En Bancoldex nos interesamos por Empresarios como usted, por eso a continuación presentamos algunas recomendaciones de seguridad para tener en cuenta y evitar se vea comprometida la información cuando hace uso del canal portal transaccional:

SEGURIDAD LÓGICA

La entidad podrá asegurarse de las siguientes formas:

a) Requerir credenciales de autenticación para el ingreso y/o uso, las cuales deberán estar obligadas a cambiarse periódicamente y tener especificaciones mayores de seguridad (longitud mínima de ocho caracteres alfanúmeros y caracteres especiales).

b) Controlar el tiempo de inactividad del usuario a través de bloqueo automático del equipo o terminal móvil (se sugiere máximo cinco minutos).

c) Limitar los privilegios de la(s) cuenta(s) de usuario(s) utilizada(s) para realizar transacciones financieras en los equipos y/o terminales para este fin, a efecto de reducir el riesgo de que con la misma sea posible la instalación de software malintencionado o controladores de dispositivos no autorizados.

d) Restringir en lo posible la ejecución de archivos como (.exe, .vbs, .com .scr, etc.) que no hagan parte de los sistemas necesarios para la elaboración de las actividades propias del cargo y que hayan sido descargados de sitios web o recibidos vía correo por parte del usuario del equipo por medio del cual se realizan las transacciones financieras.

e) 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).

f) Establecer los mecanismos 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.

g) Restringir la instalación de software que permita conexión remota (TeamViewer, LogMeIn, Hamachi, VCN, entre otros) evitando con esto que personas externas se puedan conectar fácilmente al equipo o terminal desde el cual se realizan las transacciones.

h) Asegurar que el equipo y/o terminal móvil cuente mínimo con: antivirus (con módulos de anti - keylogger, firewall personal, antispyware), software licenciado y actualizado de forma automática o supervisada (se sugiere actualización mínimo dos veces a la semana).

i) Restringir los puertos que permitan la conexión y/o acceso a dispositivos de almacenamiento extraíbles (CD, USB, SD Card, etc.).

j) Restringir el software de acceso remoto al equipo que pueda ofrecer o tener preinstalado el Sistema Operativo del respectivo equipo o terminal.

k) Actualizar periódicamente el sistema operativo del equipo o terminal con los últimos parches que corrigen vulnerabilidades que podrían ser aprovechadas. Las multinacionales como Windows e Internet Explorer acostumbran a liberar parches de actualización el primer martes de cada mes.

l) Procurar tener instalado un solo navegador, con mejores mecanismos de seguridad posibles debidamente configurados.

m) Activar mecanismos para que el equipo o terminal pueda recibir las actualizaciones de seguridad de forma automática, cada vez que sean emitidas por el fabricante para el sistema operativo respectivo y aplicaciones.

n) Mantener activos y en operación sólo los protocolos, servicios, aplicaciones, usuarios, entre otros, necesarios para el desarrollo de las actividades, en el equipo o terminal.

o) Preferiblemente, el equipo o terminal deberá ser destinado de manera exclusiva para la realización de las transacciones financieras.

p) Preferiblemente, apagar el equipo o terminal cuando no se esté utilizando, sobre todo si dispone de una conexión permanente a Internet.

q) No abrir correos con archivos adjuntos con extensión *.exe

Bancoldex a través del canal transaccional ofrece las siguientes alternativas de configuración para incrementar la seguridad, por favor tenga en cuenta las siguientes recomendaciones:

a) Consulte y depure periódicamente los usuarios que acceden al portal, esta información podrá ser valiosa en caso de aparecer conexiones y/o usuarios no autorizados por usted.

b) Registre las direcciones IP´s desde las cuales sus usuarios podrán ingresar al portal para evitar conexiones fuera de su entidad, consulte con su operador de Internet para obtener una dirección IP fija en caso que su dirección sea variable.

c) Cambie periódicamente sus contraseñas, una buena práctica es realizarlo cada 30 días.

