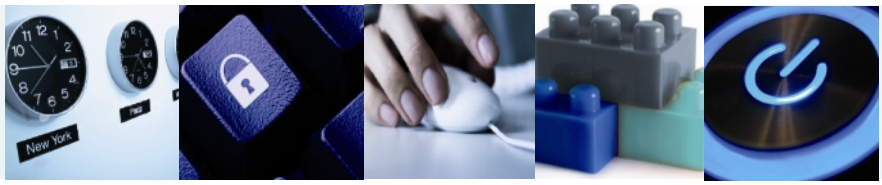
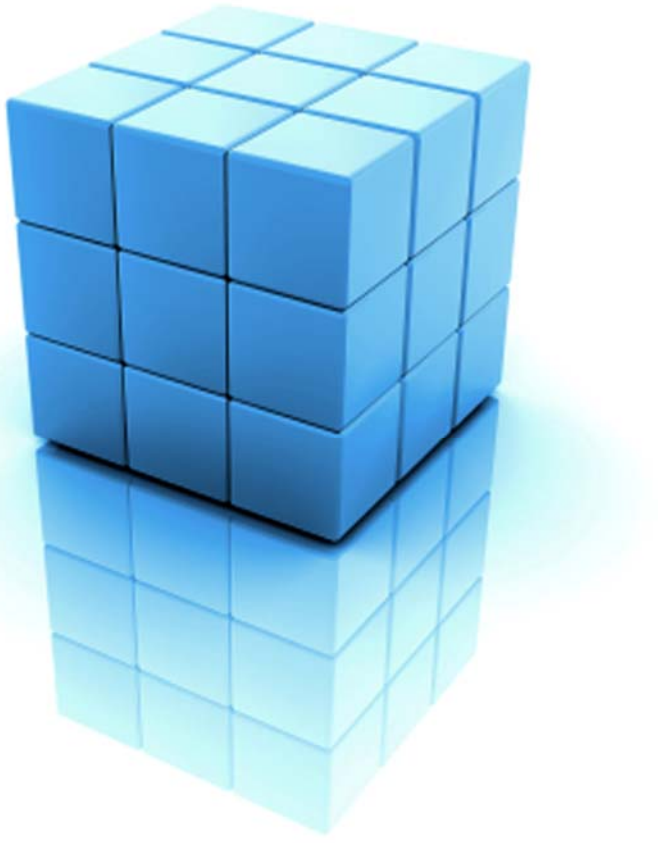
BBVA net cash

Seguridad en BBVA net cash





Índice de contenidos

1. Introducción

Las nuevas posibilidades que proporciona la acelerada evolución de Internet resultan evidentes. Posibilidades que nos permiten en BBVA net cash completar, día a día, nuestra ya nutrida y flexible gama de servicios online y, a su vez, **abren las puertas al desarrollo de nuevas formas de fraude** y estafa cada vez más avanzadas.

En BBVA net cash, conscientes de estas amenazas, **mantenemos una permanente vigilancia y trabajamos en extremar las precauciones** para que Ud. pueda seguir operando de forma segura. En el presente documento hemos recopilado todas las iniciativas puestas en marcha desde BBVA net cash para proteger tanto sus datos como el acceso de intrusos. Encontrará, además, una serie de recomendaciones que Ud. debe tener en cuenta para contribuir a que sus conexiones a Internet y su operativa online sea segura.

2. Medidas desde BBVA

2.1 El servicio

2.1.1 Administración de usuarios

BBVA net cash es una aplicación **multiusuario**. Dispone de distintos perfiles de usuario que la entidad puede asignar a sus empleados en función de su estructura operativa.

Un perfil específico, el **administrador, define y administra los usuarios** de la entidad en BBVA net cash. Pueden existir uno o varios administradores y contar con diferentes niveles de delegación (sin poder o con poderes solidario o mancomunado).

