BBVA

Creando Oportunidades

Net Cash

Recomendaciones de seguridad

BBVA
Creando Oportunidades

Índice

INTRODUCCIÓN....2

SEGURIDAD....2
Administración de Usuarios....2
Bloqueo Explícito de usuarios....3
Control de actividad....3
Credenciales de usuarios....3
Credenciales de Acceso....3
Teclado Virtual....4
Credenciales de Firma y Validación....4
Identificación y autenticación....5
Trazabilidad de las transacciones....5
Conexión....5
Cookies....5

TECNOLOGÍA....6
Integridad y confidencialidad....6
Revisión periódica del servicio....6
Auditorias....6

RECOMENDACIONES DE SEGURIDAD....7
Protección de credenciales de usuario....7
Protección de tus dispositivos....7
Prácticas seguras de acceso y navegación en internet....7

ANEXO: ATAQUES MÁS FRECUENTES....9

ATAQUES....9
Phishing....9
Pharming....9
Troyano....9
Keylogger....10
Man in the Middle....10

¿CÓMO PREVENIR LOS ATAQUES?....10

¿CÓMO ACTUAR EN CASO DE ATAQUE?....10

BBVA
Creando Oportunidades

Introducción

Los avances en la tecnología nos permiten maximizar las oportunidades de internet para ofrecer soluciones de gran valor añadido a nuestros clientes. Sin embargo, a medida que las soluciones online se vuelven más sofisticadas, también aumenta la complejidad de los intentos de fraude a los que pueden verse sometidos. En BBVA somos conscientes de las crecientes amenazas y de la importancia que tiene para tu negocio la seguridad en las transacciones. Por ello mantenemos una vigilancia y monitoreo permanente a la vez que trabajamos en nuevas medidas de seguridad para que puedas operar a través de internet de forma segura y fiable. En el presente documento te presentamos las principales iniciativas que se han puesto en marcha desde BBVA para asegurar la confidencialidad e integridad de tu información y para protegerla de cualquier ataque. BBVA Net Cash incorpora los más altos estándares de seguridad informática para protegerte de cualquier intrusión, externa o interna: su módulo de administración y control, la incorporación de modernos dispositivos de seguridad y las medidas de seguridad técnicas más avanzadas del mercado, hacen de BBVA Net Cash una de las bancas electrónicas más seguras del mercado. Además se incluyen en este documento una serie de sencillas recomendaciones que debe tener en cuenta en tu comercio para contribuir a la seguridad en todas las transacciones realizadas a través de BBVA Net Cash.

Seguridad

Administración de Usuarios

BBVA Net Cash es una aplicación multiusuario, dispone de distintos perfiles que pueden asignarse al personal del comercio en función de la estructura operativa.

El perfil Administrador, define y gestiona a las personas usuarias de la empresa. Pueden existir una o varias personas con este perfil y contar con diferentes niveles de delegación (sin poder o con poderes solidario o mancomunado).

A cada persona se le asigna un perfil que se define a nivel de detalle. Se procede de la misma manera para la autorización de operaciones, pudiendo ser:

- 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 o tan flexible como desee la empresa, con el fin de garantizar, en todo momento, que cada uno de estos perfiles:

- Acceda sólo a los servicios y cuentas que establece el perfil Administrador.
- Pueda realizar sólo aquellas consultas y operaciones que le autorice el perfil Administrador.
- Tenga o no poderes para autorizar operaciones.

- Disponga de un límite monetario en función de la operación y cuenta, según defina el perfil Administrador.
- Sólo si la persona es administradora, podrá consultar, además de su perfil, la relación de usuarios definidos en su empresa, sus perfiles, los accesos a servicios y los poderes que tienen asignados.

Bloqueo explícito de usuarios

Los perfiles administradores tienen completa autonomía para bloquear el acceso a usuarios de su empresa, de modo que, ante cualquier baja de personal, sospecha de intrusión o fraude interno, el acceso puede ser inmediatamente revocado o habilitado.

Control de actividad

Los usuarios con perfil de Administrador pueden realizar un seguimiento de la operatoria en BBVA Net Cash a través de:

- Módulo de Estadísticas: consulta de las operaciones realizadas en un período determinado.
- Auditoría de Operaciones: control de la actividad de operaciones realizadas por cada persona usuaria.
- Auditoria de Usuarios: refleja qué actuaciones ha realizado cada uno de los perfiles administradores dentro del Circuito de Usuarios.

