Servicio del portal transaccional empresarial.

Recomendaciones y consideraciones para el servicio del portal transaccional empresarial.

A) Procedimientos definidos para registrar las direcciones IP fijas desde las cuales operarán, cuando ello sea posible.

El cliente debe radicar carta con la solicitud en referencia, en la cual indiquen la dirección IP a registrar y los usuarios a los cuales se les va a otorgar el permiso con IP.

La carta debe cumplir las siguientes condiciones:

- Carta en hoja membrete.
- Fecha y ciudad.
- Referencia " registro y/o cambio de IP".
- Descripción de la solicitud datos de la empresa e información de dirección IPs a registrar).
- Nombre y firma del cliente.

Nota: Junto con la carta se debe adjuntar cámara y comercio o acta de posesión según corresponda.

La documentación debe ser entregada al gerente y/o ejecutivo Cash asignado para realizar el trámite.

B) Mecanismos de autenticación fuerte (OTP, biometría, certificados digitales, entre otros) ofrecidos por el establecimiento de crédito para la realización de operaciones.

Banco Pichincha otorga a sus clientes mecanismos de autenticación fuertes para realizar transacciones desde el portal transaccional, para esto hace entrega de Token que son asignados a los funcionarios designados por el cliente.

Mecanismo de autenticación Token

En caso de requerir reasignación de Token, se debe realizar mediante carta con la solicitud en referencia en la cual indiquen la descripción de la solicitud.

La carta debe cumplir las siguientes condiciones:

- Carta en hoja membrete.
- Fecha y ciudad.
- Referencia solicitud reasignación de Token.
- Descripción de la solicitud (datos de la empresa e información del usuario actual y usuario al que se le reasignara el dispositivo).
- Debe contener los nombres, cédulas y seriales de los Token.
- Nombre y firma del cliente del representante legal.

Documentos para el radicado:

- Carta con solicitud.
- Cámara de comercio o acta de posesión según corresponda.
- Solicitud de Servicio Portal Transaccional completamente diligenciado sin enmendaduras ni tachones.
- Fotocopia de la C.C. de las personas a las cueles se les va a realizar la reasignación del dispositivo.

La documentación debe ser entregada al gerente y/o ejecutivo Cash asignado para realizar el trámite.

C) Opciones dispuestas en el portal transaccional para administrar las cuentas de recursos públicos con el fin de implementar una estricta segregación de funciones que garantice la independencia entre los funcionaros que registran las operaciones los que las autorizan

Los clientes empresariales cuentan con un usuario administrador el cual puede asignar perfiles:

Usuario preparador: Es el encargado de alistar las transacciones dejándolas pendientes por autorizar.

Usuario autorizador: Es encargado de autorizar las transacciones pendientes hechas por el preparador.

Para todos los casos cualquier transacción que registre un usuario preparador requiere de validación y aprobación por parte del usuario autorizador.

D) Políticas establecidas para la administración de usuarios y claves (contraseñas).

Condiciones para la asignación de usuarios en el portal transaccional

- Es definido por el usuario.
- Alfanumérico, no permite caracteres especiales.
- Mínimo de 8 caracteres.
- Máximo de 20 caracteres.

Condiciones para la asignación de usuarios en el portal transaccional

- Mínimo de 8 caracteres.
- Máximo de 20 caracteres.
- Alfanumérico, permite caracteres especiales.
- Debe tener al menos una mayúscula, una minúscula y un número.

Administración de usuarios

Bloqueo: Si el usuario se encuentra bloqueado debe comunicarse a la línea de atención 650 10 00 marcando la opción 2, donde se debe registrar la solicitud para generar el desbloqueo del usuario.

Activación de Token: Acuse de recibida la entrega del Token debidamente diligenciada por el usuario que recibe.

Nota: Para realizar el desbloqueo del usuario solo se gestionará al titular.

Para la activación el acuse debe ser entregado al gerente y/o ejecutivo Cash asignado el cual lo remitirá al área encargada al interior del Banco.

Administración Claves (Contraseña)

- La recuperación de contraseña es auto gestionable por el usuario ingresando por la siguiente ruta: **https://www.bancopichincha.com.co/web/corporativo/area-clientes**

En el recuadro de cliente empresa dar clic en la opción "Para Ingresar haz clic aquí" y luego la opción **¿Olvido su contraseña?**

El sistema solicita ingresar el usuario e identificación de la persona que está realizando el proceso.

Una vez se registren estos datos se solicitará ingresar el código de Token o la clave de la tarjeta débito asociada a la persona que está recuperando la contraseña.

E) Procedimientos definidos para la personalización efectiva de las condiciones para la realización de las operaciones financieras (montos, cantidad, horarios, días y horas hábiles , entre otros).

En el portal transaccional empresarial de Banco Pichincha, el usuario administrador define para el usuario preparador y autorizador los montos transaccionales, el segundo factor de autenticación (Token / OTP / Softoken), los permisos sobre los productos, horarios, días y el registro de firma autorizada para subir y/o aprobar transacciones.

Para realizar la asignación o modificación de los permisos debe ingresar por la siguiente ruta del menú

- Administrar.
- Usuarios.
- Modificar.

