

Aspectos relevantes relacionados con la seguridad

En BBVA, somos conscientes de la necesidad de **garantizar la seguridad** durante la transferencia de datos entre el banco y sus clientes. Por ello, disponemos de las máximas medidas de seguridad para garantizar la **confidencialidad de las comunicaciones**.

Asegúrese siempre de introducir sus datos en una **página segura**.

NORMAS DE SEGURIDAD

Es importante que respete las siguientes **normas de seguridad** cada vez que se le solicite información personal a través de Internet:

1. Asegúrese de que la **conexión** se realiza a través de un **servidor seguro** comprobando alguno de los siguientes aspectos:

- La dirección (URL) del servidor, ya que la dirección de un servidor seguro comienza por https, no por http.
- Una indicación de su navegador, que se encuentra en una de las esquinas inferiores de la ventana: una **llave entera** (en lugar de rota, como aparecería en cualquier servidor no seguro) o un **candado cerrado** (en vez de abierto, como aparecería en cualquier servidor no seguro).

2. **Compruebe** los **certificado de seguridad** de la página:

- Para ello, haga clic en el icono del candado que aparece al acceder a una zona segura en la parte inferior derecha de su navegador, y asegúrese de que la fecha de caducidad y el dominio del certificado están en vigor. Entre la información que se indica, se encuentra el emisor, el período de validez y para quién se ha emitido el certificado.

Para que las siguientes medidas sean eficaces, es necesario utilizar las versiones más recientes de los siguientes navegadores:

- Internet Explorer
- Firefox
- Chrome

Además, el sitio web debe haber sido optimizado para una resolución de pantalla de 1280 x 800 píxeles o superior, para una mejor visualización.

SERVIDOR SEGURO

Los sistemas de transacciones de los servicios operan en un servidor seguro que utiliza el **protocolo SSL** (Secure Socket Layer), que se activa siempre en el momento de entrar en el sistema de servicios. El servidor transmite **los datos cifrados** mediante algoritmos de 128 bits, que garantizan que solo sean **inteligibles para el ordenador del cliente y el servidor del banco**.

Mediante el uso del protocolo SSL, garantizamos:

- Que el cliente comunica sus datos al centro servidor de BBVA.
- Que, durante la transferencia entre el cliente y el centro servidor de BBVA, los datos están encriptados, evitando así la posible lectura o manipulación por parte de terceros.

ACCESO A BBVA.BE

En BBVA, recomendamos a todos nuestros usuarios que sigan estos sencillos consejos para mantener la seguridad absoluta durante su sesión en nuestro servicio de banca a distancia.

Para cerrar su sesión en BBVA.BE, siempre debe utilizar el botón "Desconectar" de la barra de herramientas de BBVA.BE y hacer clic en "Aceptar" en la ventana que aparecerá.

De este modo, la sesión en BBVA.BE se cierra de forma segura y, en su próxima conexión a BBVA.BE, se le volverá a solicitar su número de usuario y su código de acceso.

Si no **cierra la sesión correctamente**, el servidor no considerará la sesión como cerrada hasta que haya expirado el período de tiempo determinado (tiempo de espera), lo que permitirá la **desconexión automática**. Si cambia de página en Internet sin seguir estos pasos, se podrá acceder directamente a su espacio personal en BBVA.BE sin introducir sus credenciales de acceso durante el período de tiempo que transcurre hasta la desconexión automática.

MEMORIA CACHÉ

La memoria caché del navegador permite el acceso de manera casi inmediata a las páginas Web que ha visitado recientemente.

A veces, esta posibilidad puede causar algunos **incidentes menores** en el correcto funcionamiento de las páginas. Es posible que, mediante su ordenador personal, **la última versión que se muestre sea la última versión almacenada en la memoria caché** y no la última versión almacenada en el servidor de este sitio web.

Para evitar estos problemas, le recomendamos que active en su navegador la opción de **actualizar el contenido en cada visita a la página** y que, con una determinada frecuencia, elimine todos los archivos de la carpeta de **archivos temporales de Internet**.

SEGURIDAD DE LOS CÓDIGOS

Asesoramiento

- No comparta con nadie los códigos que utiliza en BBVA.BE.
- El nombre de usuario y la contraseña deben ser diferentes. De esta manera, será más difícil para un tercero conocerlos o adivinarlos.
- Si piensa que alguien podría adivinar su contraseña, debe cambiarla tan pronto como sea posible.

Almacenamiento de códigos de acceso en los equipos

- Actualmente, los navegadores ofrecen la opción de **guardar los códigos y contraseñas** para los sitios web que requieren de ellos, que quedan almacenados en la memoria de su ordenador. **Esta práctica**, a pesar de que hace más fácil el acceso a los sitios que requieren nombre de usuario y contraseña, se **desaconseja** encarecidamente cuando los códigos almacenados corresponden a bancos o a otros servicios que, en caso de pérdida o sustracción de dichos códigos, pueden causar **graves daños a los usuarios**.
- En BBVA, le recomendamos que a nuestro servicio de banca a distancia en su equipo. Este puede ser objeto de ciertos **ataques** que pueden **enviar los códigos a otros** ordenadores conectados a Internet.

