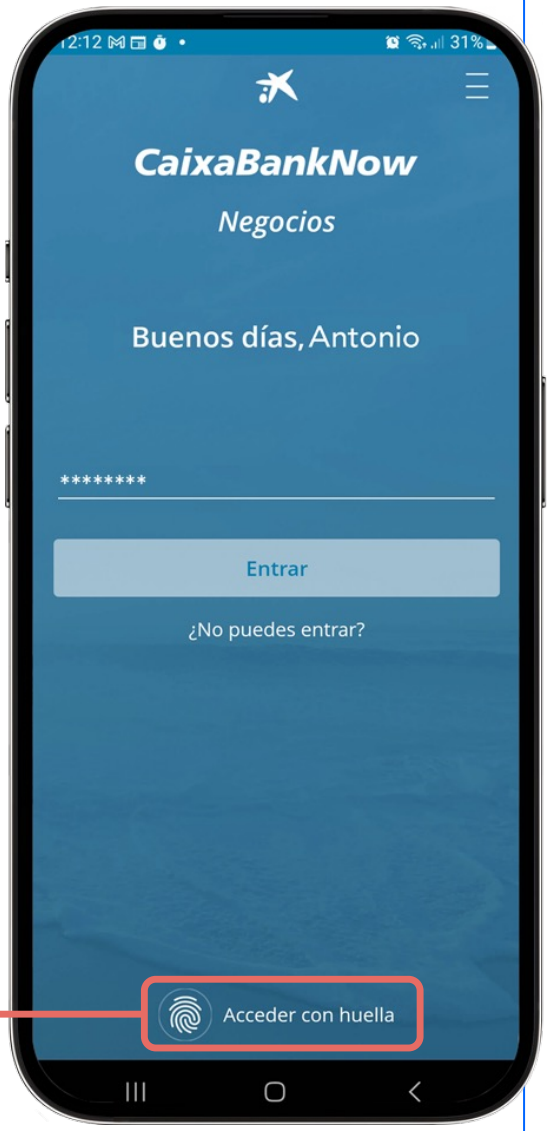
4. Sistemas de protección de datos

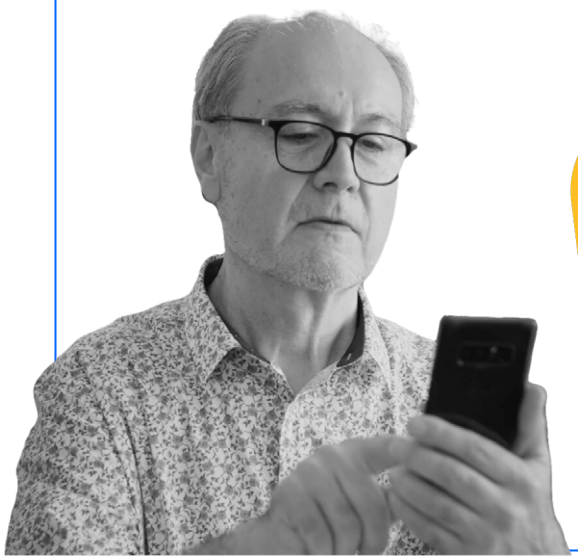
- **Identificación a través de reconocimiento biométrico.**

  Actualmente es el sistema más cómodo y seguro.

Si bien la mayoría de las entidades bancarias han introducido el acceso a través de la identificación biométrica:

- Debes tener configurado en el teléfono el acceso biométrico (para activarlo deberás ir a los ajustes del teléfono).
- El acceso biométrico no anula en ningún momento la necesidad de disponer de un PIN u otro método de identificación alternativo.





Si habitualmente no llevas **gafas** y te las pones, es posible que no te reconozca y te solicite entrar con la clave. Si tienes las manos resecas o húmedas, puede suceder lo mismo con la **huella**.

4.2. Sistemas de protección: operaciones

Cuando vas a tu **oficina bancaria** para realizar una transferencia o contratar un servicio, te piden que **firmes la documentación** de la solicitud para que el banco haga la operación.