d) Nunca ingrese al portal transaccional desde computadores ubicados en sitios públicos como: café internet, bibliotecas, universidades, entre otras.

e) Haga uso de la segregación de funciones y no asigne dos roles (ejemplo: administrador y autorizador) al mismo usuario, recuerde los atributos que tiene cada rol.

f) Capacite a sus usuarios sobre la construcción de las contraseñas, a continuación proporcionamos algunos ejemplos:

Un buen método para inventar claves seguras y fáciles de recordar es utilizar frases completas. Se puede usar las iniciales de una frase así:

Siente tu bandera cree en tu país 8 *	===>	Stbcetp8*
Mi hijo Santiago tiene 10 años +	===>	Mhst10a+

Longitud mínima: La mínima longitud recomendada es de 8 caracteres, salvo impedimentos técnicos que deberán documentarse y autorizarse.

Reutilización: La contraseña actual no debe ser igual o parecida en su estructura (ej.: p1: Juan01admin, p2: Juan02admin) a ninguna de las últimas 5 contraseñas utilizadas.

Caracteres: Toda contraseña debe tener por lo menos 1 carácter alfabético en mayúscula, uno en minúscula y un carácter numérico. Se recomienda el uso adicional de caracteres especiales (#$&-_...)

Periodicidad: Una contraseña no puede ser usada por más de 30 días. Al cabo de tal periodo debe cambiarse la contraseña, o cada vez que exista la sospecha de que la misma puede ser adivinada.

Almacenamiento: Si es absolutamente necesario escribir la contraseña, debe ser "cifrada" cambiando cada carácter con un algoritmo sencillo pero privado que no muestre la contraseña en forma textual. (ej.: p1: Juan01admin, se escribe: kVBO01BENJO. Se desplazó cada carácter alfabético una posición en el alfabeto y se cambiaron mayúsculas por minúsculas)

Los usuarios deben procurar no escribir sus contraseñas en ningún lugar físico o medio magnético. Para este efecto se recomienda utilizar métodos de creación de contraseñas fáciles de aprender y evitar la reutilización.

f) El canal portal transaccional, le permite configurar los horarios de conexión, es recomendable definir los horarios que más se acomoden con las necesidades de los usuarios y la entidad.

SEGURIDAD FISICA

La entidad podrá asegurarse de las siguientes formas:

a) Restringir el acceso al área física desde donde se realizan transacciones financieras sólo para personal autorizado.

b) 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. Se recomienda conservar las imágenes 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.

SEGURIDAD DE LA RED

La entidad podrá asegurarse de las siguientes formas:

a) 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 terminal. Esto con el objeto de evitar que de forma intencional o accidental, se descargue, instale o ejecute software malintencionado.

b) Implementar mecanismos de autenticación que permitan confirmar que el equipo o terminal móvil es un dispositivo autorizado dentro de la red de la entidad.

c) Asegurar las redes inalámbricas (WIFI) desde las cuales se realicen transacciones financieras, cuenten con las mejores condiciones y estándares técnicos disponibles. Definir un usuario con contraseña robusta y cambiarla periódicamente.

d) Si la entidad cuenta con una red inalámbrica (WIFI) para invitados, se recomienda esté totalmente aislada y segmentada de las redes LAN de la entidad.

RECOMENDACIONES DE SEGURIDAD EN LA REALIZACIÓN DE LAS TRANSACCIONES

La entidad podrá asegurarse de las siguientes formas:

a) Acceder a la página del portal transaccional de Bancoldex únicamente digitando la dirección en el navegador. Nunca realice esto a través de links, motores de búsqueda o de los favoritos o marcadores del navegador.

b) Siempre cerrar la sesión del portal transaccional al terminar las transacciones.

c) Asegurar la restricción en el acceso a los portales transaccionales de los usuarios durante sus períodos de vacaciones o licencias y darlos de baja en casos de traslado o retiros.

d) Asegurar que las personas que realizan transacciones financieras cuentan con capacitación en relación con la seguridad de la información y de las medidas que debe adoptar para mitigar los riesgos de fraude financiero.