Todas las acciones de gestión de usuarios llevadas a cabo en BBVA Net Cash, deberán ser validadas por los perfiles administradores correspondientes para que éstas sean efectivas.

Credenciales de usuarios

Los usuarios de cuentan con las siguientes credenciales que les identifican unívocamente tanto en el acceso como en la firma de operaciones:

Credenciales de Acceso

En la página de login de BBVA Net Cash (https://www.bbva.com.ar/empresas.html) se deberán informar los siguientes campos para poder acceder al servicio:
- Código de Empresa
- Código de Usuario
- Clave de Acceso

Código de Empresa: es el número de referencia (contrato) del cliente. Este número está compuesto por ocho dígitos numéricos y es asignado automáticamente al dar de alta el contrato.

Código de Usuario: es identificación unívoca dentro del contrato de BBVA Net Cash.

Clave de Acceso: cumplen los siguientes requisitos:

- Longitud de 8 dígitos alfanuméricos.
- No pueden contener caracteres especiales ni la letra “ñ”.
- No pueden ser iguales al código de usuario ni al número de referencia del contrato, ni al número

de documento del Usuario. Puede tener hasta tres caracteres numéricos y tres caracteres alfabéticos que sean correlativos en forma ascendente o descendente.
- Puede tener hasta tres caracteres numéricos y tres caracteres alfabéticos que se repitan.
- En caso de cambio o modificación, la nueva clave debe ser distinta a las 12 últimas utilizadas.

El Usuario está identificado por la relación Código de Empresa + Código de Usuario. Es decir, no pueden existir dos usuarios con el mismo ID, ni con el mismo Tipo y Número de Documento para el mismo Código de Empresa.

Teclado Virtual

El Cliente tiene la opción de ingresar el número Código de Empresa, el Código de Usuario y la Clave de Acceso utilizando un Teclado Virtual que le aparecerá en la pantalla. Esta opción es recomendada en los casos que la persona opere desde una PC pública para evitar la captura de la clave.

Credenciales de Firma y Validación

Los perfiles administradores con poder de validación y con poder de firma utilizarán los siguientes factores de seguridad durante los procesos de Firma de operaciones y Validación de acciones de administración:

Clave de Operaciones: se habilita de acuerdo al perfil asignado al usuario.

Para ser válida debe cumplir los siguientes requisitos:

- Longitud de 9 dígitos alfanuméricos sin uso de caracteres especiales ni la letra “ñ”. No pueden ser iguales al código de usuario ni al número de referencia del contrato, ni al número de documento del usuario ni a su Clave de Acceso.
- No pueden tener
- Puede tener hasta tres caracteres numéricos y tres caracteres alfabéticos que sean correlativos en forma ascendente o descendente.
- Puede tener hasta tres caracteres numéricos y tres caracteres alfabéticos que se repitan.
- En caso de cambio o modificación, la nueva clave deberá ser distinta a las 12 últimas utilizadas.

Para mayor seguridad, la Clave de Acceso y la Clave de Firma en BBVA Net Cash son diferentes.

Token: este doble factor de seguridad, consiste en la incorporación de un dispositivo de seguridad físico (Token) para la validación en el circuito de administración de usuarios y la firma de operaciones a través de BBVA Net Cash.

El sistema le solicitará a la persona usuaria que introduzca el código de seguridad de uso único (One Time Password) generado por su dispositivo de seguridad.
Este Token tiene las siguientes características:

- Es un código de 8 dígitos
- Caduca transcurridos 40 segundos
- Genera un bloqueo automático del dispositivo: tras un máximo de 6 intentos fallidos

Identificación y autenticación

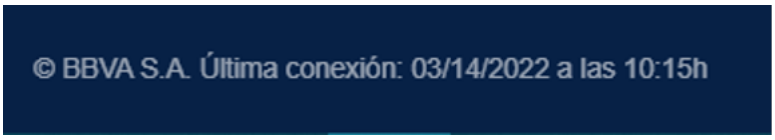
Trazabilidad de las transacciones

Los accesos y transacciones realizadas quedan reflejados en registros de operaciones automatizados que recogen la operación efectuada, la fecha y hora de la misma y la persona que la ejecutó, permitiendo determinar la validez de las operaciones registradas.