En la banca digital sucede lo mismo: se deben **autorizar las operaciones** para que el banco lleve a cabo la orden y verifique que eres tú quien lo ha solicitado.

Para ello existen diferentes tipos de validación digital segura.

Firma o clave digital

Es una contraseña alfanumérica o un código numérico de longitud variable, dependiendo de la entidad bancaria.

Hay bancos que disponen de una aplicación específica para realizar la firma.

La firma electrónica es distinta al PIN de acceso a la aplicación. Incluso aunque puedas utilizar el mismo código, no es recomendable hacerlo por seguridad.

Código de verificación

Cuando vas a realizar la operación, recibes un **SMS** en el teléfono con un **código** (numérico o alfanumérico) que debes introducir cuando lo solicita la aplicación para aceptar la operación.

El código recibido por SMS es distinto cada vez.

Tarjeta de coordenadas

Ya **casi en desuso**. Se trata de una tarjeta con información organizada por **coordenadas**.

A la hora de realizar la operación, la aplicación te solicitará el **número correspondiente** a una **casilla**.

Es una **medida dinámica**, ya que cada operación que vayas a realizar solicitará una posición distinta y, por tanto, un número nuevo.

Llave de acceso o *passkey*

Es la última **innovación** que se está implementando poco a poco en las aplicaciones bancarias y en otros servicios digitales.

Este método utiliza **tecnología criptográfica** y tiene la virtud de ser más seguro que los otros métodos.

También es más **cómodo**, ya que para usarlo solo necesitas el reconocimiento de **datos biométricos** o el mismo **código** que usas para desbloquear tu teléfono.

Criptografía: es una técnica de codificación y cifrado de datos con el fin de que la información solo sea visible para la persona a la que va dirigida.

Es decir: no hace falta recordar otra **contraseña** para el banco, ni tarjetas de **coordenadas**, ni esperar a que te envíen **mensajes** de verificación.

En un futuro no muy lejano, el uso de llaves de acceso o passkeys podría eliminar la necesidad de que tengamos que recordar y utilizar múltiples contraseñas.

Fundación Telefónica

5 PRÁCTICAS DE SEGURIDAD

5. Prácticas de seguridad

Con objeto de **prevenir riesgos** y **aumentar la seguridad** de sus usuarios, las entidades bancarias han puesto en marcha una campaña de **información** con buenas prácticas y avisos para que sepamos detectar posibles **fraudes**.

Uso del dispositivo

- Accede desde la **aplicación oficial** del banco.

La aplicación se descarga desde la tienda oficial de aplicaciones: Play Store para **Android**, App Store para **iOS**.
Ante la duda, mira en la página web de tu banco cuál es la app que hay que instalar, o pregunta a tu asesor bancario.

- Configura la pantalla de **bloqueo**.

Puedes ver en detalle cómo se hace en el curso de Reconectados "Mi teléfono".

- Elige una **contraseña robusta**.

Entre **8 y 12 caracteres**, incluyendo mayúsculas, minúsculas, números y símbolos.

- Conéctate desde una **red segura**.

Utiliza tu conexión de datos o una red Wi-Fi de **confianza**. Si estás conectado a una red pública—por ejemplo, en un hotel—, evita realizar operaciones que requieran **contraseñas** o **datos personales**.

- Mantén el **móvil actualizado**.

Buenas prácticas

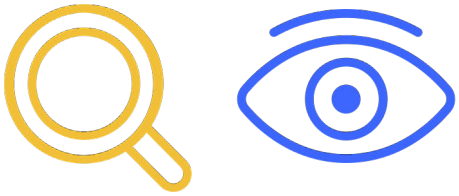
- **Lee con atención** los mensajes para autorizar operaciones.

Estos mensajes llevan reflejado el **tipo de operación** que vas a realizar. Por ejemplo, si haces una transferencia, comprueba la cuenta de origen y destino, que es el importe correcto, etc.

