Banco Serfinanza

# REGLAMENTO DE SEGURIDAD SERFINANZA VIRTUAL EMPRESAS

## RECOMENDACIONES GENERALES:

- Utilice los servicios gratuitos de personalización de transacciones y de notificación de operaciones en línea vía SMS y correo electrónico.
- Mantenga siempre sus datos actualizados, como número de teléfono, celular, correo electrónico y direcciones, recuerde que la entidad envía información de sus productos, a través de los datos registrados en el sistema.
- No abra correos electrónicos sospechosos (enviados desde cuentas de correo que no pertenezcan a Banco Serfinanza), ni descargue archivos adjuntos de correos desconocidos, los cyber-delincuentes utilizan este mecanismo para el robo de datos que luego utilizan para realizar transacciones y suplantar su identidad.
- Banco Serfinanza nunca solicita información confidencial vía correo electrónico, SMS o llamada telefónica como numero completo del producto, fechas de vencimiento de tarjeta de crédito o códigos de seguridad impresos en los plásticos. Desconfíe de las llamadas que ofrecen promociones y requieren este tipo de información confidencial, cuelgue inmediatamente.
- En caso de pérdida de sus tarjetas débito o crédito realice el bloqueo de forma inmediata. Recuerde que el bloqueo lo puede realizar a través del IVR o la línea de Servicio al Cliente llamando en barranquilla 3361990 y a nivel nacional 018000510513, de forma presencial a través de nuestra red de oficinas a nivel nacional o a través del portal web www.bancoserfinanza.com
- Banco Serfinanza nunca solicita dineros para el trámite de créditos, no se deje estafar, reporte irregularidades en nuestras líneas de atención al cliente, en barranquilla 3361990 y a nivel nacional 018000510513
- Banco Serfinanza nunca realiza recaudo de dineros a través de particulares, abogados, casas de cobranza ni asesores comerciales, todos los pagos se realizan en las cajas de la entidad, corresponsales bancarios, entidades financieras con convenio o el portal web.
- Consulte siempre los canales autorizados, números de teléfono y oficinas en nuestra página web www.bancoserfinanza.com
- Nunca preste sus tarjetas débito o crédito a terceras personas, el uso de los productos es personal, en caso de que alguno de sus familiares requiera el uso de su cupo recuerde que puede utilizar los servicios de tarjetas extendidas.
- Banco Serfinanza envía información vía SMS (mensaje de texto) UNICAMENTE desde los códigos: 890099 y 899937. Nuestra comunicación vía correo electrónico es enviada SOLAMENTE a través de las cuentas: non-response@bancoserfinanza.com, monitoreooperaciones@bancoserfinanza.com, info@bancoserfinanza.com
- Nuestras campañas pueden tener filtros de autenticación y únicamente te pedirán los cuatro últimos dígitos de la cédula y/o últimos cuatro dígitos de tu número de cuenta. Ninguna de nuestras campañas te solicitará información adicional como: Número completo de tu Tarjeta de Crédito, Fecha de Vencimiento de la misma, Claves para realizar avances, Claves de acceso al portal Web y la APP Móvil, Código de seguridad de la tarjeta CVV (3 Dígitos en la parte posterior de tu tarjeta) o Cualquier información que ponga en riesgo tu seguridad financiera. Nuestros correos UNICAMENTE podrán redireccionarte a la página oficial de campañas de la Entidad www.tarjetaolimpica.com.co
- En caso de solicitar la cancelación de sus tarjetas débito o crédito recuerde que no nunca debe entregarlas a ninguna persona. Cerciórese de destruirlas personalmente.

## CANALES ELECTRÓNICOS

### SERFINANZA VIRTUAL EMPRESAS:

- Acceda al portal digitando siembre www.bancoserfinanza.com nunca lo haga a través de un link o enlace.
- Ingrese al portal web únicamente desde computadores personales, no use computadores públicos o desconocidos.
- No utilice la opción recordar clave en los navegadores.
- Evite conectarse a internet mediante redes inalámbricas públicas y/o gratuitas.
- Proteja su clave del portal web, recuerde que su uso es personal, no las comparta con nadie incluso con funcionarios de la entidad.
- No permita que terceras personas utilicen su cuenta para fines ilícitos, cyber-delincuentes están solicitando la realización de pagos a sus productos crediticios con recursos adquiridos fraudulentamente a entidades financieras.
- Culmine la sesión con las opciones de salida segura.
- Mantenga actualizado el software de su computador y su antivirus.
- Mantenga actualizado su navegador de internet frecuente con la última versión disponible.
- Recuerde que sus claves son secretas y privadas, no las comparta con nadie, incluso si funcionarios de la entidad se las solicitan.
- Cambie continuamente sus claves de acceso y memorícelas, no utilice datos como nombres, fechas especiales, ciudades, meses del año, etc., trate de combinar caracteres especiales y letras sin sentido.
- Si sospecha o conoce de cualquier sitio web que le solicite información personal o algún correo electrónico cuyo dominio no sea @bancoserfinanza.com a nombre de la entidad, infórmelo inmediatamente en nuestras líneas de atención al cliente o a la cuenta de correo seguridaddigital@bancoserfinanza.com

