REQUISITOS DE SEGURIDAD INFORMÁTICA

Para impedir el acceso no autorizado a las Cuentas del Cliente por parte de terceros, así como para asegurar que la información clave siga intacta, el Banco insta a su Clientela a que observen las siguientes medidas de seguridad informática:

- Asignar una computadora fija para realizar operaciones en el Sistema la que no se utilice para otros usos; salvo que sean las de los servidores del Banco, no ingresar a las páginas web desde esta computadora y, si los medios técnicos lo permiten, deshabilitar el acceso a las direcciones de Internet.
- Restringir o deshabilitar completamente el acceso remoto a la computadora asignada desde otras computadoras de la red de área local. No habilitar la administración remota en la computadora asignada. Si los medios técnicos lo permiten, poner la computadora asignada en una red separada, protegida por un cortafuegos y sistemas de detección de ataques.
- Cambiar todas las contraseñas predeterminadas al instalar el Sistema por nuevas que sean únicas y modificarlas de forma periódica (por lo menos una vez cada tres meses).
- Utilizar un software antivirus en base regular, manteniéndolo actualizado.
- Cada cierto tiempo (por lo menos una vez a la semana) iniciar un escaneo antivirus para la detección inmediata de software malicioso.
- Únicamente utilizar software de carácter legal en su computadora.
- Cada cierto tiempo (por lo menos una vez a la semana o bien en el día de publicación) actualizar el sistema operativo.
- Examinar los Usuarios administradores en la computadora designada y convertir en usuarios estándar a todos los que no realizan operaciones en el Sistema.
- Si los medios técnicos lo permiten, asignar a las personas que sí realizan operaciones en el Sistema al grupo de usuarios separado, el que proporcione acceso sólo a las aplicaciones determinadas.
- Ingresar a los servidores del Banco sólo desde las direcciones conocidas de los servidores del Banco.
- Si no se puede conectar con el servidor del Banco, reportarlo inmediatamente al Banco.
- Guardar soportes de información clave en un lugar seguro (en una caja fuerte) y no entregarlos a ninguno salvo que sea persona autorizada.
- Nunca copiar las claves de firma electrónica cerradas (privadas) al disco duro local de la computadora, aunque intente eliminarlas enseguida.
- Cada cierto tiempo (conforme a las condiciones del Acuerdo) realizar una modificación planeada de las claves vigentes.
- Cada cierto tiempo (por lo menos una vez al mes) comprobar la integridad de los soportes de información clave, verificando la presencia de los archivos de firma electrónica.
- Nunca dejar los portadores de información clave desatendidos, conectarlos a la computadora únicamente por el periodo de uso y desconectarlos al acabar las operaciones bancarias. En caso de dejarse el terminal del Sistema desatendido, bloquear la pantalla hasta que se introduzca la contraseña para desbloquearla.
- Inmediatamente modificar las claves de firma electrónica en caso o sospecha de comprometidas.

- Siempre mantener el Sistema actualizado.

- No instalar actualizaciones ni abrir enlaces en correos electrónicos haciéndose pasar por el Banco. En caso de recibir un mensaje así, reportarlo inmediatamente al Banco.

- Todos los días, durante y después de las horas hábiles del Banco, realizar una entrada adicional al Sistema para examinar la lista de mensajes salientes del mismo día. Al descubrir documentos sospechosos, reportarlo inmediatamente al Banco.

- Si se sospecha una desaceleración de la computadora, desconectarla de la red de área local e Internet y dirigirse al administrador del sistema para que realice una examinación completa mediante un escaneo de los archivos y memoria de la computadora.

- Si, a pesar de las precauciones, ocurrió un incidente de seguridad informática, en ningún caso se podrá apagar la computadora, sino sólo desconectarla de la red de área local e Internet, inmediatamente dirigirse al administrador del sistema y reportar al Banco del incidente para que realice una pronta investigación y adopte las medidas necesarias para reunir pruebas.

- Al identificar el Cliente algunas operaciones sospechosas en el Sistema, reportarlo inmediatamente al Banco.