



En BBVA somos conscientes de la necesidad de garantizar el tránsito de información entre el Banco y sus clientes. Por este motivo, BBVA cuenta con las máximas medidas de seguridad para garantizar la confidencialidad de las comunicaciones entre el Banco y el cliente. Los servicios transaccionales funcionan sobre un servidor seguro utilizando el protocolo SSL (Secure Socket Layer), que se activa siempre al entrar al servicio. El servidor seguro establece una conexión de modo que la información se transmite cifrada mediante algoritmos de 128 bits, que aseguran que sólo sea inteligible para el ordenador del cliente y el servidor del banco; de esta forma, al utilizar el protocolo SSL se garantiza:

- Que el cliente está comunicando sus datos al centro servidor de BBVA y no a cualquier otro que intentara hacerse pasar por éste.
- Que entre el cliente y el centro servidor de BBVA los datos viajan cifrados, evitando su posible lectura o manipulación por terceros.

Siempre debe comprobar que está introduciendo sus datos en una página segura. No olvide seguir las siguientes normas de seguridad siempre que le sean solicitados sus datos personales por Internet:

1. Verifique que la conexión se está realizando a través de un servidor seguro comprobando alguno de los siguientes aspectos:

- Mediante la dirección (URL) del servidor, ya que en un servidor seguro comienza por https: cuando normalmente lo hace por http.
- Mediante una indicación de su programa navegador consistente en que en una de las esquinas inferiores de la pantalla aparece una llave entera (en vez de rota como en cualquier servidor no seguro) o un candado cerrado (en vez de abierto como en cualquier servidor no seguro).

2. Compruebe los certificados de seguridad de la página en que se encuentra:

- Para ello, pulse en el icono del candado que aparece al acceder a una zona segura, en la parte inferior derecha de su navegador, y verifique que la fecha de caducidad y el dominio del certificado están vigentes. En la información de detalle aparece el emisor, el período de validez y para quién se ha emitido el certificado.

Para que estas medidas sean efectivas, es necesario que el navegador utilizado por el cliente sea alguno de los siguientes:

- Internet Explorer 6 y superiores.
- Firefox 3 y superiores.
- Chrome 4.0

Además, para permitir una mejor visualización, la web ha sido optimizada para una resolución de pantalla de 1280x800 píxeles o superiores.

Y recuerde que BBVA nunca le enviará por correo electrónico solicitud de que informe sus datos personales. En caso de recibir un mensaje en este sentido, por favor, no facilite dato alguno y contacte inmediatamente con el teléfono de BBVA 902 18 18 18.

## I. ASPECTOS DE ESPECIAL IMPORTANCIA RELATIVOS A LA SEGURIDAD.

### I.1. Utilización de la Memoria Caché y de las Utilidades de Almacenamiento de Claves en su Ordenador.

I.1.1. Memoria Caché del Navegador.

I.1.2. Almacenamiento de Claves en Ordenadores.

### I.2. Medidas para Potenciar la Seguridad en sus Accesos a BBVA.es.

I.2.1. Información Relativa a la Seguridad de sus Claves.

I.2.2. Desconexión de BBVA.es.

I.2.3. Ingeniería Social.

### I.3. Cifrado de Datos en BBVA.es.

I.3.1. Acceso a BBVA.es - Conexión Segura.

### I.4. Prevención y Detección de Ataques de Virus Informáticos.

I.4.1. Virus Informáticos.

I.4.2. Tipos de Ataques Informáticos.

I.4.3. Precauciones para Evitar Posibles Ataques Informáticos.

I.4.4. Difusión de Virus.

I.4.5. Síntomas en Ordenadores Atacados por un Virus Informático.

### I.5. Utilización de Tarjetas en Internet y en el Comercio Electrónico.

I.5.1. Tarjetas Virtuales.

### I.6. Protección de Datos Personales.

I.6.1. Política de Protección de Datos del BBVA.

## II. ENLACES DE INTERÉS.

### I. ASPECTOS DE ESPECIAL IMPORTANCIA RELATIVOS A LA SEGURIDAD

#### I.1. Utilización de la Memoria Caché y de las Utilidades de Almacenamiento de Claves en su Ordenador.

##### I.1.1. Memoria Caché del Navegador.

Esta memoria, le permite a su navegador acceder de manera casi inmediata a aquellas páginas web almacenadas en ella, es decir, aquellas páginas que Vd. ha visitado recientemente.

