Seguridad

Su información está segura en BANCOLOMBIA

En BANCOLOMBIA nos hemos propuesto asegurar la confidencialidad, disponibilidad e integridad de la información, uno de nuestros recursos más valiosos. Para dar buen manejo a los datos que nos suministran los clientes y a las transacciones que realizan a través de los diferentes canales, contamos con normas y políticas de seguridad que con el estricto cumplimiento protegen apropiadamente los datos y aspectos confidenciales de los clientes y del Banco.

Estas políticas permiten mitigar los riesgos latentes al definir el adecuado manejo de la información; por lo tanto, constituyen una herramienta de permanente consulta por parte de los empleados. En forma paralela, se desarrollan programas de sensibilización sobre el valor de la información al interior de la organización para potenciar el cumplimiento de las políticas.

Las políticas de seguridad se aplican a la información suministrada por los clientes, a la procesada dentro de la institución y a cada una de las plataformas tecnológicas del Banco, independientemente del lugar geográfico donde éstas se encuentren.

Así mismo, contamos con el compromiso de firmas internacionales en la realización de pruebas de penetración a nuestros sistemas y en la evaluación del cumplimiento tanto de las políticas para los empleados, clientes y terceros como para las implementadas en todas las plataformas tecnológicas.

Todo lo anterior, unido a la actual estructura de la entidad en el ámbito de Seguridad Informática, está apoyado en consultorías realizadas sobre el tema por empresas de reconocida trayectoria.

Estos son algunos de los elementos de alta tecnología que BANCOLOMBIA utiliza para garantizar la seguridad en sus transacciones:

1. **Cifrado de alta seguridad**

El Servicio Alterno Transaccional ofrece gran seguridad en lo que ha Cifrado se refiere. El Cifrado es la técnica de usar las matemáticas para ocultar la información privada a terceros, con el fin de transmitirla en

forma segura, a través de redes públicas como Internet. De esta manera la información sólo puede ser entendida por quien la origina y por el destinatario de la misma.

Todas las transacciones que usted realice serán Cifrado a 128bits, una de las formas más fuerte de Cifrado disponible comercialmente para proteger información en sitios web de Internet.

Para poder disfrutar del potencial de Cifrado ofrecido, su navegador debe tener una versión superior o igual a Microsoft Internet Explorer 6.0, el cual incluye el nivel de Cifrado a 128bits.

En la parte inferior derecha del navegador o en la parte superior se encuentra el candado cerrado. Esto indica que todos los datos intercambiados entre usted y Grupo Bancolombia viajan Cifrado de modo que no puedan ser leídos ni modificados por terceros.

2. **Firewall (muro de fuego)**

Es un sistema que previene el acceso no autorizado a nuestra red corporativa y evita que programas mal intencionados envíen información al exterior.

3. **Certificación**

Cada uno de los sitios del Servicio Alterno Transaccional, en los cuales el cliente debe ingresar información confidencial, está certificado tanto funcionalmente como en términos de seguridad

4. **.Antivirus**

Moderno esquema de protección centralizada para estaciones y servidores.

Controles de seguridad que posee el canal.

Este servicio tiene las siguientes características:

1. Pueden acceder todos los usuarios de la SVE que posean un token activo.
2. No es un servicio de uso diario. Se habilita sólo cuando se presenten eventualidades con la SVE.
3. Sólo se pueden realizar pagos de nómina y proveedores con archivo en formatos SAP y PAB, más no se puede realizar la inscripción de nuevas cuentas.
4. El Servicio alterno transaccional cuenta con los roles de seguridad que el cliente tenga dentro de la SVE, esto significa que si la empresa es de esquema control dual en la contingencia seguirá aplicando de la misma forma.
5. Los clientes que desean, por temas de seguridad, restringir para que las transacciones sólo se puedan realizar desde direcciones IP registradas, en el momento de la contingencia podrán seguir contando con este servicio (este servicio se puede solicitar mediante una carta firmada por el representante legal de la empresa donde nos indique los datos de la empresa a solicitar el servicio y las direcciones IP de las cuales se realizaran las conexiones del equipo del cual se transará).
6. El uso del canal puede ser habilitado o deshabilitado por la empresa. Para esto debe hacer una solicitud a Bancolombia por medio de una carta firmada por el representante legal de la empresa (Por defecto está habilitado).
7. En el momento de la aprobación de una transacción, el usuario aprobador deberá digitar el serial del token para poder ser aprobada la operación.