- No uses la aplicación con **personas desconocidas** cerca.
- No uses la aplicación en **dispositivos ajenos**.
- **No compartas** tus claves.

5.1. Identificación de riesgos

Desconfía de mensajes que solicitan una **confirmación de identidad** o que aceptes nuevas normativas.



Los mensajes sospechosos suelen ser muy **genéricos**: "Estimado cliente...", "Notificación a usuario...", "Querido amigo...".

Evita cualquier mensaje no solicitado que parezca de tu banco y contenga **ficheros adjuntos**.

Las amenazas de **fraude** pueden llegar por **cualquier canal**: teléfono, SMS, correo electrónico, WhatsApp... Incluso pueden aparentar ser mensajes de familiares y conocidos.


Sabadell

Hemos detectado una conexión con tu usuario a las 11:51 del 17/11/2024, con un dispositivo SM-A315G desde un ANDROID 10. Si no has sido tu, cambia tu contraseña en tu área de cliente pulsando aquí:

Cambio de contraseña - Área de cliente

Contacta con nosotros: 963 085 000 Solicita una cita previa.

También te atenderemos:

Certificado de seguridad:

Banco de Sabadell, S.A. - Avda. Óscar Esplá, 37, 03007 Alicante – Inscrito en el Registro Mercantil de Alicante, Tomo 4070, Folio 1, Hoja A-156980 - CIF A08000143. Dirección de correo electrónico: info@bancsabadell.com.

Ejemplos

Recibes una **llamada** de tu banco diciendo que ha habido problemas de acceso con la app y que necesitan las claves de acceso.

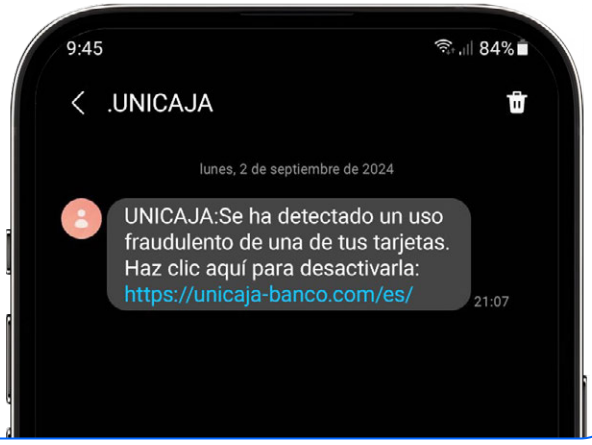
Los bancos no van a pedir nunca tus claves por teléfono.

Recibes un **mensaje** solicitando tus credenciales o datos personales, y para ello tienes que usar un enlace de internet que te envían.

Es un **fraude**. Al igual que en el caso de las llamadas telefónicas, **el banco no te va a pedir información por mensaje, ni te va a enviar enlaces de ningún tipo**.

Recibes un mensaje o correo diciendo que se han detectado movimientos sospechosos y se va a bloquear tu cuenta en menos de 8 horas a menos que entres en el enlace que acompaña al mensaje.

Es un fraude. Desconfía de cualquier comunicación que parezca una **situación de alarma** o te quiera inducir a una **acción inminente**.