Para **borrar los códigos almacenados** en un ordenador, solo tiene que seguir una serie de pasos simples que puede consultar en el **manual de ayuda de su navegador**.

Prevención y detección de ataques de virus

Los **virus** son programas cuyo objetivo es **instalarse** en el ordenador de un usuario **sin que este haya dado su permiso y/o tenga conocimiento de ello**. Hay varios tipos de virus, pero todos tienen en común que se propagan y difunden, en el mismo equipo y en toda la red.

Es fácil contribuir sin saberlo a la propagación de un virus, mediante la transferencia de mensajes de correo electrónico que contengan archivos adjuntos infectados por el virus. **La colaboración de todos** los usuarios de Internet es fundamental para **prevenir la propagación** del virus en la red.

Hay muchos tipos de archivos que pueden estar infectados por virus: le recomendamos que no confíe en las extensiones de archivo como .exe, .com o .bat y que solamente **ejecute** en su ordenador personal **aquellos archivos** que procedan de un remitente **de confianza**.

Le recomendamos **que no descargue** en su ordenador **archivos que no hayan sido verificados y certificados** y **que no abra correos electrónicos procedentes de destinatarios desconocidos**.

Precauciones

- Configure correctamente **la seguridad del sistema y la conexión** a Internet y compruebe regularmente el nivel de seguridad de la conexión. No modifique la configuración de seguridad de su equipo a menos que disponga de los conocimientos adecuados. En ese caso, configure todos sus equipos y su software con los niveles de seguridad más altos.
- Asegúrese periódicamente de que su sistema operativo, su navegador y todo el software que utiliza habitualmente **estén actualizados**.
- Instale un **cortafuegos** y un software **antivirus** y asegúrese de actualizarlos periódicamente.
- Realice **copias de seguridad** periódicas de los archivos.
- Si utiliza conexiones **combinadas** (por ejemplo, ADSL y cable), **apague el ordenador** cuando cierre la sesión. De este modo, evitará la exposición de su equipo a posibles ataques.
- Asegúrese de que las páginas web en las que deba introducir datos confidenciales sean **seguras**: para ello, compruebe los iconos del candado y la llave, y que la dirección comienza por https.
- Antes de seleccionar un **vínculo** en una página web, **asegúrese** de que le remite a la dirección deseada. También es habitual incluir vínculos en un correo electrónico que parecen remitir a un sitio web legítimo, pero que le dirigen a un sitio web que no tiene nada que ver con la empresa de la cual procede el mensaje, si se examinan con mayor atención. Manténgase alerta, incluso cuando el diseño del sitio web parezca legítimo.
- Ponga especial atención y cuidado a la hora de **descargar software**: en caso de duda, no permita descargas desde sitios que no sean completamente de su confianza
- Configure su **correo electrónico** para recibir solo los mensajes en formato de texto. No ejecute ningún archivo adjunto desde el correo electrónico con el cuál se le ha enviado. Trate de guardar el archivo en su disco duro y, si está infectado, el antivirus lo detectará. Rechace los archivos procedentes de chats o grupos de noticias que no haya solicitado de antemano. Encripte los mensajes y archivos importantes.

PROTECCIÓN DE DATOS

En BBVA, **garantizamos la protección de los datos** de nuestros clientes.

El distintivo de la Asociación Española de Certificación Electrónica (ACE) nos acredita como la **primera entidad financiera que se** adhiere a su **Código ético de protección de datos en Internet**.

El sitio web de BBVA (Banco Bilbao Vizcaya Argentaria) en Bélgica, www.bbva.be, no reconoce automáticamente ninguna información sobre la identidad de los visitantes de sus páginas. Para los servicios de banca a distancia, con el **fin de garantizar la seguridad y confidencialidad de las transacciones**, el usuario debe **identificarse y autenticarse** a sí mismo en el sistema **mediante sus código de acceso**. En caso de que el usuario solicite información sobre nuestros servicios o productos o desee iniciar un proceso de reclamación o queja mediante el envío de formularios incluidos en páginas web de BBVA, será necesario en todos los casos registrar los datos personales básicos para que podamos responder a su petición.

Todos los datos se transfieren con absoluta confidencialidad, y **no son accesibles para terceros** para ningún fin distinto de aquel para el que se han solicitado. Para más información o para realizar un comentario personal sobre la aplicación de los derechos de acceso, cancelación, rectificación y oposición previstos en la ley belga sobre protección de datos de carácter personal, puede ponerse en contacto con nosotros a través de:

bbvabe@bbva.com, número de teléfono +32 (0)2 512.32.62 o por correo postal a BBVA, sucursal en Bélgica, Atención al Cliente, Avenue des Arts 43, 1040 Bruselas.