Conexión

- Información de la última conexión

Cada vez que la persona usuaria ingrese en BBVA Net Cash se le mostrará la fecha y hora de su última conexión de la siguiente manera:



- Desconexión automática

A los 10 minutos de inactividad, se procede a finalizar la sesión del usuario y desconectarlo del sistema, pudiendo indicar si quiere mantener la sesión activa o cerrarla automáticamente.

Cookies

Las cookies son: necesarias para la navegación de modo seguro por cualquier página web

Se colocan en el sistema operativo del Usuario, ,están activas sólo durante la conexión a BBVA Net Cash y son borradas cuando el Usuario se desconecta de la aplicación.

Tecnología

Integridad y confidencialidad

Asimismo BBVA cuenta con medidas tecnológicas que garantizan la integridad y la confidencialidad de las credenciales de usuario, las comunicaciones y la información que se transmite entre la empresa y BBVA.

Credenciales de usuario

- Todas las claves operativas de las personas usuarias 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.

Comunicaciones

- Las comunicaciones de BBVA Net Cash 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.

Información

- BBVA garantiza la confidencialidad de la información gestionada y almacenada en los sistemas y bases de datos de BBVA Net Cash. Asimismo, esta información se encuentra protegida mediante diferentes sistemas de seguridad permitiendo el acceso únicamente al personal autorizado.
- 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.

Revisión periódica del servicio

Los sistemas que dan soporte a los servicios de banca electrónica son revisados periódicamente mediante herramientas de análisis automático de vulnerabilidades, aplicando las últimas técnicas de ataque (hacking ético).

Auditorias

Los sistemas y procesos en 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.

BBVA
Creando Oportunidades

Recomendaciones de seguridad

A continuación se detallan una serie de sencillas medidas para que tu experiencia en BBVA Net Cash cuente con un mayor nivel de seguridad.

Protección de credenciales de usuario

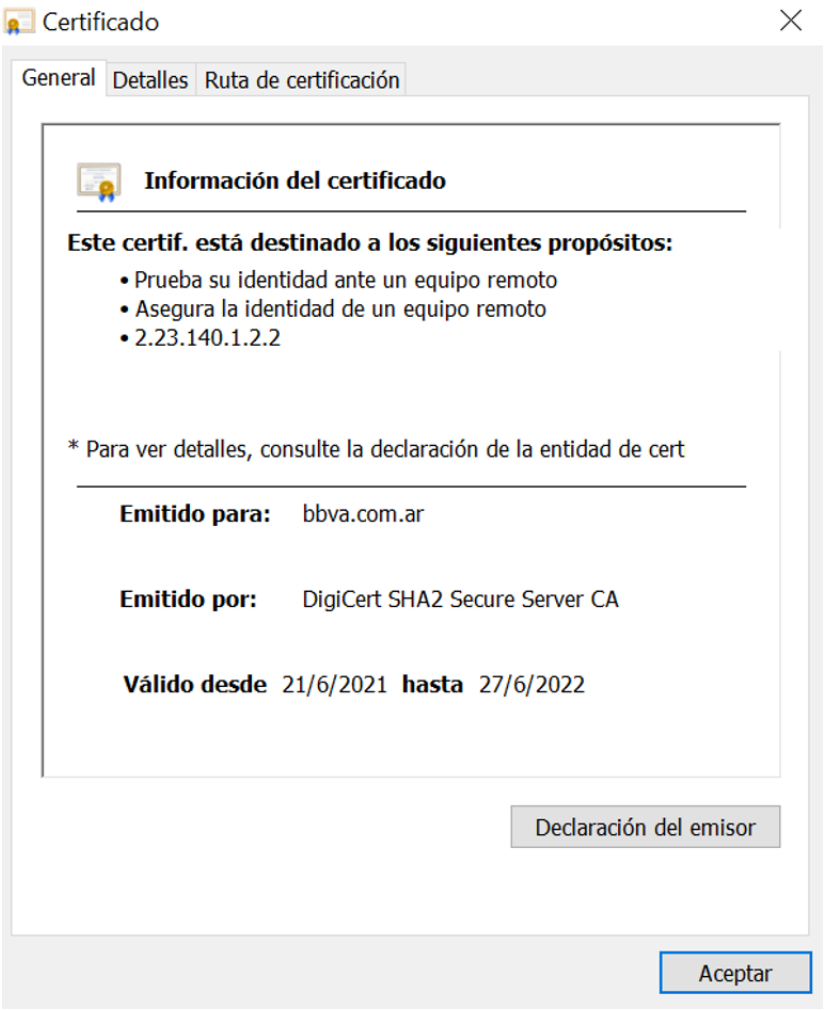
- Es importante no compartir las claves con nadie bajo ningún concepto. Nunca se deben informar en páginas web distintas al entorno seguro de BBVA Net Cash.
- Tus claves de acceso y firma en BBVA Net Cash son personales, intransferibles y secretas, deberás custodiarlas de forma segura.
- Ningún empleado/a del banco te solicitará (por llamada, correo electrónico o SMS) las claves, el Token, los números de tus cuentas, el código de seguridad u otros datos personales.
- No ingreses a páginas desde el link de un correo o mensaje. Si querés ingresar a BBVA Net Cash, te recomendamos que tipees la dirección en el navegador.
- En caso de recibir un mensaje solicitando tus claves personales, no facilites ningún dato y, por favor, comunicate inmediatamente con el Centro de Atención BBVA Empresas (CATE) al 0800-333-4646 opción 1 o por medio del Formulario de Contacto