A cada usuario se le asigna **un perfil** que se define con el máximo nivel de detalle. En el caso de la autorización de operaciones, las opciones son:

- **Sin poder:** no puede autorizar operaciones.
- **Apoderado:** puede ser solidario o mancomunado.
- **Auditor:** puede frenar incluso las órdenes firmadas totalmente hasta que no tengan su autorización.

Esta estructura permite que el **circuito de usuarios** sea **tan restrictivo como desee la entidad**, con el fin de garantizar, en todo momento, que cada uno de ellos:

- acceda sólo a los servicios y cuentas que establece el administrador.
- pueda realizar sólo aquellas consultas y operaciones que le autorice el administrador.
- tenga o no poderes para autorizar operaciones.
- disponga de un límite monetario en función de la operación y cuenta, según defina el administrador.
- sólo si es administrador, pueda consultar, además de su perfil, la relación de usuarios definidos en su entidad, sus perfiles, el acceso a servicios y los poderes que tienen asignados.

2.1.2 Control de actividad

Los usuarios pueden realizar un seguimiento de la operatoria de la entidad en BBVA net cash a través de:

- el módulo de **Estadísticas (*Ficheros>Estadísticas*)**: consulta de las operaciones realizadas en un período determinado.
- la **Auditoría de órdenes (*Ficheros>Auditoría*)**: control de la actividad de operaciones de cada usuario de la entidad.
- la **Auditoría de usuarios (*Administración y control>Administración de usuarios>Consulta auditoría*)**: refleja qué actuaciones ha realizado cada uno de los administradores dentro del circuito de usuarios.

2.1.3 Credenciales de usuario en BBVA net cash

● Para la **firma de operaciones**, BBVA net cash ofrece al usuario **opciones distintas** de firma para que pueda seleccionar la que mejor se adapte a su operativa. Así, el usuario definirá si **su modo de firma es mediante clave** de operaciones (contraseña de nueve caracteres) **o mediante firma por fórmula** (aplicación de una fórmula aritmética al número que BBVA net cash le indique).

● **Doble factor de seguridad**: consiste, básicamente, **en la incorporación de un dispositivo de seguridad**, en este caso Token Plus, **para la validación en el circuito de usuarios y la firma de operaciones** a través de BBVA net cash. De esta forma y con este fin, el sistema le solicitará que introduzca el código de seguridad de seis dígitos generado por Token Plus (de uso único) además de su clave de firma. El dispositivo es personal e intransferible, se entrega uno por usuario firmante.

Adicionalmente, el sistema le solicitará que informe su número de teléfono móvil para, **en caso de pérdida o robo** del dispositivo Token Plus, **recibir su código de seguridad vía SMS** y seguir operando con normalidad.

En caso de que fuera necesario, BBVA pone a su disposición un modelo especial de Token Plus **habilitado para usuarios con discapacidad visual.**

● Para mayor seguridad, **la clave de acceso y la clave de operaciones** en BBVA net cash son **diferentes**. Aunque las contraseñas no caducan, le recomendamos modificarlas cada mes.

● El **tamaño de la clave de acceso** es de 8 caracteres **alfanuméricos** para dificultar su deducción por terceros mediante la prueba de opciones.

● Las contraseñas se almacenan **cifradas irreversiblemente** en sistemas especializados de gestión de usuarios e identidades, de forma que nadie puede obtenerlas ni deducirlas.

Obligatoriedad de modificar la clave de acceso en el primer acceso: para prevenir la suplantación del usuario, en su primera conexión a BBVA net cash, se le requiere que modifique su clave de acceso.

Bloqueo de usuarios:

● El **error** en la introducción del usuario o la clave de activación **cinco veces seguidas**, provoca el bloqueo de la referencia en BBVA net cash que no podrá ser activada hasta que BBVA no genere una nueva clave de activación.

● En el caso de la **clave de acceso y la de operaciones**, tras **tres intentos fallidos**, el usuario queda bloqueado.