En ocasiones, esta posibilidad puede provocar algunos pequeños incidentes en el correcto funcionamiento de las páginas que Vd. visita, pues lo que Vd. verá a través de su ordenador personal puede no ser la última versión almacenada en el servidor de dicha página web, sino la almacenada en la memoria caché de su ordenador (esto es especialmente importante en aquellas páginas, que entre sus particularidades está la de tener un determinado periodo de tiempo de vigencia, como por ejemplo, las páginas de BBVA.es).

Para evitar estos inconvenientes, le recomendamos que marque en su Navegador la opción de "actualizar contenidos cada vez que se visita la página", y que con una cierta periodicidad (una vez por semana), elimine todos los archivos de la carpeta de archivos temporales de Internet (consulte el manual de su navegador).

### I.1.2. Almacenamiento de Claves en Ordenadores.

Actualmente los navegadores ofrecen a sus usuarios la posibilidad de guardar las claves y contraseñas de los sitios web que las requieren, quedando éstas almacenadas en la memoria de su ordenador. Esta posibilidad es especialmente delicada si el acceso a ese equipo es compartido por varias personas; de la misma forma que Vd. nunca pondría la clave de su tarjeta de crédito al alcance de otras personas, le recomendamos que no las guarde en un ordenador al que pueden acceder varias personas (ej. cibercafés, puestos de trabajo, etc.).

Esta práctica aunque facilita los accesos a los sitios donde es solicitado un número de usuario y clave, es completamente desaconsejable cuando lo que se almacenan son las claves de sus bancos u otros servicios que en caso de pérdida o sustracción pudieran provocar graves daños a los usuarios.

Por eso desde BBVA.es recomendamos no guardar nunca sus claves de acceso a nuestro servicio de Banca a Distancia en su ordenador, porque aun en el caso de que Vd. sea la única persona con acceso a dicho ordenador, éste puede ser objeto de ciertos ataques informáticos que puedan enviar sin su consentimiento dichas claves a otros ordenadores conectados a Internet.

Si Vd. tiene almacenadas sus claves en su ordenador y desea borrarlas, deberá realizar una serie de sencillos pasos que podrá consultar en el manual de ayuda de su navegador.

## I.2. Medidas para Potenciar la Seguridad en sus Accesos a BBVA.es.

### I.2.1. Información Relativa a la Seguridad de sus Claves.

El PIN de su tarjeta BBVA, su clave de acceso a BBVA.es, y su clave de operaciones en BBVA.es, son claves privadas, que deberá custodiar de forma segura, pues todo aquel que pudiera acceder a sus claves podría operar con sus productos y servicios en BBVA. Por este motivo le recomendamos que no comunique a nadie bajo ningún concepto dichas claves. Nadie en BBVA conoce cuales son sus claves, éstas se encuentran almacenadas en nuestros sistemas cifradas con un algoritmo irreversible, de forma que nadie en BBVA puede conocerlas.

Asimismo le recomendamos que su PIN, clave de acceso y clave de operaciones de BBVA.es sean distintas entre sí, con el fin de dificultar su conocimiento y deducción por terceras personas. En el caso que Vd. sospeche que alguien haya podido tener acceso a dichas claves, no dude en cambiarlas inmediatamente.

Por último, en caso de recibir un SMS de confirmación de una operación que no está realizando, por favor, póngase en contacto inmediatamente con BBVA en el teléfono 902 22 44 66 y si llama desde el extranjero en el + 34 91 374 7368. La rapidez de esta llamada es fundamental.

### I.2.2. Desconexión de BBVA.es.

Una vez que Vd. desee finalizar su sesión en BBVA.es, deberá terminarla utilizando siempre el botón "Desconexión" de la barra de herramientas de BBVA.es y pulsar en "Aceptar" en la pantalla que le aparecerá a continuación. Únicamente siguiendo estos pasos habrá finalizado con seguridad su sesión en BBVA.es. Así la próxima vez que entre en BBVA.es se le solicitarán de nuevo su Número de Usuario y Clave de Acceso.