Protección de tus dispositivos

- Actualizá periódicamente tu sistema operativo y la versión del navegador con los parches correspondientes, para protegerlo de posibles errores de seguridad detectados.
- Configurá tu equipo y todos sus programas con los niveles más altos de seguridad.
- Mantené el acceso a tus dispositivos bloqueados con una clave, PIN o huella.
- Instalá y mantené activos y siempre al día un firewall o cortafuegos y sus programas antivirus y antispyware. Verificá los documentos recibidos desde el exterior con el antivirus.
- Limpiá periódicamente las cookies y los archivos temporales.
- Realizá periódicamente copias de seguridad (backup) de tus archivos.
- Evitá descargas desde páginas web desconocidas, pues pueden contener software malicioso o componentes espía. Siempre descargá desde los sitios oficiales.
- Verificá los permisos que le otorgás a las aplicaciones.
- Desactivá las conexiones inalámbricas cuando no las estés utilizando.

Prácticas seguras de acceso y navegación en Internet

- Evitá acceder a páginas con contenido sensible desde dispositivos o WiFi públicos.
- Te recomendamos siempre teclear directamente la URL en tu navegador o utilizar la opción de Favoritos del mismo.
- Verificá que la página en la que te encontrás sea segura. Recordá revisar que la dirección cuente con un símbolo de un candado cerrado y la dirección comience con https://.
- Comprobá el certificado de seguridad en la página web, pulsando sobre el símbolo del candado cerrado. Verificá que la fecha de caducidad y el dominio se encuentren vigentes.
- En la información de detalle debe aparecer el emisor, el período de validez y la entidad para la que se ha emitido el certificado (BBVA). Lo podrás encontrar de la siguiente manera:



- No utilices la opción de "autocompletar contraseñas" de tu navegador. Si está habilitada, las contraseñas que introducís en la página web quedan almacenadas en el ordenador y, cuando vuelvas a introducir tu usuario, el campo de clave se rellenará automáticamente. Esta opción en un dispositivo de uso compartido puede provocar que alguien utilice tus claves personales.
- Para finalizar con seguridad su sesión en BBVA Net Cash, utilizá el botón "Salir" que aparece en la parte superior derecha.

IMPORTANTE:
En caso de recibir un correo electrónico, mensaje de texto, llamada telefónica, etc. solicitando sus claves personales o Token, no facilites ningún dato.

En caso de haber sido víctima de ataque o tener la sospecha de haberlo sido, contactate inmediatamente con el CATE.