- El error en la introducción del **código de seguridad generado por Token Plus** cinco veces seguidas, provoca el bloqueo del usuario en BBVA net cash.
- El administrador de usuarios tiene autonomía para bloquear el acceso a usuarios de su entidad, de modo que, ante cualquier baja de un empleado, **el acceso puede ser inmediatamente revocado.**

2.1.4 Identificación y autenticación

Trazabilidad de las transacciones: los accesos y transacciones realizadas quedan reflejadas en **registros de operaciones automatizados** que recogen la operación efectuada, la fecha y hora de la misma y el usuario que la ejecutó, permitiendo determinar la validez de las operaciones registradas.

Información de la última conexión:

- Si el usuario entra por primera vez, BBVA net cash se lo indicará.
- En sucesivos accesos, BBVA net cash mostrará al usuario la fecha y hora de su última conexión (Figura 2.1.4.1).

Figura 2.1.4.1

Cookies sólo activas durante la sesión: las cookies que se colocan en el sistema operativo del usuario, necesarias para la navegación de modo seguro por cualquier página web, están activas sólo durante la conexión a BBVA net cash y **son borradas cuando el usuario se desconecta de la aplicación.**

Desconexión automática de la sesión: como medida adicional de seguridad, a los **10 minutos** de inactividad en BBVA net cash, se procede a finalizar la sesión del usuario y desconectarlo del sistema (Figura 2.1.4.2).

Figura 2.1.4.2

2.1.5 Cumplimiento normativo de regulaciones nacionales e internacionales

BBVA cumple en todos sus servicios con las normas y regulaciones de los países en los que opera. El compromiso de BBVA con estas regulaciones se recoge en el Código de Conducta, de obligado cumplimiento para todos los empleados.

2.2 La tecnología

2.2.1 Confidencialidad e integridad

De todas las credenciales de usuario:

- Todas las claves operativas de usuarios se almacenan **cifradas irreversiblemente** en sistemas especializados de gestión de usuarios e identidades, de forma que nadie puede obtenerlas o deducirlas.
- Los procedimientos operativos de BBVA no requieren que nadie en el Banco disponga de las claves operativas de sus clientes, por lo que **nadie las conoce ni se las solicitará** personalmente.

De las comunicaciones:

- Las comunicaciones de los servicios transaccionales y de banca a distancia de BBVA se cifran mediante **protocolo SSL de 128 bits** para preservar la confidencialidad e integridad de las comunicaciones por Internet.
- Los certificados empleados por BBVA para proporcionar este servicio son generados por **Verisign Inc.**
- Adicionalmente, las comunicaciones sensibles que tienen lugar en las redes internas de BBVA se encuentran adecuadamente protegidas según el entorno operativo y el protocolo utilizado.

De la información:

- La información almacenada en los sistemas y bases de datos internas se encuentra protegida mediante diferentes sistemas de seguridad permitiendo **el acceso únicamente a los empleados autorizados.**
- BBVA dispone de un sistema automatizado de gestión de privilegios de acceso a la información que garantiza el acceso controlado y restringido al personal autorizado.

2.2.2 Seguridad física de los Centros de Proceso de Datos

Los Centros de Proceso de Datos de BBVA están dotados con amplias **medidas de seguridad física** para la protección de los sistemas de proceso de datos, destacando, entre otras, las siguientes:

- CPD bunkerizado.
- Control de accesos individualizado al recinto y a las diferentes salas técnicas, dotados de sistemas de detección de elementos peligrosos.
- Equipos humanos de vigilancia física y vídeo vigilancia del perímetro y el interior de las instalaciones en régimen de 24x7.
- Sistemas de detección y protección específicos ante intrusión, incendio, inundación, corte de suministros y otros eventos catastróficos.

Además, al disponer de dos Centros de Proceso de Datos plenamente operativos, BBVA **garantiza la salvaguarda y recuperación de la información**, en caso de que fuera necesario.

2.2.3 Arquitectura de seguridad

Con el fin de conseguir la máxima seguridad en el diseño de sus sistemas, BBVA ha dispuesto una **arquitectura de seguridad específica** especialmente para aquellos que dan servicio a sus clientes a través de Internet.