En el caso de no desconectarse correctamente, el servidor no dará por finalizada su sesión hasta que no se supere un período de tiempo (time-out) en el que se activará una desconexión automática, por eso si Vd. cambia de página en Internet y visita otras webs sin realizar estos pasos, al teclear de nuevo accederá directamente a su sesión en BBVA.es, ya que ésta aún no habrá finalizado correctamente, si no ha transcurrido el período de tiempo necesario para que se active el procedimiento de desconexión automática.

Desde BBVA.es recomendamos a todos nuestros usuarios seguir estos sencillos pasos que permitirán mantener la plena seguridad de sus sesiones a través de nuestro servicio de Banca a Distancia.

### I.2.3. Ingeniería Social.

Se trata de convencer al usuario para realizar algo que en realidad no debería hacer. Por ejemplo, una práctica común consiste en llamar o escribir un email (phishing) al usuario haciéndose pasar por un administrador del sistema y solicitarle sus claves de acceso y operaciones con alguna excusa. Por su seguridad, es fundamental que Vd. no revele sus datos (nº de usuario y claves de acceso y operaciones) a nadie, ni por correo electrónico ni a través del teléfono, Vd. es el único que conoce sus claves de acceso y operaciones. **Nadie en BBVA conoce ni debe conocer cuales son sus claves.**

## I.3. Cifrado de Datos en BBVA.es.

### I.3.1. Acceso a BBVA.es - Conexión Segura.

En BBVA somos conscientes de la necesidad de garantizar el tránsito de información entre el Banco y sus clientes. Por este motivo, BBVA cuenta con las máximas medidas de seguridad para garantizar la confidencialidad de las comunicaciones entre el Banco y el cliente.

**Recuerde que BBVA nunca le solicitará ni por correo electrónico, ni por teléfono ni por SMS que informe de sus claves de BBVA.es. Sus claves de BBVA.es son secretas y únicamente Vd. debe conocerlas para su utilización exclusiva en la propia BBVA.es ([www.bbva.es](http://www.bbva.es)).**

En caso de recibir un mensaje en este sentido, no facilite dato alguno y contacte inmediatamente con BBVA en el 902 18 18 18.

Los servicios transaccionales funcionan sobre un servidor seguro utilizando el protocolo SSL (Secure Socket Layer), que se activa siempre al entrar al servicio. El servidor seguro establece una conexión de modo que la información se transmite cifrada mediante algoritmos de 128 bits, que aseguran que sólo sea inteligible para el ordenador del cliente y el servidor del banco; de esta forma, al utilizar el protocolo SSL se garantiza:

- Que el cliente está comunicando sus datos al centro servidor de BBVA y no a cualquier otro que intentara hacerse pasar por éste.
- Que entre el cliente y el centro servidor de BBVA los datos viajan cifrados, evitando su posible lectura o manipulación por terceros.

Siempre debe comprobar que está introduciendo sus datos en una página segura. No olvide seguir las siguientes normas de seguridad siempre que le sean solicitados sus datos personales por Internet:

1. Verifique que la conexión se está realizando a través de un servidor seguro comprobando alguno de los siguientes aspectos:

- Mediante la dirección (URL) del servidor, ya que en un servidor seguro comienza por https: cuando normalmente lo hace por http.
- Mediante una indicación de su programa navegador consistente en que en una de las esquinas inferiores de la pantalla aparece una llave entera (en vez de rota como en cualquier servidor no seguro) o un candado cerrado (en vez de abierto como en cualquier servidor no seguro).

2. Compruebe los certificados de seguridad de la página en que se encuentra:

- Para ello, pulse en el icono del candado que aparece al acceder a una zona segura, en la parte inferior derecha de su navegador, y verifique que la fecha de caducidad y el dominio del certificado están vigentes. En la información de detalle aparece el emisor, el período de validez y para quién se ha emitido el certificado.
- Para que estas medidas sean efectivas, es necesario que el navegador utilizado por el cliente sea alguno de los siguientes:

- Internet Explorer 6 y superiores.
- Firefox 3 y superiores.
- Chrome 4.0

## I.4. Prevención y Detección de Ataques de Virus Informáticos.

### I.4.1. Virus Informáticos.

Se trata de programas informáticos cuyo objetivo es instalarse en el ordenador de un usuario sin su conocimiento y/o permiso. Existen diversos tipos de virus, pero todos suelen tener en común la propiedad de propagarse y difundirse, dentro del mismo equipo y a través de la red.