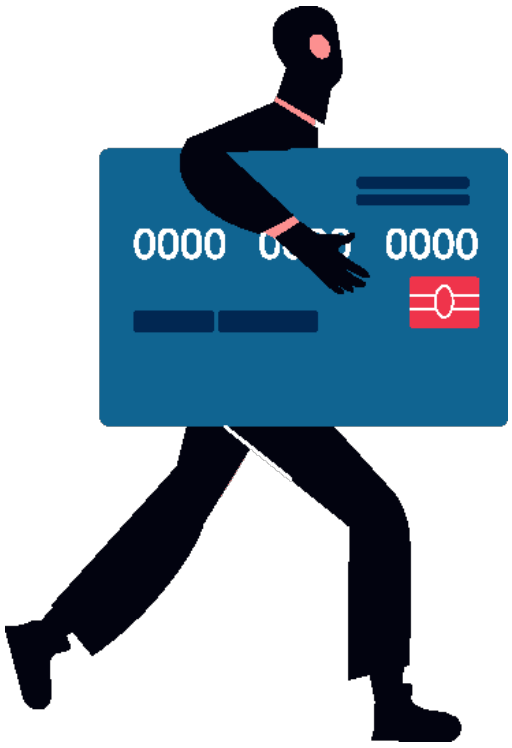
5.2. Prácticas de seguridad: qué hacer

En general, ante cualquier mensaje que te parezca **sospechoso**:

- No pinches ni descargues **archivos adjuntos**.
- No pinches en **enlaces de internet**.
- No facilites **información personal**.
- Bloquea los **números sospechosos**.

Aun con todas las precauciones, todos podemos caer en la trampa. Si tienes dudas o piensas que has sido **víctima de un fraude**:

- **Contacta** con tu banco por los **cauces habituales** (asesor online, teléfono de la oficina, etc.).
- **Denúncialo** a la policía.