En concreto, y para minimizar el nivel de exposición hacia Internet, **sólo se mantiene expuesta la capa de presentación** (que realiza las funciones de autenticación de usuario, autorización de acceso a aplicaciones web y control seguro de sesión) mediante proxy inverso de seguridad.

2.2.4 Sistemas específicos de protección

Cortafuegos y sistemas antivirus y anti-intrusos permanentemente actualizados:

- BBVA realiza una **segregación de sus redes** y sistemas con **varios niveles de cortafuegos.**
- Además, los sistemas internos de BBVA se encuentran permanentemente protegidos mediante **sistemas antivirus y de detección de intrusión.**
- Ambos tipos de sistemas se gestionan en régimen de 24x7 y se encuentran **permanentemente actualizados**, lo que permite prevenir la acción de nuevas amenazas de forma permanente.
- Todos **los sistemas** de vigilancia, alerta y respuesta de seguridad ante posibles fraudes son **monitorizados y supervisados** por un equipo de especialistas en régimen de 24x7x365 en las instalaciones del Centro de Proceso de Datos.

Registros de actividad de todos los componentes: BBVA dispone en sus sistemas y aplicaciones de banca a distancia de registros de actividad (logs) de todos los componentes críticos, que dan soporte a los servicios de detección de intentos de fraude y análisis forense de actividades u operaciones sospechosas o reportadas como fraudulentas.

Revisión periódica del servicio aplicando las últimas técnicas de ataque: los sistemas que dan soporte a los servicios de banca a distancia son revisados periódicamente mediante herramientas de análisis automático de vulnerabilidades.

Auditorías internas y externas: los sistemas y procesos de BBVA son objeto de auditorías de seguridad periódicas tanto por parte del departamento independiente de Auditoría como por parte de auditorías externas específicas o asociadas con auditorías financieras o de cumplimiento.

2.2.5 La calidad como factor estratégico

El Centro de Proceso de Datos de BBVA tiene establecido un Sistema de Gestión de Calidad que cumple con los requisitos de la norma UNE-EN iso 9001:2000.

El personal del CPD está formado en los procesos de calidad que dan soporte a la certificación ISO 9001:2000, y el personal clave de soporte está certificado en auditoría de calidad.

BBVA forma parte del Information Security Forum, en el que están presentes más de 270 de las principales y mayores empresas mundiales.

3. Medidas que Ud. debe tomar: recomendaciones al usuario

3.1 Protección de sus credenciales de usuario

● Sus claves de acceso y operaciones en BBVA net cash son **personales, intransferibles y secretas**, y deberá custodiarlas de forma segura. Estas claves se encuentran almacenadas en los sistemas de BBVA **cifradas** con un algoritmo y, por lo tanto, **nadie, ni siquiera BBVA, las conoce.**

● Su Token Plus es **personal e intransferible.**

● **No comunique a nadie, bajo ningún concepto,** sus claves personales y nunca las informe en páginas web distintas al entorno seguro de BBVA net cash.

● **Elija claves de difícil deducción**. Además, le recomendamos que cambie de contraseña periódicamente.

● **Desconfíe de las páginas que le soliciten datos personales**, a no ser que sean relacionados con la prestación de un servicio.

● En caso de recibir un mensaje solicitándole sus claves personales, **no facilite ningún dato** y, por favor, póngase inmediatamente en contacto con el servicio de atención al cliente de BBVA net cash:

902 33 53 73

3.2 Protección de su ordenador

● Actualice periódicamente su **sistema operativo** y la **versión de su navegador** con los parches correspondientes, para protegerlo de posibles agujeros o errores detectados.