Anexo: Ataques frecuentes

Son varias las modalidades a través de las cuales los ciberdelincuentes, utilizando diferentes medios, logran robar nuestros datos para luego estafarnos. Promocionando ofertas tentadoras, notificando a la persona que su clave caducó o que debe actualizar el perfil para evitar ser estafado. Hay una lista sin fin de recursos que utilizan los delincuentes para hacernos caer en su trampa entre los que podemos mencionar:

El denominado **Phishing**. Un tipo de delito cibernético cuyo objetivo es obtener información confidencial de la persona usuaria(número de cuentas, códigos, claves, etc.) para un uso fraudulento. El método más común consiste en el envío masivo de correos electrónicos, en el que los ciberdelincuentes suplantan la identidad, en la mayoría de casos, de una compañía conocida y en el que solicitan información personal y bancaria. Normalmente agregan un enlace que redirecciona a una página web fraudulenta para que el usuario introduzca la información solicitada (credenciales, números de tarjeta, etc).

Las llamadas telefónicas (**vishing**) donde los delincuentes se hacen pasar nuevamente por organizaciones conocidas y utilizan diferentes pretextos para terminar obteniendo información bancaria y personal del usuario. En la mayoría de los casos solicitan la clave Token o SMS para realizar alguna transacción. Actualmente están latentes las estafas por DEBIN, donde los delincuentes con el objetivo de pagarte una supuesta compra inducen a sus víctimas a ingresar al home banking para aceptar un DEBIN que termina debitando el monto de la cuenta y no acreditandolo.

Se conoce como **Smishing** (mensajes falsos) al delito donde los delincuentes envían por SMS o mensajes de WhatsApp enlaces o información con el objetivo de obtener datos personales de sus víctimas para luego estafarlas. Por lo general se hacen pasar por organismos oficiales que informan sobre facturas impagas, devolución de importes, descuentos tentadores, falsas alertas de seguridad, etc.

El **Pharming** es una modalidad de fraude electrónico que consiste en manipular las direcciones DNS (Domain Name Server) para conducir a la personaa una página web falsa que imita visualmente a la original. Desde aquí, los delincuentes acceden a la información confidencial del usuario.

Malware o “software malicioso” es un término que describe cualquier programa o código malicioso que tiene por objetivo robar, cifrar o borrar datos, alterar o secuestrar funciones básicas del dispositivo sin el conocimiento o permiso de la persona propietaria para asumir el control parcial del mismo. De esta manera, el delincuente solicita una suma de dinero para otorgarle nuevamente el control del dispositivo.

Cualquier empresa puede ser víctima del conocido Fraude al CEO (Chief Executive Officer) donde los delincuentes engañan a un empleado, con posibilidad de dar órdenes de pago a los bancos, para que realice una operación en su beneficio. Es una técnica que suele ejecutarse a través del correo electrónico suplantando la identidad de un proveedor habitual, de un alto directivo o socio de la empresa.Se aprovecharon de una operación existente de la compañía para realizar la estafa. Por lo general los correos demandan cierta urgencia y confidencialidad.

El registrador de pulsaciones o **Key-logger** es un tipo de software o hardware que se encarga de registrar las pulsaciones que se realizan en el teclado, para obtener contraseñas o claves cifradas y así traspasar las medidas de seguridad de las entidades financieras.

Man in the Middle, es una operación en la que el delincuente se sitúa en medio del cliente y del servidor que envía y/o recibe información del cliente. De esta forma, el ataque se produce en el mismo momento en que la información fluye y es alterada por el estafador (por ejemplo se modifica la cuenta de abono en una transacción).

¿Cómo prevenir los ataques?

Si bien desde BBVA hemos puesto en marcha medidas de seguridad para que tu negocio pueda operar de forma segura y fiable, se deben tomar las precauciones necesarias mencionadas en el punto de Recomendaciones de seguridad. Es importante remarcar a todas las personas usuarias que **en caso de recibir un correo electrónico, mensaje de texto, llamada telefónica, etc. solicitando sus claves personales, no facilite ningún dato.** En caso de haber sido víctima de ataque o tener la sospecha de haberlo sido, contactate inmediatamente con el Centro de Atención BBVA Empresas.

Centro de Atención BBVA Empresas: 0800 333 4646

Horario de atención **Lunes a Viernes de 7.30 a 18 Hs**

Formulario de Contacto