Fundación Telefónica

6 FUNCIONAMIENTO DE LA BANCA DIGITAL

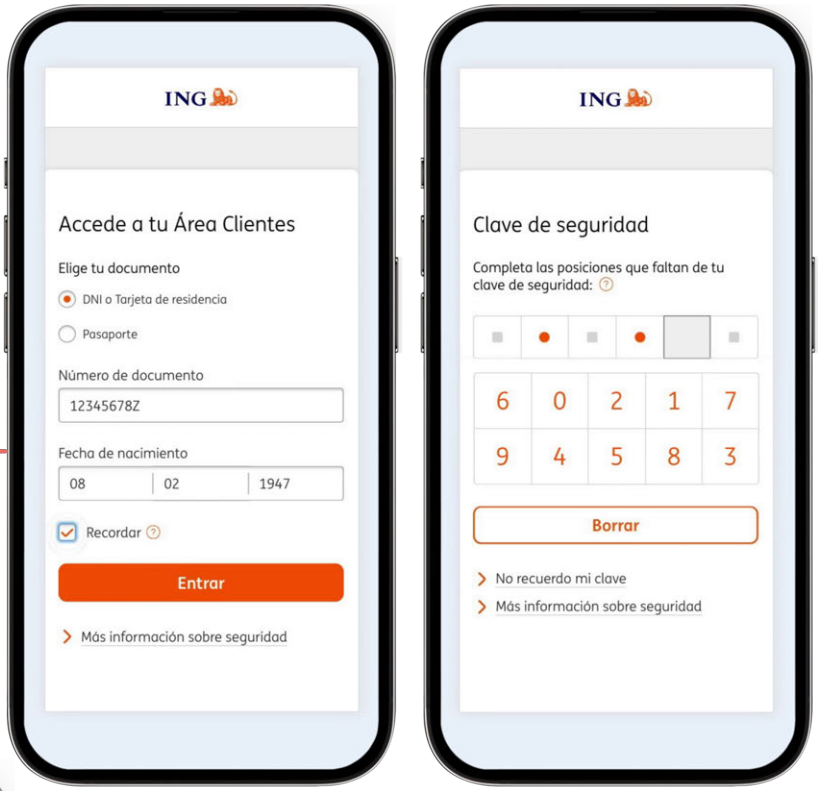
6. Funcionamiento de la banca digital

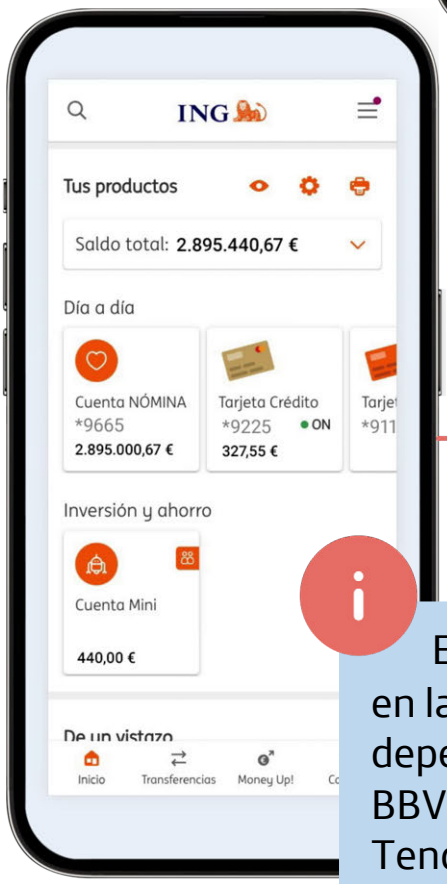
6.1. Acceso

Recuerda contectarte a internet con los **datos** móviles o a través de una **red Wi-Fi de confianza**.

Abre tu aplicación bancaria y rellena los datos identificativos necesarios, normalmente tu DNI o nombre de usuario y una contraseña.
La primera vez que entras puede pedir algún dato adicional.

1





2

La primera pantalla será tu posición global, donde aparecerán tus cuentas bancarias, tarjetas y otros servicios que tengas contratados.

En este ejemplo vemos la manera de acceder en la aplicación del banco ING. Recuerda que, dependiendo de tu banco (Santander, CaixaBank, BBVA, etc.), algunas opciones pueden variar. Tendrás las mismas funcionalidades, pero posiblemente estén organizadas de otro modo.

6.2. Posición global

Pulsa en cualquiera de tus cuentas o tarjetas para ver los movimientos y realizar operaciones:

Modo discreción: oculta las cantidades numéricas en tus saldos.

Menú general, donde tendrás acceso a tu perfil de usuario y a todas las funciones de la aplicación.

Desliza la página arriba y abajo para verlo todo.

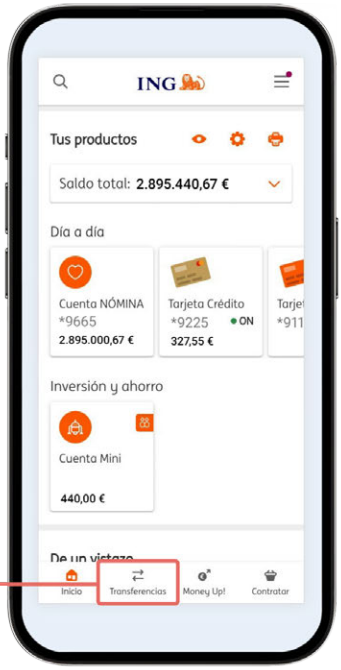
Saldo global, incluyendo todas tus cuentas.

Operaciones **frecuentes** y funciones **destacadas**.

6.3. Hacer una transferencia

1

Busca y pulsa en el apartado de Transferencias. Será un botón destacado en la pantalla principal, aunque también puede formar parte de un menú desplegable (ej, ⋮ o ☰) o encontrarse dentro de la cuenta desde donde quieres hacerla.