● **Configure** su equipo y todos sus programas con los **niveles más altos de seguridad.**

● Instale, mantenga activo y siempre al día un **firewall o cortafuegos.**

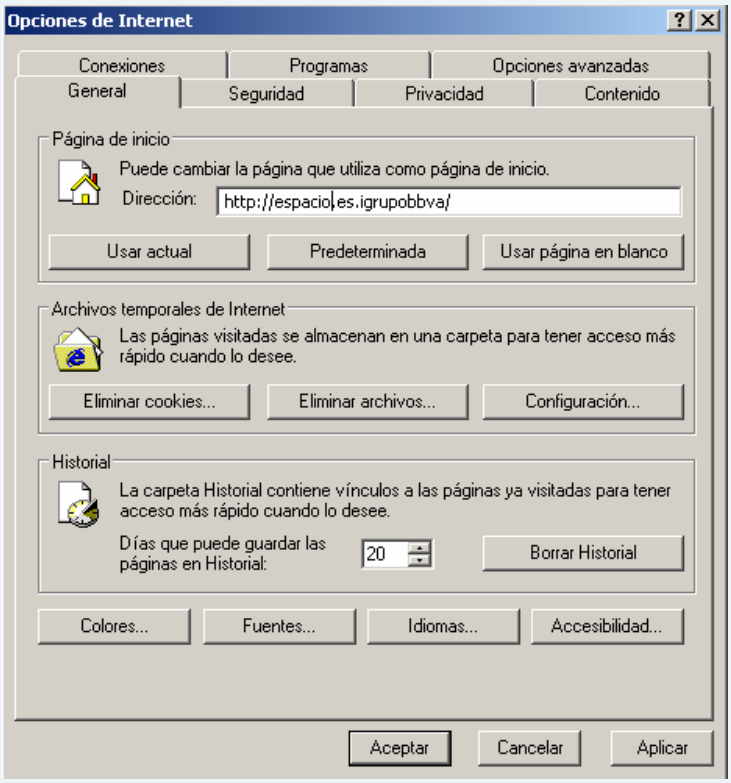
● Instale, mantenga activo y siempre al día sus programas **antivirus y antispyware.** Verifique los documentos recibidos desde el exterior con el antivirus.

● Realice periódicamente **copias de seguridad** (backup) de sus archivos.

● **Evite descargas desde páginas web desconocidas**, pues pueden contener virus o componentes espía.

● Limpie periódicamente las **cookies y los archivos temporales** (Figura 3.2.1).

Figura 3.2.1



3.3 Prácticas seguras de acceso y navegación por internet

● **Evite** conectarse a páginas de contenido privado desde **ordenadores públicos**.

● Verifique que está conectado con el **servidor seguro**. En la parte inferior de su navegador debe aparecer un símbolo de un candado cerrado.

● Compruebe el certificado de seguridad en la página web, pulsando sobre el símbolo del candado cerrado:

- ● La fecha de caducidad y el dominio deben estar vigentes.
- ● En la información de detalle debe aparecer el emisor (Verisign), el período de validez y la entidad para la que se ha emitido el certificado (BBVA).

● **No utilice la opción de "autocompletar contraseñas"** de su navegador. Si está habilitada, las contraseñas que introduce en la página web quedan almacenadas en el ordenador y, cuando vuelve a introducir su usuario, el campo de clave se rellena automáticamente. Esta opción en un ordenador de uso compartido puede provocar que alguien utilice sus claves personales.

● **Compruebe la fecha y hora de la última conexión.**

● Para finalizar con seguridad su sesión de BBVA net cash, utilice el botón <**Desconexión**> que aparece en la parte superior derecha.

4. Virus y ataques más frecuentes

Phishing: En el caso de que reciba un email solicitándole la confirmación o introducción de información confidencial relacionada con su banca electrónica (claves de entrada, firma, …), está Ud. siendo víctima de un ataque de PHISHING. Básicamente, **se define como el intento de obtener datos de acceso mediante la suplantación de la apariencia y el nombre de la entidad remitente, en nuestro caso, BBVA.**

El esquema básico de funcionamiento es el siguiente:

1. Se difunde de forma masiva un mensaje (spam) en el que se informa de que los usuarios de BBVA net cash deben confirmar sus datos de acceso.
2. El mensaje incluye un enlace a una página desde la que debe realizar la confirmación de los datos. En ocasiones, el enlace inicia la descarga de software malicioso.
3. El usuario accede al enlace que lleva a una página "similar" a la auténtica BBVA net cash y, con toda confianza, introduce en ella sus datos.
4. Como la página es falsa y está controlada por los estafadores, son ellos los que realmente reciben los datos del usuario, y con ellos tienen libre acceso a las cuenta real del usuario afectado.