#### I.4.2. Tipos de Ataques Informáticos.

**Troyanos:** Introducción en un ordenador personal, enmascarado dentro de un programa, de una rutina o conjunto de instrucciones no autorizadas y desconocidas por el usuario del ordenador, que transforman el comportamiento del ordenador de manera que lo que en él se haga pueda ser visto desde otro ordenador conectado en la Red.

**Trampas (trap door) o puertas traseras (back door):** Son un conjunto de instrucciones dentro de un programa, que permiten el acceso a los mismos sin pasar ni dejar rastro en los controles de seguridad del programa. Suele tratarse de entradas que dejan los programadores creadores del programa para uso particular.

**Gusanos (Worms):** Este tipo de ataque utiliza las redes de comunicaciones para transmitirse de un sistema a otro de forma automática, utilizando las agendas de sus programas de correo electrónico.

**Bombas Lógicas:** Son aquellos programas instalados dentro de otros, cuyo código se ejecuta al realizarse una operación determinada o en una fecha concreta, provocando una serie de acciones sobre las que el usuario no tiene control. Como ejemplo de este tipo de programas, el virus informático "Viernes 13" que se ejecuta los viernes 13 de cada mes.

**Bacterias:** Programas cuyo objetivo es reproducirse dentro de un sistema hasta consumir todos sus recursos y saturar la actividad del equipo por completo.

**Bulos (Hoax):** Son los correos electrónicos que comunican ciertos rumores falsos con el único objetivo de transmitirse y aumentar la información de "baja calidad" que circula por Internet. Potencialmente no son demasiado dañinos, se trata de simples correos electrónicos que difunden un rumor y que por supuesto son fáciles de eliminar y que Vd. no debe contribuir a su propagación a pesar de sus amenazadoras consecuencias del tipo: "... en caso de no reenviar a un número determinado de direcciones de correo que Vd. conozca (amigos, familiares, etc.)...".

**Bromas (Joke):** No son exactamente un virus, sino programas descargados desde Internet y/o transmitidos por correo electrónico cuyo fin es hacer creer a quien los ha ejecutado, que su equipo ha sido infectado con un virus informático que le provocará importantes daños en su equipo y en la información almacenada en él. Se caracterizan por ser sugestivos tanto por el dibujo de su icono y su nombre.

#### I.4.3. Precauciones para Evitar Posibles Ataques Informáticos.

- Configure adecuadamente la seguridad de su sistema y de su conexión a Internet.
- Mantenga permanentemente actualizado su sistema operativo, navegador y programas de uso más extendido (Flash, Acrobat, suites de Office, etc), la mejor forma es programar que dichas actualizaciones se efectúen de forma automática.
- Instale y mantenga siempre al día y activo un firewall y un programa antivirus.
- No cambie las configuraciones de seguridad de su equipo salvo que cuente con los conocimientos apropiados.
- Compruebe con frecuencia el nivel de seguridad de su conexión a Internet (antivirus, firewall, puertos, datos sensibles en la configuración de cuentas...)
- Instale y mantenga siempre al día y activo un firewall y un programa antivirus.
- Realice periódicamente copias de seguridad de sus archivos.
- Configure su equipo y todos sus programas con los niveles más seguros que le permitan.
- En caso de utilizar conexiones con Tarifa Plana (por ejemplo ADSL y cable) apague el ordenador una vez terminada su sesión, para así evitar la exposición de su equipo a posibles ataques informáticos.
- Si su conexión a Internet es a través de su línea telefónica habitual revise como mínimo una vez al mes el Acceso Telefónico a Redes para ver la conexión. Tenga especial cuidado con algunas páginas, que son capaces de crear por sí mismas, o solicitan la instalación, de un nuevo Acceso Telefónico a Redes con un número de teléfono tipo 906.
- Actualice sus programas con las últimas versiones originales de las casas fabricantes.
- Antes de seleccionar un enlace en una página web, compruebe que este enlace le remitirá a la dirección deseada.
- Compruebe que en aquellas páginas web en las que deba introducir información confidencial, son lugares seguros (con los iconos del candado y/o la llave) y que empiezan por https:
- Preste especial atención y precaución cuando realice descargas de programas, y en caso de duda no permita esta descarga en aquellos sitios que no son de su plena confianza.
- NUNCA ejecute un archivo adjunto desde el mensaje de correo que lo ha transmitido, intente guardar este archivo en su disco duro y en caso de estar infectado el antivirus lo detectará. Es fundamental tener instalado y actualizado un Antivirus y un Firewall en su ordenador.
- Cifre sus mensajes y archivos más importantes.
- Rechace aquellos archivos de los chats o grupos de noticias que no haya solicitado previamente.
- Configure su cuenta de correo para recibir únicamente mensajes en formato texto.
- Por último, si a pesar de todas estas recomendaciones Vd. tiene alguna duda sobre un archivo, correo o página web es mejor no abrirlo o ejecutarlo antes de permitir el comienzo de un ataque informático.