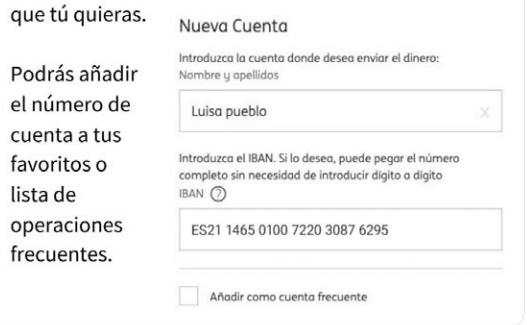


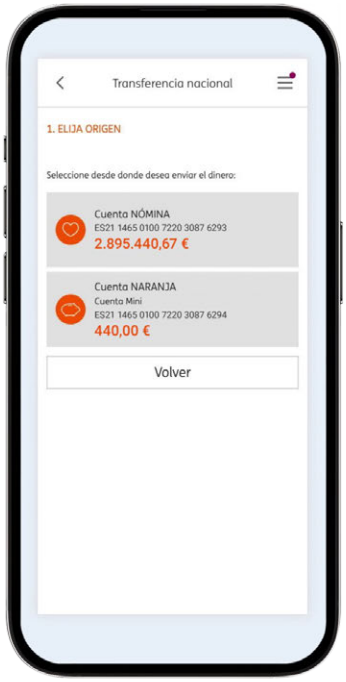
Selecciona el tipo de transferencia que quieres realizar.

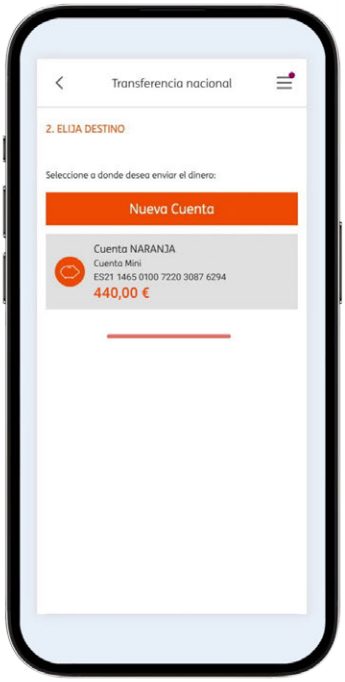
2

Selecciona la cuenta de **origen** (desde donde transfieres el dinero).
A continuación, escoge la cuenta de **destino**. Podrás escoger entre las cuentas frecuentes a donde transfieres dinero, o introducir el número de cuenta que tú quieras.

Podrás añadir el número de cuenta a tus favoritos o lista de operaciones frecuentes.







6. Funcionamiento de la banca digital

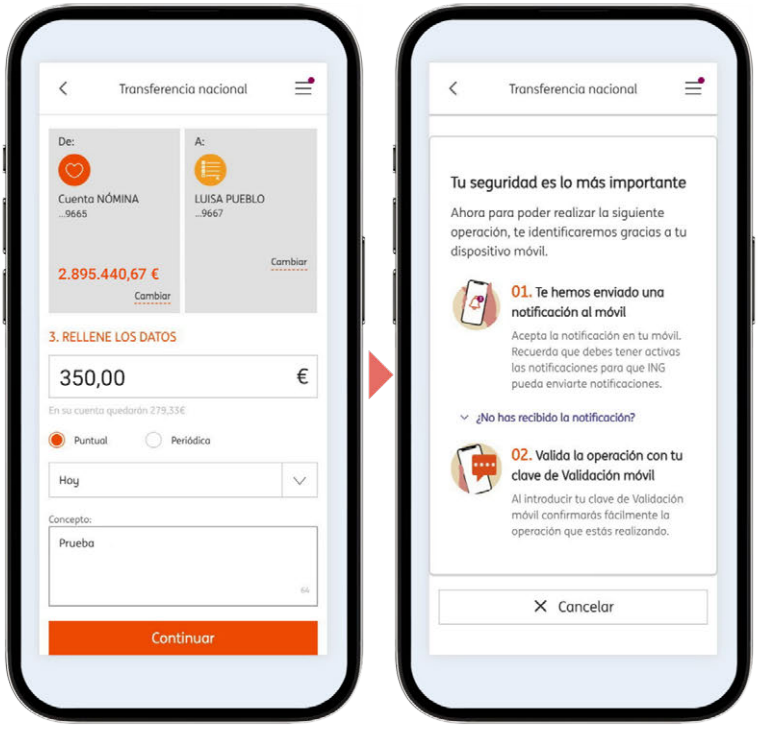
Fundación Telefónica

3

Indica la cantidad que quieres transferir, si es una transferencia puntual o periódica e introduce un concepto.

