



## **Términos y Condiciones**

### **Banca Electrónica de BBVA EMPRESAS**

#### **1. INTRODUCCIÓN:**

El presente documento regula y explica las condiciones particulares del Canal **Banca Electrónica de BBVA Empresas**, disponible vía Internet en la página web [www.bbva.pa](http://www.bbva.pa), para Clientes Personas Jurídicas (**EL CLIENTE**), de **BBVA Sucursal Panamá**, en adelante denominado **EL BANCO**, así como los derechos y obligaciones tanto del **CLIENTE** como de **EL BANCO**. El presente documento contiene los parámetros generales de activación, utilización, modificación, bloqueo, personalización, medidas de seguridad, entre otros.

Sólo debe aceptarlo cuando comprenda y esté de acuerdo con su contenido. Si requiere más información, comuníquese con nosotros a través de:

■ [www.bbva.pa](http://www.bbva.pa)

■ Contact Center: (+57 )(601) 4432600 Línea de atención BBVA Sucursal Panamá.

Este documento es aplicable exclusivamente para BBVA Sucursal Panamá.

#### **2. DEFINICIONES Y CONDICIONES ESPECÍFICAS DEL SERVICIO**

La **Banca Electrónica de BBVA Empresas** es el canal a través del cual **EL CLIENTE** a través de Internet, en la página web de **EL BANCO**, [www.bbva.pa](http://www.bbva.pa) puede acceder a diferentes servicios y efectuar transacciones con sus productos de forma ágil, confiable, oportuna y segura, bien sea a través de plataformas de propiedad de **EL BANCO BBVA COLOMBIA** o de terceros contratados para la prestación de los servicios ofrecidos.

A través de la **Banca Electrónica de BBVA Empresas**, **EL CLIENTE** podrá acceder y operar los productos/servicios que tiene contratados con **EL BANCO**, entre otros: contratar nuevos productos/servicios, consultar productos y saldos, realizar pagos, transferencias, entre otros movimientos.

A través de la Banca Móvil, **EL CLIENTE** tendrá funcionalidades complementarias a la Banca Electrónica tales como la generación del Soft Token para la autorización de las operaciones permitidas dentro de la Banca Electrónica.



## 2. PARAMETRIZACIÓN DE OPERACIONES:

EL BANCO pone a disposición de EL CLIENTE, la posibilidad de personalizar y parametrizar las operaciones monetarias y no monetarias que puede realizar a través de la **Banca Electrónica BBVA Empresas**.

EL CLIENTE podrá establecer límites para transacciones desde una cuenta en Pesos de Colombia hacia Panamá y tendrá la facultad de establecer:

- División de los límites por operación;
- Límite de firma: El monto máximo permitido por transacción será el que configure **EL CLIENTE** en el módulo de “Administración de usuarios” el cual aplicará para cada usuario configurado;
- Límite Diario: El monto máximo diario para transaccionar, será el que el cliente configure en el canal en el módulo de “Modificación de límites” sobre el servicio de “Transferencia internacional Panamá”. Este límite es acumulativo por el valor de cada transacción;
- Límite Mensual: El monto máximo mensual para transaccionar, será el que EL CLIENTE configure en el canal en el módulo de “Modificación de límites” sobre el servicio de “Transferencia internacional Panamá”. Este límite es acumulativo por el valor de cada transacción.
- Configuración de IP Fija si cuenta con este servicio.
- Configuración de firmas mancomunadas, de tal manera que le permita al CLIENTE contar con un control dual antes de firmar y enviar los pagos.
- Configuración del servicio de cifrado de archivos.
- Configuración de un rango de horarios esto es: hora de inicio y hora fin para ingresar y procesar operaciones en el portal BBVA Net Cash, que permite bloquear tanto el acceso como el procesamiento de operaciones fuera de este horario.

