Sobre las precauciones al efectuar los pagos electrónicos en el sistema de banca electrónica de servicio

Estimados clientes,

Con el fin de evitar el acceso no autorizado a sus fondos por parte de los malhechores y para evitar los hechos comprometedoresde acerca de su información clave se recomienda observar las siguientes **precauciones** al utilizar el sistema de banca electrónica de servicios (en adelante BES).

- seleccionar los ordenadores que no serán utilizados para ningún otro propósito que para trabajar en el sistema BES; no ejecutar, y si es técnicamente posible, prohibir el acceso al Internet a cualquier página, excepto las páginas de los servidores del Banco, desde este ordenador;

- cambiar todas las contraseñas estándar que fueron determinadas al instalar el sistema en las contraseñas propias y únicas, efectuar un cambio periódico de contraseñas;

- utilizar sólo el software con licencia;

- utilizar de forma regular el software antivirus con la última versión de las bases de signaturas, revisar regularmente los discos locales con el software antivirus e instalar la actualización del sistema operativo Windows;

- comprobar el grupo de "Administradores" en el ordenador fijado, excluir a todos los usuarios habituales de este grupo que no trabajan con el sistema electrónico BES;

- para los usuarios que trabajan con el sistema electrónico BES - crear una directiva particular de grupo para permitir el inicio sólo de las determinadas aplicaciones, así como filtrar el acceso a las redes externas en el principio "lista blanca";

- para el acceso a los servidores del Banco usar sólo las direcciones IP que Usted conoce de los servidores de Internet del Banco, indicadas en el acuerdo sobre el uso de medios electrónicos BES firmado entre el Cliente y el Banco;

- si no hay posibilidad de conectar con el servidor del Banco hace falta notificarlo con prontitud al Banco;

- almacenar en un lugar seguro (en una caja fuerte) y no transmitir a nadie los medios de comunicación con la información clave (los originales de claves cerradas (de secreto) de firmas digitales y sus copias de trabajo), asegurando su acceso sólo a las personas autorizadas;

- no dejar a los medios de comunicación con la información clave sin vigilancia, conectarlos al ordenador solamente durante su uso e inmediatamente desconectarlos después de las operaciones bancarias;

- los originales de las claves cerradas (de secreto) de las firmas digitales guardar separadamente de las claves de trabajo y otras copias);

- comprobar regularmente la integridad de los medios de comunicación clave (los originales y copias del trabajo), efectuar la verificación de la disponibilidad de los archivos con la firma digital;

- Cambiar inmediatamente las claves de la firma digital en el caso de los hechos comprometedores o la sospecha de los hechos comprometedores;

- En todos los casos de despido o cambios de los titulares del certificado de claves de la firma digital, así como en el caso de despido o cambios del único órgano ejecutivo de la organización, elaborar las nuevas claves para la firma gidital;

- instalar oportunamente todas las actualizaciones del sistema BES;

- no instalar las actualizaciones, y no abrir los enlaces en los correos electrónicos recibidos a nombre del Banco por e-mail, no abrir los enlaces en los mensajes de correo electrónico, así como, por ejemplo al recibir un mensaje, reportarlo inmediatamente al Banco;

- cada día, al acabar el día operacional del Banco y al finalizar el día laborable, después de trabajar con el sistema BES, llevar a cabo la entrada adicional en el sistema de control de la lista de los documentos de salida para el día actual; si se notan los documentos sospechosos, hace falta contactar inmediatamente con el Banco;

- en el caso de sospecha de ralentizar el ordenador hace falta desconectar físicamente el ordenador de la red local e Internet y contactar con el administrador del sistema comunicándole sobre la necesidad de una completa exploración antivirus de todos los archivos y la memoria del ordenador;

- si el incidente de seguridad ha sucedido, en todo caso no hace falta apagar el ordenador, es necesario sólo desconectarlo físicamente de la red local y del Internet, hace falta ponerse inmediatamente en contacto con el administrador del sistema y reportarle el incidente en el Banco para su pronta investigación y efectuación de las mediadas apropiadas para reunir pruebas.