#### I.4.4. Difusión de Virus.

Vd. puede contribuir sin conocerlo a la difusión de virus, mediante el reenvío de correos electrónicos con archivos adjuntos infectados con algún virus informático. Es fundamental la colaboración de todos los usuarios de Internet para evitar la propagación de virus informáticos a través de la red.

Existen diversos archivos que pueden estar infectados con virus, pero desconfíe de aquellos cuyas extensiones sean de tipo .exe, .com, .bat, que aunque son los más frecuentes, sólo debe ejecutar en su ordenador personal cuando el proveedor de dicho archivo sea de su confianza. En este sentido, le recomendamos de nuevo que no descargue en su ordenador los archivos que no estén contrastados y certificados y que no abra los correos de destinatarios desconocidos.

#### I.4.5. Síntomas en Ordenadores Atacados por un Virus Informático.

Lista de principales síntomas que pueden observarse en una computadora que sospeche pueda estar infectada por un virus informático:

- Realización de operaciones más lentamente.
- Incremento del tiempo en la ejecución y carga de programas.
- Disminución puntual y/o permanente de forma no justificada, del espacio libre en el disco duro y de la memoria RAM disponible.
- Aparición de programas desconocidos en la memoria.

#### I.5. Utilización de Tarjetas en Internet y en el Comercio Electrónico.

BBVA pone a su disposición todos los medios a su alcance para garantizar la seguridad en su operativa con sus Tarjetas BBVA. La seguridad en sus consultas y operaciones por BBVA.es y Línea BBVA está garantizada porque se basa en un sistema de Claves Seguras. Puede activar los servicios de Banca por Internet, BBVA.es, y Banca Telefónica, Línea BBVA, simplemente conociendo los 16 dígitos de su Tarjeta BBVA y el PIN que utiliza en los cajeros (este PIN es secreto y solamente Vd. lo conoce). Para ambos servicios, BBVA.es y Línea BBVA, una vez validados estos datos, deberá definir una Clave de Acceso para acceder al servicio y una segunda clave denominada Clave de Operaciones que le permitirá realizar una amplia gama de operaciones bancarias.

Nadie en BBVA conoce cuales son sus claves, éstas se encuentran almacenadas en nuestros sistemas cifradas con un algoritmo irreversible, de forma que nadie en BBVA puede conocer sus claves.

No obstante, le recomendamos que siga estos consejos para incrementar la seguridad en el uso de las Tarjetas BBVA:

- La tarjeta debe estar firmada y es absolutamente personal e intransferible.
- Memorice su número secreto. No lo escriba nunca ni se lo diga a nadie bajo ninguna circunstancia. No utilice como número secreto datos personales fácilmente deducibles. (Ejemplos: número de matrícula, fecha de nacimiento, etc.)
- Destruya las tarjetas caducadas con unas tijeras. No las tire sin destruirlas.
- Permanezca atento a la fecha de caducidad de su tarjeta BBVA. Si no recibiera una tarjeta nueva, avise inmediatamente a su oficina BBVAo llame a Línea BBVA al 902 22 44 66.

