BBVA

Creando Oportunidades

Seguridad en BBVA Net cash

Client solutions

Mayo 2018

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 completa 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 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 sean seguras.

1. Medidas desde BBVA

1.1 El servicio / Administración de usuarios

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

Un perfil específico, el **administrador**, define y administra los usuarios de la empresa 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:

01	**Sin poder**	No puede autorizar operaciones
02	**Apoderado**	Puede ser solidario o mancomunado
03	**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 empresa**, 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.

1.2 El servicio / 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>** (*Firmas y ficheros>Estadísticas*): consulta de las operaciones realizadas en un período determinado.
- La **<Auditoría de órdenes>** (*Firmas y ficheros>Firma y seguimiento de ficheros*): control de la actividad de operaciones de cada usuario de la entidad.
- La **<Auditoría de usuarios>** (*Administración>Auditoría*): refleja qué actuaciones ha realizado cada uno de los administradores dentro del circuito de usuarios.

1.3 El servicio / Credenciales de usuario

BBVA Net cash incorpora el **doble factor de seguridad que consiste**, básicamente, en la **incorporación de un dispositivo**, token, para la validación en el circuito de usuarios y la firma de operaciones. De esta forma, el sistema le solicitará que introduzca el código de seguridad de seis dígitos (de uso único) generado por el dispositivo. Este dispositivo puede ser físico o estar instalado en su teléfono móvil (mediante la descarga de la app de BBVA Net cash*).

*Entornos Android/iOS. Si dispone de un terminal Blackberry/Windows Mobile debe descargarse la app de BBVA Token.

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

- Aunque las contraseñas no caducan, le recomendamos modificarlas cada mes.
- El **tamaño de la clave de acceso** es 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, tras tres intentos fallidos, el usuario queda bloqueado.
- El error en la introducción del código de seguridad generado por su dispositivo de seguridad 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.**

1.4 El servicio / 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.

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.

1.5 El servicio / 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.

1.6 La tecnología / 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** 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.

1.7 La tecnología / 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 Tier IV Gold en sostenibilidad operativa.
- 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.

1.8 La tecnología / 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.

1.9 La tecnología / 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 antimalware 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 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. Medidas que Ud. debe tomar: recomendaciones

2.1 Protección de sus credenciales de usuario

- Utilice **contraseñas complejas y de difícil deducción**, que contengan mayúsculas, minúsculas y números intercalados.
- **No comparta** con nadie **sus contraseñas**. Las contraseñas son secretas y únicamente su propietario debe conocerlas para su utilización.
- **No apunte sus contraseñas** en post-its o cuadernos; **memorícela o utilice gestores de contraseñas** especializados. Puede encontrar programas gratuitos de este tipo en www.osi.es.
- **Desactive** la opción de **guardar contraseña** de su **navegador.** Es más seguro insertarla cada vez que acceda.
- **Cambie** sus contraseñas periódicamente. Si sospecha que alguien ha podido averiguar su contraseña de acceso, debe modificarla cuanto antes.
- **No utilice la misma contraseña en distintos** servicios (email, evernote, otros bancos, …).
- Su dispositivo físico de seguridad es **personal e intransferible.**
- En caso de recibir un mensaje solicitándole sus claves personales, **no facilite ningún dato,** y póngase inmediatamente en contacto con el servicio de atención al cliente de BBVA Net cash: 91 224 98 02/902 33 53 73

2.2 Protección de su ordenador

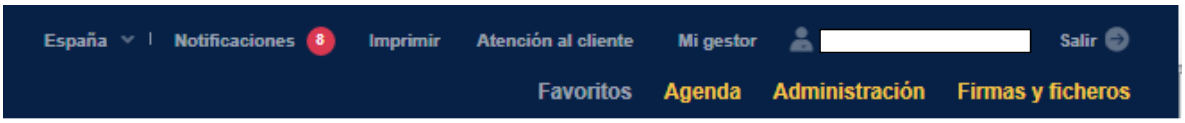
- Mantenga permanentemente actualizados su **sistema operativo y la versión de su navegador** con los parches correspondientes, para protegerlo de posibles agujeros o errores detectados.
- **Configure** su equipo y todos sus programas con los **niveles más altos de seguridad**.
- Instale, mantenga activo y siempre al día un **firewall o cortafuegos.**
- Instale, mantenga activo y siempre al día sus programas **antimalware**. 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.
- **No conecte** ningún **dispositivo externo** de **origen dudoso**, como pendrives, discos duros y móviles de desconocidos en sus dispositivos.
- Limpie periódicamente **las cookies y los archivos temporales**.
- Descargue programas y aplicaciones únicamente de **sitios oficiales.**
- Configure un **patrón de desbloqueo** en sus teléfonos móviles y tabletas, para que no pueda acceder a ellos un tercero.