## 3. OBLIGACIONES DE EL CLIENTE:

Con la suscripción del presente documento de Términos y Condiciones, antes de empezar a operar en la **Banca Electrónica de BBVA Empresas** y durante la vigencia de la relación con EL BANCO, EL CLIENTE se obliga a lo siguiente:

1. Configurar y realizar la personalización y parametrización de operaciones monetarias y no monetarias, en especial las siguientes: i) Creación de usuarios y asignación de atribuciones; ii) Definir los criterios de firmas mancomunadas, cuando el cliente por razones de seguridad lo estime necesario en su utilización; iii) Configurar el servicio de mensajería para envío de notificaciones sobre órdenes de pago; iv) Configurar un rango de horarios, u hora de inicio y hora fin, y días para el ingreso y procesamiento de operaciones en la Banca Electrónica de BBVA Empresas (Control de horarios); vi) Configurar las cuenta(s) ordenante para los servicios de pagos y transferencias; vii) Ajustar los límites de sus transacciones monetarias de acuerdo con el volumen transaccional, por ejemplo

por lote o archivo diario y mensual acorde al valor de las transacciones que habitualmente realiza a través de la entidad o que su actividad amerite; viii) Configurar el servicio de cifrado de archivos, cuando por razones de seguridad lo estime conveniente; ix) Establecer límites por usuario, servicio, cuenta ordenante e importes.

2. En desarrollo del deber de debida diligencia **EL CLIENTE** se obliga a informarse sobre la forma como debe implementar la personalización de operaciones y a exigir las capacitaciones y las explicaciones verbales y escritas necesarias, precisas y suficientes que le permitan la adecuada personalización de la **Banca Electrónica de BBVA Empresas**.
3. Seguir las recomendaciones impartidas por EL BANCO para el manejo de la de la Banca Electrónica de BBVA Empresas y/o de los equipos asociados al funcionamiento de la misma.
4. Cambiar periódicamente sus claves, usuarios, contraseñas y demás seguridades de acceso a la **Banca Electrónica de BBVA Empresas**, custodiarlos en debida forma, no conservarlos en su teléfono celular ni en mensajes de datos remitidos o recibidos a través del mismo, no suministrarlos a terceros no autorizados, ni almacenarlos en navegadores.
5. Mantener actualizada su información de cliente que reposa en EL BANCO, especialmente su dirección física, datos de contacto y correo electrónico entre otros.
6. No compartir el ambiente de trabajo personal con el laboral, evitando el uso de equipos empresariales para temas personales.
7. Consultar y verificar en las operaciones de pago los datos de los beneficiarios e importes antes de firmarlos y enviarlos (Nº Identificación, Nº cuenta y Banco destino), así como los registrados en los diferentes módulos de pagos (Proveedores, nóminas, traspasos, etc.) antes de firmar y enviar las transacciones. Así como eliminar aquellos que no sean reconocidos.
8. Dar aviso oportuno a EL BANCO y abstenerse de realizar transacciones en el momento que evidencie archivos de pago creados, borrados y/o modificados sin su autorización, así como también, al detectar beneficiarios o cuentas que no hayan sido creadas o cualquier otra circunstancia sospechosa o situación irregular. Por aviso oportuno se entiende el informado al Banco antes de firmar y enviar las operaciones para su procesamiento.

## 4. OBLIGACIONES DEL BANCO

Además de las obligaciones correspondientes a los productos contratados y vigentes, **EL BANCO** se obliga a:

1. Poner a disposición de EL CLIENTE la plataforma tendiente a la prestación oportuna de los servicios ofrecidos en la **Banca Electrónica de BBVA Empresas**.
2. Conservar los registros electrónicos (logs, documentos, archivos, etc.) derivados de las claves y operaciones de **EL CLIENTE**.
3. Establecer y asegurar el cumplimiento de todos los estándares y políticas de seguridad que se consideren pertinentes para habilitar el uso de la plataforma. Estos estándares y políticas se encuentran acorde a lo establecido en la

normativa vigente, especialmente lo previsto en la Circular Básica Jurídica expedida por la Superintendencia Financiera de Colombia (Parte I, Título II, capítulo I, numeral 2.3..4.11) así como lo establecido en el Acuerdo Bancario No. 006 de 2011 emitido por la Superintendencia de Bancos de la República de Panamá, aplicable para cuentas, productos y/o servicios de la Sucursal de BBVA Colombia radicada en Panamá.

4. Dar soporte a **EL CLIENTE** respecto al uso de la **Banca Electrónica de BBVA Empresas**, lo anterior a través de los canales informados por **EL BANCO**.
5. Informar al **CLIENTE** sobre cualquier modificación de los servicios ofrecidos en la aplicación y/o de los presentes términos y condiciones, lo anterior a través de la página [www.bbva.pa](http://www.bbva.pa) y a través de la aplicación donde estarán permanentemente actualizados.