Antes de pulsar en Continuar, comprueba que estén bien todos los datos.

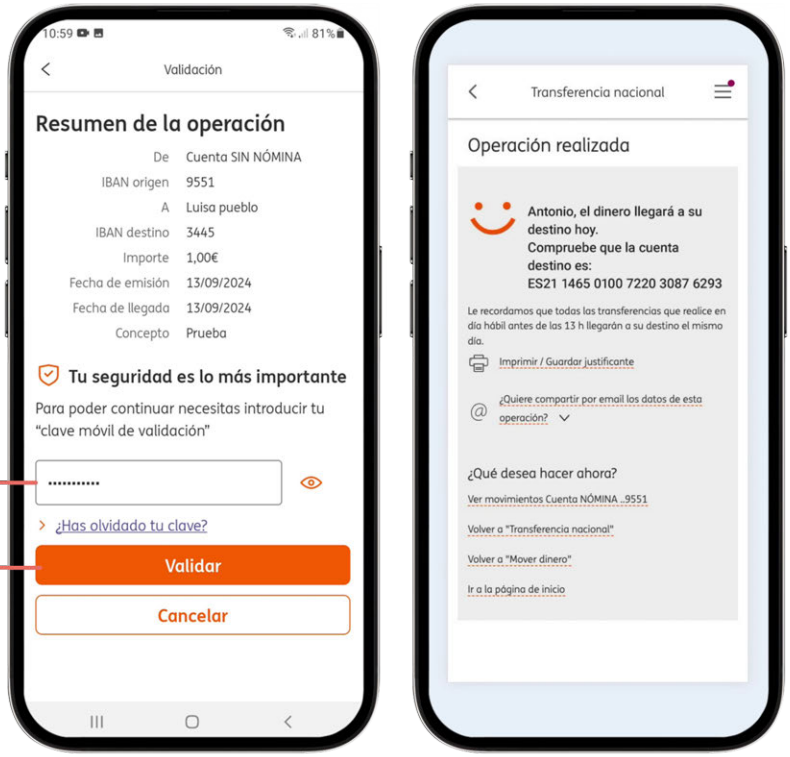
A continuación te pedirá que valides la operación empleando el método que utilice tu banco: contraseña, código temporal enviado por SMS, entrar en otra aplicación para firmar, etc.



4

En este ejemplo, el banco solicita que introduzcas tu contraseña para validar la operación.

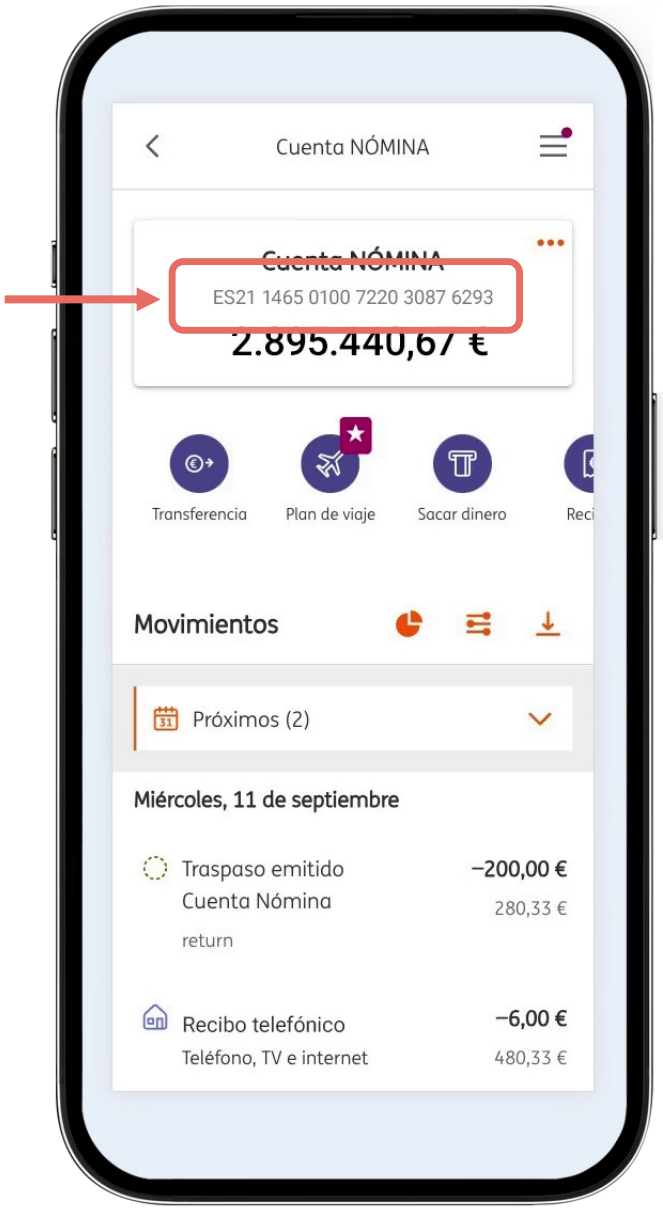
Por motivos de seguridad, la transferencia puede anularse si tardas mucho tiempo en validar la operación, pero no te preocupes, porque hay tiempo de sobra (normalmente, alrededor de cinco minutos).