En relación con las atribuciones del usuario administrador, estas son definidas por el representante legal a través del formato de parametrización definido, el formato debe ser entregado al gerente y/o ejecutivo Cash asignado para realizar el trámite.

F) Procedimientos y mecanismos para registrar oportunamente el cambio de los números telefónicos o correos electrónicos donde se notifican las operaciones realizadas.

Para realizar actualización de datos se debe establecer comunicación a través de la línea de atención en:

- Bogotá al 650 10 00.
- Resto del país al 018000 919 918 marcando la opción 2, donde se debe registrar la solicitud para generar la actualización de datos según corresponda.

G) Canales y mecanismos establecidos para alertar las operaciones desconocidas y para presentar las quejas o reclamaciones sobre las operaciones repudiadas.

Se encuentra habilitada la línea de atención nacional Call Center, en:

- Bogotá al 650 10 00.
- Resto del país al 018000 919 918 marcando la opción 2.

Adicionalmente los puede realizar gerente y/o ejecutivo Cash asignado para atender la solicitud.

H) Capacitación que se debe impartir a los funcionarios encargados de realizar las operaciones sobre las medidas de seguridad que deben acoger.

Cuando se asigna o reasigna un token el banco realiza la capacitación al funcionario en sitio o a través de teleconferencia.

Adicionalmente en caso de requerirlo el cliente a través del gerente y/o ejecutivo Cash puede solicitar sesiones de aclaración o refuerzos de capacitación en temas funcionales y de seguridad del portal transaccional.

I) Medidas que se deben adoptar sobre los equipos donde se realizan las operaciones, después de identificar transacciones no autorizadas.

Para todos los clientes se recomienda el registró de la dirección IP de los equipos PC desde donde se realizarán las transacciones, en caso de transacciones no autorizadas si no se ha registrado el equipo se recuerda la importancia del registro.

En caso que desde un equipo que se registró la IP se realice una transacción, se recomienda revisar las atribuciones del usuario autorizador que la aprobó.

J) Otras recomendaciones a tener en cuenta

- Mantener actualizado el software operativo, de seguridad y antivirus de los equipos en los cuales se realizan operaciones con recursos públicos, utilizando herramientas de seguridad adecuadas (antivirus, antispyware, firewall, etc.).
- Evite realizar transacciones en lugares de concesión pública a Internet.
- No compartir con otros usuarios los equipos desde los cuales se realizan las operacionescon recursos públicos. Estos equipos deben ser de uso exclusivo de los administradores de las cuentas y no se debe ingresar a los portales desde otros equipos.
- No abrir correos de dudosa procedencia, no instalar archivos que puedan contener software malicioso ni navegar por sitios desconocidos en los equipos donde se realizan las operaciones.
- **Acceso al portal:**
  - Acceder siempre a nuestro portal web, tecleando siempre usted mismo la dirección de la página de nuestro Banco. El único sitio autorizado para ingresar a la Entidad es **www.bancopichincha.com.co.**
  - Verifique que la dirección electrónica a la que está accediendo empieza con las siglas **"https"**, es decir, que además cuenta con una letra "s".
  - No siga enlaces que se encuentren en correos electrónicos, aunque vengan de alguien conocido, mensajería instantánea o banners, que le podrían conducir a páginas falsas de la Entidad Financiera.
  - Valide siempre que en la parte superior o inferior del navegador aparezca el icono de un candado cerrado. De lo contrario no realice ninguna transacción.
  - Al finalizar una transacción por Internet asegúrese de cerrar la sesión y borrar los archivos temporales.
- **Manejo de claves o contraseñas:**
  - No compartir las claves ni los elementos de seguridad como los tokens.
  - Recuerde que debe utilizar contraseñas fuertes con símbolos, números, mayúsculas y minúsculas. No utilice datos como fechas de nacimiento, nombres de familiares, mascotas, entre otros a los cuales se pueda tener fácil acceso.
  - Procurar cambiar las contraseñas periódicamente.
  - Memorice las contraseñas, no utilice la opción de almacenar que ofrece el navegador.
  - Recuerde que el BANCO PICHINCHA, NUNCA lo contactará para solicitarle información confidencial como las contraseñas de sus cuentas, a través del teléfono, del correo electrónico o de cualquier otro medio.
- Mantenga su dispositivo de seguridad (token) en un lugar privado y seguro, no lo comparta con terceros, ni permita que este en un lugar visible.
- Atender oportunamente los mensajes de texto o correos electrónicos que se envían notificando las operaciones realizadas, aun cuando ellos se reciban en horarios no hábiles.
- Si encuentra una operación inusual, póngase de inmediato en contacto con nosotros.
- Verificar con frecuencia el saldo de las cuentas.
- Es importante que mantenga actualizado en el Banco el correo institucional, teléfono, persona de contacto, entre otros para la notificación de las operaciones realizadas.
- Implementar estándares de seguridad, calidad e idoneidad, para la contratación de terceros encargados de la revisión y mantenimiento de los equipos e instalación de software o hardware que soportan la realización de operaciones en su entidad.
- Recuerde tener actualizado los datos de contacto de su Gerente de Relación para cualquier duda, recomendación o asesoría que requiera.