## 5. MEDIDAS DE SEGURIDAD Y PRÁCTICAS DE PROTECCIÓN PROPIA:

**EL CLIENTE** se obliga a emplear la debida diligencia en el manejo de la **Banca Electrónica de BBVA Empresas** en especial, a implementar las siguientes recomendaciones de seguridad, las cuales deben ser difundidas en manuales de procedimiento a sus empleados y funcionarios, para garantizar un adecuado manejo del Canal. Las siguientes medidas, son recomendaciones mínimas que **EL CLIENTE** debe aplicar:

### 5.1. Medidas y prácticas de seguridad generales:

1. Cuando **EL CLIENTE** sea una entidad territorial o entidad pública se compromete a implementar las recomendaciones de seguridad de la información impartidas por el Ministerio de Tecnologías de la Información y las Comunicaciones, por medio de la Dirección de Estándares y Arquitectura de Tecnologías de la Información, denominado Guía 18, dirigido a las entidades públicas de orden nacional y territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno en Línea, disponible en la página del Ministerio de Tecnologías de la Información y las Comunicaciones, para elevar el aseguramiento de los equipos o terminales móviles asignados por la entidad, donde se realizan las transacciones financieras como los son: pago de nómina, pagos de seguridad social, pagos de contratación y transferencias de fondos, entre otros.
2. Configurar la(s) IP(s) fija(s) desde la(s) cuál(es) accederá a la **Banca Electrónica de BBVA Empresas** e informarla al Banco. En el caso de entidades públicas o territoriales es obligatorio, salvo que no sea posible técnicamente. En los demás casos será optativo.

3. No acceder a información (correo, web, SMS) de los cuales no se tiene certeza del remitente, ni hacer clic sobre links o descargar archivos adjuntos.
4. Consultar y verificar en las operaciones de pago los datos de los beneficiarios e importes antes de firmarlos y enviarlos (Nº Identificación, Nº cuenta y Banco destino), así como los registrados en los diferentes módulos de pagos (Proveedores, nóminas, traspasos, etc.), y eliminar aquellos que no sean reconocidos.
5. Cerrar la sesión al terminar de trabajar en la **Banca Electrónica de BBVA Empresas**.
6. Dar aviso oportuno a **EL BANCO** y abstenerse de realizar transacciones en el momento que evidencie archivos de pago creados, borrados y/o modificados sin su autorización, así como también, al detectar beneficiarios o cuentas que no hayan sido creadas o cualquier otra circunstancia sospechosa o situación irregular presentada en la **Banca Electrónica de BBVA Empresas**. Por aviso oportuno se entiende el informado al Banco antes de firmar y enviar las operaciones al banco para su procesamiento.
7. Mantener actualizados los datos de contacto, números de teléfonos, correos electrónicos y partícipes de las cuentas para alertamiento de operaciones.
8. Apagar el equipo o dispositivo dedicado a la **Banca Electrónica de BBVA Empresas**, cuando no se esté utilizando, sobre todo si dispone de una conexión permanente a Internet.
9. Notificar inmediatamente a **EL BANCO** sobre el cambio, hurto o pérdida del equipo desde el cual se conecta a la **Banca Electrónica de BBVA Empresas** y solicitar inmediatamente el bloqueo de sus canales.
10. Notificar inmediatamente a **EL BANCO** si recibe correos o mensajes extraños.
11. Notificar inmediatamente a **EL BANCO** si recibe notificaciones que no corresponden a su actividad y transacciones.
12. Requerir credenciales de autenticación para el ingreso y/o uso, las cuales deberán estar obligadas a cambiarse periódicamente y tener especificaciones mayores de seguridad de conformidad con la tecnología y mecanismos técnicos que disponga **EL BANCO**.
13. En cualquier situación extraña o sospechosa, abstenerse de realizar operaciones en la Banca Electrónica de BBVA Empresas y solicitar al Banco el bloqueo inmediato de la misma.