2.3 Prácticas seguras de acceso y navegación por internet

- En **ordenadores comunes** o si está conectado a **wifis públicas**, **no acceda a páginas** en las que necesite utilizar usuario y contraseña. **Tampoco facilite datos personales** como dirección postal, teléfono, etc…
- Evite conectarse a páginas de contenido privado desde **ordenadores públicos.**
- **Si tiene que introducir sus credenciales**, compruebe que la dirección (URL) del servidor comienza por **https**, esto significa que está accediendo a un servidor seguro.
- Otra indicación de que el **servidor es seguro** es la presencia de un **candado cerrado** (en vez de abierto como en cualquier servidor no seguro) a la derecha o a la izquierda de la dirección (URL).
- **Compruebe los certificados de seguridad** de la página en que se encuentra pulsando en el icono del candado que aparece al acceder a una zona segura, o bien al certificado desde la barra de navegación, y verifique que la fecha de caducidad y el dominio del certificado están vigentes. En la información de detalle aparece el emisor (Verisgn), el período de validez y para quién 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 <Salir>** que aparece en la parte superior derecha.



3. Virus y ataques más frecuentes

Los virus informáticos son programas cuyo objetivo consiste en instalarse en el ordenador de un usuario sin su permiso ni conocimiento. 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.

Es fácil contribuir sin conocerlo a la difusión de virus mediante el reenvío de correos electrónicos con archivos adjuntos infectados. Es fundamental la colaboración de todos los usuarios de internet para evitar su propagación.

Existen varios tipos de virus, entre ellos destacamos:

Phishing: consiste en el envío de un email en el que se suplanta la identidad de una organización muy conocida, y a través del cual se solicitan los datos del usuario (dirección, datos bancarios, contraseñas,…). Parea que el usuario proporcione dichos datos, en la mayoría de los casos, es necesario que siga un enlace que aparece en el email y, una vez en esa falsa página, introduzca la información solicitada.

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:

- En ocasiones, el logo parece distorsionado o estirado. Además suelen presentar faltas de ortografía o expresiones en desuso.
- Se refieren a Ud. como “cliente estimado” o “usuario estimado” en lugar de incluir su nombre real.

- Le advierten que su cuenta/servicio de banca electrónica se cerrará a menos que reconfirme su información de acceso inmediatamente.
- El tono del correo resulta amenazante.
- El texto hace referencia a “compromisos de seguridad” o “amenazas de la seguridad” y requiere efecto inmediato.
- 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.

Ransomware: se trata de un lucrativo método de delincuencia tecnológica. Habitualmente encubiertos como “servicios de entrega de paquetería” o cualquier otra excusa creíble, se propagan a través del correo electrónico con enlaces que facilitan la instalación de programas o descarga de archivos infectados. Este virus bloquea el acceso a la información del ordenador, y pide un rescate económico que supuestamente facilitará la clave para descifrar la información.

A continuación, incluimos una serie de indicaciones para protegerse del ransomware:

- No siga enlaces ni descargue archivos adjuntos de correos que crea que son sospechosos.
- Utilice solo software legal y manténgalo permanentemente actualizado.
- Tenga siempre instalado y actualizado un antivirus.
- Realice frecuentemente copias de seguridad. En caso de que resulte infectado, podrá recuperar la información sin pagar el rescate.

Troyanos: se introducen en un ordenador personal, enmascarados dentro de un programa. Transforman el comportamiento del ordenador de manera que lo que en él se haga pueda ser visto desde el ordenador del delincuente.

Para prevenir la infección por un troyano debe seguir las mismas indicaciones que hemos comentado anteriormente con el ransomware:

- No siga enlaces ni descargue archivos adjuntos de correos que crea que son sospechosos.
- Utilice solo software legal y manténgalo permanentemente actualizado.
- Tenga siempre instalado y actualizado un antivirus.

Bulos (hoax): son correos electrónicos que comunican ciertos rumores falsos con el único objetivo de transmitir y aumentar la información de baja calidad que circula por internet. Generalmente, no son demasiado dañinos y son fáciles de eliminar.

Para prevenir estos ataques, siga las recomendaciones que le indicamos y comuníquenos cualquier situación o comunicación sospechosa que reciba: **91 224 98 02** / **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 antimalware actualizado.
- Mantener actualizado el software de su equipo.

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