### SERFINANZA MOVIL EMPRESAS:

- Utilice siempre su teléfono celular personal para ingresar a la Serfinanza Móvil de Banco Serfinanza.
- Mantenga el software y antivirus de tu dispositivo móvil actualizado.
- Evite conectarse a internet mediante redes inalámbricas públicas y/o gratuitas.
- No acceda a enlaces informados a través de mensajes SMS/MMS no solicitados y que impliquen la descarga de contenidos en el equipo.
- No descargue aplicaciones de sitios sospechosos, valide siempre que sean aplicaciones seguras.
- Utilice la opción de salida segura antes de cerrar el navegador o la APP de su teléfono.
- En caso de pérdida del celular solicite el bloqueo del mismo al operador de telefonía.
- Sólo active las conexiones por Bluetooth y Wi-Fi cuando vaya a utilizarlas.
- No conecte su teléfono celular en equipos públicos o inseguros.
- Cambie continuamente sus claves de acceso y memorícelas, no utilice datos como nombres, fechas especiales, ciudades, meses del año, etc., trate de combinar caracteres especiales y letras sin sentido.

### ENTES TERRITORIALES Y ESE:

¡En banco Serfinanza siempre pensamos en tu seguridad! Al momento de realizar transacciones en línea es fundamental que las personas que estén autorizadas sean precavidas para proteger la seguridad de las mismas.
A continuación, compartimos algunas recomendaciones de seguridad esenciales que se deben tener en cuenta:

- Mantener todo el tiempo actualizado el software operativo y de seguridad de los equipos en los cuales se realizan operaciones con recursos públicos.
- No compartir las claves o elementos de seguridad.
- Registra las direcciones IP desde las cuales realicen las operaciones con recursos públicos.
- Evita ingresar a los canales electrónicos (Web Banking) desde equipos diferentes a los asignados a los administradores de las cuentas.
- Atiende oportunamente los mensajes de texto o correos electrónicos que se envíen notificando las aletas de las transacciones realizadas con los recursos públicos.
- Verifica periódicamente el saldo de las cuentas.
- No abras correos de dudosa procedencia, ni instales archivos que puedan contener software malicioso. Evita navegar por sitios desconocidos en los equipos donde se realizan las transacciones con recursos públicos.
- Para mayor seguridad, procura inscribir correos institucionales en los que puedas recibir notificaciones de las operaciones realizadas.
- Implementa 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.
- Evita en todo momento utilizar redes wifi de acceso público para realizar transacciones en línea.
- Ten mucha precaución con el contenido de algunos anuncios divulgados a través de redes sociales.
- Mantén una estricta Segregación de los perfiles disponibles en el canal Web Banking (Administrador, Operador y Aprobador), con el fin de garantizar la independencia entre los funcionaros públicos que registran las operaciones de los que las autorizan.
- Define Políticas para la administración de usuarios y claves (contraseñas).
- Personaliza las condiciones para la realización de las operaciones financieras de acuerdo a los niveles de atribución de los perfiles.
- Asegúrate siempre de escribir la dirección de acceso al portal transaccional de nuestro banco (www.bancoserfinanza.com) y evita acceder desde enlaces recibidos mediante correos electrónicos o mensajes de texto.
- Recuerda: Banco Serfinanza nunca solicita información confidencial vía correo electrónico, SMS o llamadas telefónicas como los números completos del producto, fechas de vencimiento de tarjeta de crédito o códigos de seguridad impresos en los plásticos, credenciales de acceso a los canales electrónicos (usuarios y contraseñas). Desconfía de toda solicitud que reciba de este tipo de datos.
- Siempre que haya cambio de funcionarios públicos autorizados para el manejo de los productos financieros recuerda informar inmediatamente al Banco y proporcionar las respectivas actas de posesión y demás documentos que acrediten al nuevo personal autorizado. Recuerda actualizar oportunamente el cambio de los números telefónicos o correos electrónicos donde se notifiquen las operaciones realizadas.
- Con la finalidad de facilitar los procesos de conciliación entre los administradores salientes y entrantes, se recuerda que la información de extractos y consulta de movimientos se encuentran disponibles en canales físicos (oficinas) y electrónicos (Web Banking).
- Para facilitar el uso del Portal Transaccional Banca Empresas los nuevos administradores pueden consultar un instructivo en la página web www.bancoserfinanza.com en la ruta Servicio al Clientes/Educación Financiera/Manual de Uso Canales