Aunque BBVA nunca le solicitará sus claves de acceso y firma de BBVA net cash por correo electrónico, aquí les incluimos algunas pistas para reconocer este tipo de ataques:

1. En ocasiones, el logo parece distorsionado o estirado. Además suelen presentar faltas de ortografía o expresiones en desuso.
2. Se refieren a Ud. como "cliente estimado" o "usuario estimado" en lugar de incluir su nombre real.
3. Le advierten que su cuenta/servicio de banca electrónica se cerrará a menos que reconfirme su información de acceso inmediatamente.
4. El tono del correo resulta amenazante.
5. El texto hace referencia a "compromisos de seguridad" o "amenazas de la seguridad" y requiere efecto inmediato.
6. La url no es https:// y no aparece el candado de seguridad en la barra inferior del navegador. Los links falsos incluyen este icono dentro de la ventana para engañarle.

Pharming: En este caso, se intercepta el paso entre el nombre nemotécnico de la URL y la dirección IP devuelta, para mandar al usuario en vez de a la web de, por ejemplo, su banco a una réplica, donde los delincuentes se hacen con datos confidenciales del usuario. A diferencia del phishing no se recibe ningún email, el usuario es redirigido a una página fraudulenta cuando teclea la URL en el navegador.

Troyanos: Este tipo de virus queda latente en el ordenador del usuario y va almacenando las claves cuando éste se conecta a entidades financieras, etc y cuando ha acumulado los suficientes datos, los transmite al ciberdelincuente.

Man in the middle: El atacante es capaz de leer, insertar y modificar datos intercambiados entre el cliente y el Banco. De este modo, puede modificar los datos de una transacción por detrás (ej: cuenta de abono, importe, …), sin que el usuario sea consciente. Este último define y firma una transacción en pantalla, aunque realmente al banco le llega firmada la transacción modificada por el atacante.

5. Anexo

5.1 LOPD

En BBVA garantizamos la protección de los datos de nuestros clientes. El sello de la Asociación Española de Comercio Electrónico (AECE), nos avala como la primera entidad financiera adherida a su Código Ético de Protección de Datos en Internet. La web de BBVA, Banco Bilbao Vizcaya Argentaria. S.A., en BBVA net cash, no reconoce de modo automático ningún dato referente a la identidad de los visitantes de sus páginas. En los servicios de Banca on-line, con el objeto de garantizar la seguridad y confidencialidad de 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 páginas web de BBVA, será en todo caso necesario recoger aquellos datos personales que correspondan para poder informarle sobre su solicitud.

Todos estos datos son tratados con absoluta confidencialidad, siendo utilizados para las finalidades para las que han sido solicitados, en el marco de la Ley Orgánica de Protección de Datos de Carácter Personal y demás normas jurídicas concordantes.

BBVA net cash

BBVA net cash cuenta con un **apartado específico sobre seguridad** en su página de bienvenida privada. Ud. encontrará información sobre virus y ataques más frecuentes, recomendaciones, información sobre actualizaciones de sistemas operativos y programas antivirus, … Acceda periódicamente.
Para prevenir estos ataques, siga las recomendaciones que le indicamos y comuníquenos cualquier situación o comunicación sospechosa que reciba:

902 33 53 73

A partir de esta comunicación, el servicio de atención al cliente de BBVA net cash pondrá en marcha el protocolo de actuación ante el fraude establecido: un equipo de especialistas se encargará de analizar el caso. Si se confirma la sospecha, se le recomendará:

- Formatear su disco duro.
- Instalar un antivirus actualizado.
- Instalar un cortafuegos.
- Instalar un programa antiespía.
- Mantener actualizado el software de su equipo.

En todos los casos confirmados, se procederá al cambio de la clave de acceso del usuario afectado.