Recomendaciones de seguridad para el uso de canales y productos

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 y puede llegar a destinatarios no autorizados en caso de desactualización de la información.
- No abra correos electrónicos sospechosos, 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.
- Serfinansa 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 alguno de sus productos realice el bloqueo de forma inmediata.
- Serfinansa nunca solicita dineros para el trámite de créditos, no se deje estafar, reporte irregularidades en nuestras líneas de atención al cliente.
- Serfinansa 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.serfinansa.com.co.
- Nunca preste sus tarjetas a terceras personas, el uso de los productos es personal, utilice los servicios de tarjetas extendidas en caso de requerir trasladar cupo de crédito a algún miembro de su familia.
- Serfinansa solo envía información vía SMS (mensaje de texto), desde códigos cortos de operadores nacionales, nunca desde números telefónicos tradicionales o WhatsApp.

Recomendaciones por tipo de canal:

Seguridad en oficinas

- Realice las operaciones monetarias (pagos, retiros, y giros) únicamente en las cajas de la oficina, las cuales están debidamente señalizadas y poseen ventanilla, recuerde que en los puntos de atención ubicados en los almacenes Olímpica no contamos con la infraestructura de cajas, utilice las cajas del establecimiento comercial (corresponsal bancario).
- Realice sus consultas únicamente en los módulos de información de las oficinas y puntos de atención, nuestros funcionarios están plenamente identificados con carnet, elementos institucionales y/o uniforme.
- Evite mostrar y/o contar el dinero antes de que se encuentre en presencia del cajero.
- Evite cambiar billetes a personas que los aborden al interior de las oficinas.
- Desconfíe de personas que ceden varias veces el turno y que abandonan la fila continuamente, si nota actitudes sospechosas notifique a un funcionario de la entidad.
- Siempre verifique la información impresa en el soporte de la operación.
- Al utilizar los PINPAD proteja la clave al digitarla, no permita que terceros y funcionarios de la entidad observen los números ingresados.
- En caso de realizar operaciones por altas sumas de dinero, utilice el acompañamiento gratuito de la policía nacional.

- No permita que personas desconocidas se acerquen a la ventanilla de caja cuando le corresponda realizar su operación.
- Por su seguridad, no entregue formularios de trámites y solicitudes con su firma y huella en blanco o con campos sin diligenciar.

Seguridad en canales electrónicos

- Portal Web:

- Acceda al portal digitando siembre www.serfinansa.com.co 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.
- Actualice periódicamente el software de su computador, así como el 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 a nombre de la SERFINANSA, infórmelo inmediatamente en nuestras líneas de atención al cliente.

- IVR y call center:

- Nuestros números de contacto para servicio al cliente son:
  Barranquilla: 3361990 **Armenia:** 7359855 • **Bogotá:** 7436978 • **Bucaramanga:** 6970355 • **Cali:** 4851221 • **Cartagena:** 6930439 • **Medellín:** 6040553 • **Montería:** 7898910 • **Neiva:** 8630055 **Pereira:** 3400623 • **Santa Marta:** 4366104 • **Sincelejo:** 2762016 • **Valledupar:** 5894133 • **Resto del País:** 018000510513
- Cuando Usted haga uso de este canal, una grabación le informará que por seguridad y mejoramiento en la calidad del servicio, su llamada será grabada y monitoreada.
- Nuestros agentes telefónicos nunca solicitan el número completo del producto, fechas de vencimiento de tarjeta de crédito o códigos de seguridad impresos en los plásticos.
- Nunca proporcione su clave de consulta a funcionarios de la entidad.
- Realice las llamadas desde un teléfono personal y proteja su clave cuando la esté digitando.
- Responda claramente las preguntas de seguridad para identificar su identidad.

- App Serfinansa:

- Utilice siempre su teléfono celular personal para ingresar a la APP de Serfinansa.
- Mantenga el software 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 de los servicios Web que requieren contraseña, antes de cerrar el navegador de su teléfono.
- Utilice antivirus en su celular.
- 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.

Seguridad en establecimientos de comercio presenciales

- Nunca descuide de vista su tarjeta de crédito cuando pague en establecimientos comerciales presenciales, verifique que su tarjeta es leída una única vez. En Colombia solo se deben realizar operaciones con lectura de chip, manténgase atento.
- Nunca utilice a terceras personas para realizar operaciones con su tarjeta, siempre hágalas personalmente.
- Nunca asigne claves transaccionales sencillas de descifrar, tales como fechas de nacimiento, número de documento de identidad, número de teléfono, nombres etc.
- Cuando le devuelvan su tarjeta verifique que sea la suya.
- Exija siempre el comprobante de la compra y verifique el monto antes de firmarlos.

Seguridad en establecimientos de comercio electrónico

- Realice operaciones únicamente en sitios de comercios electrónicos reconocidos y seguros.
- Realice operaciones únicamente desde equipos de uso frecuente celular o pc.
- Evite conectarse a internet mediante redes inalámbricas públicas y/o gratuitas.
- Desconfíe de los sitios de comercio electrónico que ofrecen grandes beneficios o descuentos.
- Cuando realice compras por teléfono, asegúrese que el establecimiento recibe la información de seguridad mediante captura de datos por el teclado del teléfono, evite dictar información de su producto a un agente de venta telefónica.
- Actualice periódicamente el software de su computador, así como el antivirus.
- Mantenga actualizado su navegador de internet frecuente con la última versión disponible.
- Cuando compre tiquetes aéreos, realice la compra del tiquete directamente con la aerolínea o en una agencia de viajes reconocida. Recuerde que en estos establecimientos reciben todos los medios de pago.
- Cuando realice operaciones desde Aplicaciones Móviles, valide siempre que la APP obedece a un establecimiento de comercio reconocido. Descargue siempre las app de comercios desde una tienda autorizada como Appstore o GooglePlay, no instale Apps provenientes de correo electrónico, SMS o links en redes sociales.

Seguridad en cajeros electrónicos no propios

- Al usar un ATM o cajero electrónico verifique que no haya ningún objeto extraño adherido al cajero.
- Antes de introducir la tarjeta en la ranura, verifique que esta no tenga objetos extraños adheridos a esta.
- No haga caso a avisos impresos pegados en el cajero que le indican cómo hacer sus operaciones.
- Nunca acepte ayuda de un extraño cuando use un cajero automático.

- Párese cerca al cajero automático y use su cuerpo y sus manos como escudo para asegurarse de que nadie lo vea ingresar su clave.
- No se deje distraer, intimidar o apurar en hacer su transacción en el cajero automático por terceras personas.
- Si usted no ha terminado su transacción y es abordado por un tercero, presione el botón Cancelar, recoja su tarjeta y retírese.
- No acepte ayuda de terceros, realice su operación por si mismo.

Seguridad en corresponsal bancario

- No acepte ayuda de terceras personas para realizar operaciones en el corresponsal bancario
- Proteja sus claves de acceso y no permita que los funcionarios del corresponsal o terceras personas puedan ver las claves al digitarlas
- Nunca entregue sus claves a terceros ni a funcionarios del corresponsal.
- Reclame siempre el soporte de la operación en el corresponsal y verifique los montos antes de retirarse del corresponsal.
- Cuente bien el dinero retirado y valide la autenticidad del dinero antes de retirarse del corresponsal.
- Los funcionarios del corresponsal nunca solicitan información confidencial de sus productos o claves de acceso.
- El Corresponsal no está autorizado para prestarte servicios financieros por cuenta propia.
- El corresponsal no está autorizado para realizar ningún tipo de cobro por la transacción realizada diferente a las tarifas establecidas y divulgadas por Serfinansa.