Recomendaciones para uso de su computador

1. **Antivirus:**

Es un programa especializado en la detección y prevención de virus y otro tipo de software mal intencionados Evita que su computador se descarguen e instalen programas maliciosos como troyanos bancarios que pueden capturar la información del cliente o tomar control de este para realizar transacciones.

Recomendaciones del antivirus

- Instalar y mantener actualizado su computador personal con antivirus y antispyware, con una periodicidad semanal, de manera que éste lo protegen contra espionaje y robo de información.

- Estos programas tienen una opción que le permitirá que se actualicen automáticamente, consulte la ayuda del programa.

- En el mercado existen varias compañías de antivirus que ofrecen programas y servicios que lo pueden apoyar y asesorar en prevención de virus y otro código malicioso.

2. **Parches del sistema operativo y el navegador de internet:**

Los parches de seguridad corrigen errores internos de su computador que lo hacen más susceptible a ataques. Si estos parches no se instalan y el cliente se conecta a internet, un atacante puede detectar qué parches le faltan Atacar a al computador, permitiéndole instalar software malicioso con el que podrá capturar los datos del usuario o tomar control del computador. El ataque inicial no requiere de una persona, sólo requiere de un sitio mal intencionado o de un sitio conocidos que ha sido vulnerado.

3. **Usar software legal:**

El software ilegal, tanto sistema operativo como aplicaciones, usualmente esta modificado para tener puertas traseras que permiten a los defraudadores tener un acceso al computador, aun si el sistema esta actualizado o tiene un antivirus.

4. **Firewall:**

El firewall es un programa que le ayuda a proteger su equipo de accesos externos no autorizados para evitar daños y robo de información. También evita algunas conexiones desde su computador a servidores de personas mal intencionadas.

Recomendaciones para el firewall

- Instalar y mantener actualizado su computador un firewall personal

- Tenga actualizado el firewall

Algunos fabricantes

- Firewall de Windows
- McAfee Personal Firewall

- Symantec Personal Firewall
- Iptable (Linux - Mac).
- Squbе (Linux - Mac)
- Microsoft Isa Server
- Squbе (Linux - Mac)
- Check Point.
- Junipper

5. Usuario seguro:

Usar un usuario administrador para navegar en Internet no es recomendado porque permite la instalación de software malicioso con permisos de administrador en los sistemas. Teniendo en cuenta eso, se recomienda que no se use un computador donde se tenga privilegios de administrador para realizar transacciones financieras. Si se tiene usuario administrador del computador, se recomienda que cree un usuario no administrador en el sistema y que lo use para navegar en Internet, y sólo use el usuario administrador cuando sea estrictamente necesario.

6. Antispyware:

Es un programa especializado en la detección y prevención de software dañino, como troyanos.

Recomendaciones para antispyware:

Debe permanecer activo todo el tiempo y se debe actualizar periódicamente (mínimo una vez por semana).

7. Protección de la Red WI-Fi:

Una red de Wi-Fi es lo que comúnmente se conoce como red inalámbrica, y permite conectar un equipo a una red con el fin de acceder a los diferentes recursos. Evite conectarse a redes inalámbricas desde sitios públicos, pues existe un riesgo muy alto de que sean redes con poca seguridad que permitan capturar toda su información personal y/o financiera por ejemplo: la red inalámbrica de un centro comercial.

Recomendaciones para WIFi:

- No exponga su máquina transaccional a redes inalámbricas desconocidas.

- Utilice la conexión a Internet sólo cuando vaya a utilizar el servicio.

- Al configurar los dispositivos de red cambie las contraseñas que traen por defecto.

- No realice transacciones bancarias a través de redes inalámbricas en sitios públicos.

Recomendaciones de navegación:

- Verificar la fecha y hora de su última conexión. Una vez identificado con su NIT o documento de identidad y su serial de Token, en la parte superior izquierda podrá comprobar la fecha y hora de la última conexión a la página del Servicio Alterno Transaccional.

- Haga caso omiso a los mensajes de correo electrónico que tengan un remitente desconocido, evitando además abrir los enlaces o archivos adjuntos, ya que estos pueden contener software malicioso camuflado en los temas de moda. Recuerde que solo a través del Buzón Seguro **Mis Mensajes**, eventualmente, podría recibir de nosotros, información con URLs adjuntas.

- Sea precavido al realizar descargas de programas gratuitos desde Internet, a través de este tipo de descargas es posible que se instale en su computador un software malicioso.

- Cuando navegues o compres por internet asegúrate de hacerlo en páginas confiables y seguras.

- No ingreses al **Servicio Alterno Transaccional** desde lugares públicos como café internet y centros comerciales, éstos pueden tener programas maliciosos.