- Al efectuar una compra, no la pierda de vista y asegúrese que le devuelven la tarjeta.
- Antes de iniciar un viaje, compruebe la fecha de caducidad y su límite de crédito, y anote el número + 34 91 374 7368 donde te atenderán en caso de que tenga cualquier problema con su tarjeta.
- Conserve una copia del justificante de la transacción y contraste los cargos reflejados en el extracto.
- En caso de encontrarse en el extranjero en una situación de emergencia, puede ponerse en contacto con Línea BBVA en el teléfono + 34 91 374 7368
- Muy importante: Denuncie inmediatamente la desaparición de su tarjeta en el teléfono 902 22 44 66 y si llama desde el extranjero en el + 34 91 374 7368. La rapidez de esta llamada es fundamental.

### **I.5.1. Tarjetas Virtuales.**

Se trata de un medio de pago diseñado especialmente para realizar compras sólo por Internet, donde la presencia física de la tarjeta no es necesaria. Sus características son:

Consiste en un número de tarjeta, con una fecha de caducidad y un número de identificación personal (PIN) elegido por Vd. No necesita soporte físico para poder hacer sus compras por Internet (sólo deberá recordar el número de tarjeta y la fecha de caducidad). Funciona como una tarjeta de prepago, es decir, sólo tiene que hacer una carga antes de utilizarla, y las compras irán siempre contra el saldo cargado, no pudiendo sobrepasarlo. El límite máximo de carga son 100.000 ptas. / 601,012 Euro. Su tarjeta virtual le permite acceder al servicio BBVA.es.

Para contratar las tarjetas virtuales BBVA sólo necesita indicarnos su e-mail y el número de identificación personal (PIN) que quiera asignar a su tarjeta virtual BBVA clic-e.

Es un medio de pago del sistema VISA y por tanto será operativo en comercios virtuales que admitan esta marca.

BBVA pone a su disposición dos modalidades de Tarjeta Virtual BBVA clic-e con las que le será muy cómodo y seguro realizar sus compras en Internet:

- Tarjeta Virtual BBVA clic-e Identificada.
- Tarjeta Virtual BBVA clic-e Anónima con esta tarjeta anónima, los únicos datos que se conocerán al realizar el pago de bienes o servicios en Internet serán el número de la tarjeta y la fecha de caducidad de la misma, sin posibilidad alguna de poder asociar estos datos con la identidad de la persona física o jurídica propietaria de la tarjeta.

### **I.6. Protección de Datos Personales.**

#### **I.6.1. Política de Protección de Datos del BBVA.**

En BBVA garantizamos la protección de los datos de nuestros clientes. El sello de la Asociación de Certificación Electrónica (ACE), nos avala como la primera entidad financiera adherida a su Código Ético de Protección de Datos en Internet. El Web de BBVA, Banco Bilbao Vizcaya Argentaria, en [www.bbva.es](http://www.bbva.es), no reconoce de modo automático ningún dato referente a la identidad de los visitantes de sus páginas. En los servicios de Banca a Distancia, con el objeto de garantizar la seguridad y confidencialidad en las transacciones, es necesaria la previa identificación y autenticación del usuario en el sistema, a través de la solicitud de claves de acceso. En aquellos supuestos en que el usuario solicite información sobre servicios o productos o desee realizar tramitación de reclamaciones o incidencias, a través del envío de formularios residentes en las páginas web de BBVA, será en todo caso necesario recoger aquellos datos personales imprescindibles para poder informarle sobre su solicitud.

Todos estos datos son tratados con absoluta confidencialidad, no siendo accesibles por terceros para finalidades distintas para las que han sido solicitados. Cualquier consulta o comentario personal dirigidos al ejercicio de los derechos de acceso, cancelación, rectificación u oposición que reconoce la Ley 15/99 LOPD puede remitirlos a: [atencion.clientes@grupobbva.com](mailto:atencion.clientes@grupobbva.com), o por escrito a BBVA Servicio de Atención al Cliente, Apdo. Nº 1598 FD 28080 Madrid.

### **II. ENLACES DE INTERÉS**

- [OSI \(Oficina de Seguridad del Internauta\).](#)
- [Centro de Respuesta a Incidentes de Seguridad\(INTECO-CERT\)](#)
- [Gestión Fraude Electrónico INTECO-CERT.](#)