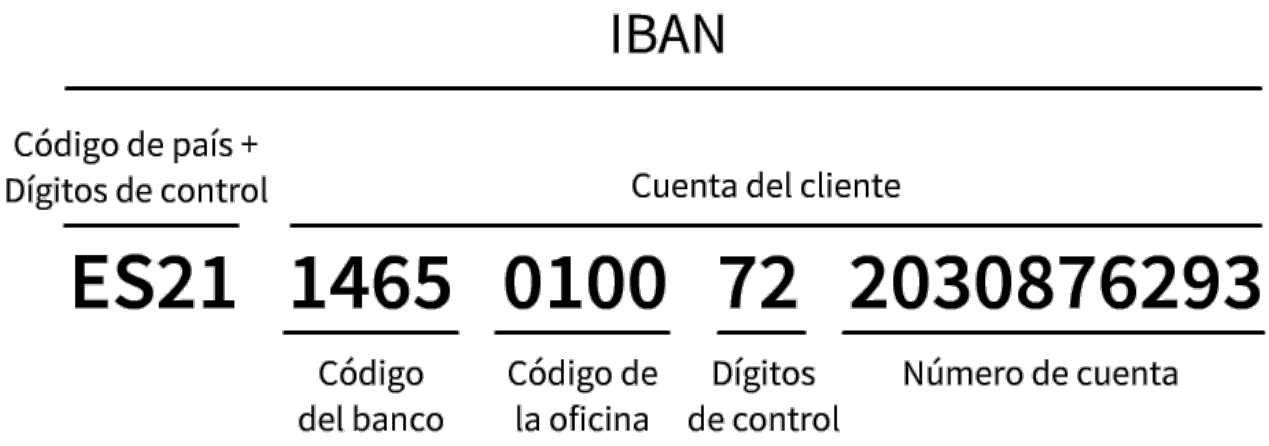


IBAN

El IBAN es tu número de cuenta normalizado en formato internacional. Está formado por el código del país (ES, en el caso de España), un código de control de dos dígitos, y a continuación los números tradicionales del número de cuenta (siempre son 20, en el caso de España).

Puedes encontrar el IBAN de tu número de cuenta accediendo a ella y normalmente habrá cerca un botón para poder copiarlo, por si necesitas pegarlo en otra aplicación.





¡Gracias!

Notas

Notas

Créditos

Esta obra ha sido editada y coordinada por Fundación Telefónica.

Puedes acceder gratuitamente a los contenidos del proyecto Reconectados de Fundación Telefónica a través de este enlace:

https://www.fundaciontelefonica.com/voluntarios/reconectados/cursos-online/


Fundación
Telefónica