5.2. Medidas y prácticas de seguridad sobre los equipos de cómputo y dispositivos con acceso a la Banca Electrónica BBVA Empresas y el espacio físico dónde se encuentran:

1. En la medida de lo posible, el equipo o dispositivo desde el cual opera la **Banca Electrónica de BBVA Empresas**, deberá ser destinado de manera exclusiva para la realización de las transacciones financieras.
2. Restringir o prohibir, según corresponda el acceso remoto a los equipos o

dispositivos destinados para el funcionamiento de la **Banca Electrónica de BBVA Empresas**

3. Implementar medidas de seguridad informática para que sus funcionarios no compartan en los equipos de cómputo o dispositivos destinados al funcionamiento de la **Banca Electrónica de BBVA Empresas**, el ambiente laboral con el personal, es decir, que estos equipos o dispositivos no puedan ser utilizados por sus empleados y funcionarios para temas personales (buzones de correo personal).
4. Restringir el acceso a correos personales, redes sociales, y en general a otros sitios no asociados con las funciones del operador, desde el equipo y/o dispositivo. Esto con el objeto de evitar que de forma intencional o accidental, se descargue, instale o ejecute un software malintencionado.
5. Asegurar que el(los) equipo(s), dispositivo(s) y/o terminal(es) destinados a la operación de la **Banca Electrónica de BBVA Empresas**, cuenten mínimo con un antivirus (con módulos de anti - keylogger, firewall personal, antispymware), con software licenciado y actualizado de forma automática o supervisada, y que los equipos y sistemas operativos mantengan las actualizaciones más recientes.
6. Limitar los privilegios de la(s) cuenta(s) de usuario(s) de los equipos, dispositivos y/o terminales móviles utilizado(s) para realizar transacciones financieras, a efecto de reducir el riesgo de que con la misma sea posible la instalación de software malintencionado o controladores de dispositivos no autorizados.
7. Establecer procedimientos automatizados o por medio del soporte técnico que disponga la entidad, para efectuar el borrado regular de: archivos temporales del sistema operativo, archivos temporales de Internet, cookies, historial de navegación y descargas (se sugiere mínimo una vez a la semana).
8. Establecer los mecanismos de control necesarios para que la instalación, actualización o desinstalación de programas o dispositivos en el equipo o terminal móvil, sea realizada únicamente por los funcionarios del área de sistemas o tecnología, o el personal designado por la Entidad para este tipo de requerimientos. Adicionalmente, estas actividades deben ser revisadas y aprobadas por el funcionario que desempeñe el rol de oficial de seguridad de la información, y/o las áreas responsables de la seguridad de la información y/o los designados por la entidad para efectuar este tipo de aprobaciones.
9. Restringir la instalación de software que permite conexión remota (TeamViewer, LogMeIn, Hamachi, VCN, entre otros) evitando con esto que personas externas se puedan conectar fácilmente al equipo, dispositivo o terminal móvil desde el cual se realizan las transacciones.
10. Restringir los puertos que permitan la conexión y/o acceso a dispositivos de

almacenamiento extraíbles (CD, USB, SD Card, etc.).

11. Procurar tener instalado un solo navegador, en el que esté comprobada la adecuada compatibilidad y operación de servicios en línea de EL BANCO, con los mejores mecanismos de seguridad posibles debidamente configurados y el cual deberá estar permanentemente actualizado a efecto de garantizar la disposición de mejoras o correcciones a su funcionamiento.
12. Activar mecanismos para que el equipo, dispositivo o terminal móvil pueda recibir las actualizaciones de seguridad de forma automática, cada vez que sean emitidas por el fabricante para el sistema operativo respectivo y aplicaciones.
13. Mantener activos y en operación sólo los protocolos, servicios, aplicaciones, usuarios, entre otros, necesarios para el desarrollo de las actividades, en el equipo, dispositivo o terminal móvil destinado a la **Banca Electrónica de BBVA Empresas**.
14. No acceder a la **Banca Electrónica de BBVA Empresas** desde Wi-Fi públicas.
15. Restringir el acceso al área física desde donde se realizan transacciones financieras sólo para personal autorizado.
16. No compartir equipos de cómputo, móviles, ni dispositivos de seguridad (hard token) desde donde se realicen las operaciones a través de la **Banca Electrónica de BBVA Empresas**.
17. En lo posible, contar con cámaras de video, las cuales deben cubrir al menos el acceso principal al área y el funcionario que utilice el equipo, dispositivo o terminal móvil. Las imágenes deberán ser conservadas por lo menos seis (6) meses o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.
18. No compartir información/claves, garantizando su manejo confidencial de la información necesaria para transar.
19. Recuerde que al utilizar la Banca Electrónica en redes Wi-Fi públicas se expone a que la información necesaria para transar se vea expuesto o comprometida dado el riesgo de robo de información e infección por virus.

### 5.3. Medidas y prácticas de seguridad respecto de los usuarios con acceso a la Banca Electrónica de BBVA Empresas:

1. Garantizar que los usuarios autorizados según sus responsabilidades tengan acceso personal y exclusivo a los equipos, dispositivos y terminales móviles en los que se accede a la **Banca Electrónica de BBVA Empresas**.
2. No compartir información/claves, garantizando su manejo confidencial e intransferible.
3. Informar al Banco cualquier cambio/actualización de usuario(s) y solicitar la capacitación del (los) mismo(s), antes de permitir que este opere la **Banca Electrónica de BBVA Empresas**.
4. Controlar el tiempo de inactividad del usuario a través del bloqueo automático del equipo, dispositivo o terminal móvil (se sugiere máximo cinco minutos).



## 6. FIRMA ELECTRÓNICA

Las partes acuerdan que el requisito de firma en el presente Reglamento, de conformidad con lo dispuesto la legislación colombiana, en el decreto 2364 de 2012, así como en la Ley panameña No. 51 de 2008, queda satisfecho y tendrá plenos efectos jurídicos con la aceptación electrónica que **EL CLIENTE** haga con la utilización de:

1. Su NIP y/o Código y/o Clave; y/o
2. Imposición de huella o la utilización de cualquier otro sistema biométrico; y/o
3. La utilización de Token y/o códigos de transacción enviados a su aplicación móvil SMS o celular; y/o
4. La utilización de números de identificación personal, y/o
5. La imposición en el presente documento de Términos y Condiciones, de su firma manuscrita escaneada, y/o
6. La utilización de sistemas, y/o
7. La utilización de botones de aceptación de tipo “sí”, “aceptar” o “acepto”, y/o
8. La combinación de los anteriores mecanismos y/o cualquier otro establecido entre **EL CLIENTE** y **EL BANCO** como elemento de identificación para realizar operaciones a través de los distintos canales.

## 7. INFORMACIÓN, MODIFICACIÓN Y ACEPTACIÓN DEL DOCUMENTO:

**EL BANCO** puede darle a conocer a **EL CLIENTE** el presente documento de Términos y Condiciones, con sus anexos, sus actualizaciones y modificaciones, con la entrega personal del mismo, por envío a la dirección física o electrónica que **EL CLIENTE** haya registrado o mediante publicación en la aplicación o en la página web [www.bbva.pa](http://www.bbva.pa).

**EL CLIENTE** puede decidir libremente si lo acepta o no. No son válidas las aceptaciones parciales o condicionales.

El Reglamento, sus modificaciones o actualizaciones se entienden aceptadas por **EL CLIENTE** de las siguientes formas:

1. Si se acepta/firma electrónicamente el Reglamento, mediante cualquiera de las formas previstas en el numeral 3 del presente Reglamento.
2. Si utiliza el servicio cualquiera de los servicios disponibles a través de la Banca Móvil previstos en este Reglamento o se beneficia de ellos en cualquier forma. Por utilización se entiende el hecho de beneficiarse **EL CLIENTE** del servicio. No habrá lugar a aceptaciones condicionales o parciales.
3. Si **EL CLIENTE** no se opone al contenido del mismo, cancela su servicio o termina su relación comercial con **EL BANCO** dentro de los 45 días calendarios siguientes a que el Reglamento, sus modificaciones o actualizaciones sea publicado.

Este documento y sus actualizaciones reemplazan los que se hayan publicado o se le hayan comunicado anteriormente a **EL CLIENTE** sobre este servicio. **EL BANCO** puede modificarlo o actualizarlo en cualquier momento, siempre que las situaciones de mercado y regulatorias lo requieran. Para tal efecto, publicará la modificación o actualización correspondiente en la la página web [www.bbva.pa](http://www.bbva.pa) de acuerdo con lo previsto en las



normas vigentes aplicables, para que entren en vigencia las modificaciones.