Seguridad en Skandia

- Recuerde que Skandia nunca solicita información personal de clientes a través de correos electrónicos.
- Le sugerimos que cambie su contraseña de acceso al Portal de Clientes, por lo menos cada 3 meses.
- Lo invitamos por su seguridad a registrar preguntas propias en el portal transacciona lo cual le permitirá contar con mayor seguridad
- Los aportes a sus contratos realícelos por cuenta propia y únicamente en las entidades recaudadoras autorizadas por Skandia.
- Siempre revise que su comprobante de consignación de aportes (Formato Único de Recaudo) tenga el sello y timbre de la caja del Banco, así como las 2 referencias detalladas (número del producto y documento de identidad o nit).
- Recuerde que Skandia utiliza únicamente el formato único de recaudo como documento válido para realizar un aporte en el Banco.
- No entregue efectivo ni cheques que no se encuentren girados a nombre de Skandia a: Financial Planner o Asesores Pensionales; realice las transacciones de manera personal; Skandia no se hace responsable por este tipo de situaciones.
- Si el aporte lo realiza en cheque a nombre de Skandia, siempre al dorso del cheque escriba la leyenda “Para consignar en”, incluya el número de contrato destino del aporte, su nombre, su número de identificación y teléfono de contacto.
- Los retiros de fondos debe hacerlos a través de nuestro Portal de Clientes, desde nuestro sistema de Audiorespuesta o directamente en nuestras oficinas a nivel nacional, diligenciando el formato respectivo.
- Por su seguridad, usted debe diligenciar por su cuenta los formatos o las solicitudes de vinculación, retiros de fondos u otro formato; no entregue a los Financial Planner formatos de retiros y/o transaccionales con su firma y huella y sin diligenciar.
- Cuando realice cualquier transacción sobre su contrato, compruebe que ésta se ha hecho efectiva; puede verificar a través de nuestro Portal de Clientes, o el sistema de audiorespuesta o a través de nuestro Contact Center. No reciba información de transacciones por parte de un Financial Planner o Asesor de Pensiones.
- Skandia no se hace responsable por transacciones que realice su Financial Planner en su nombre bajo su consentimiento a través de formatos de retiros, traslados o transferencias entre fondos que usted firmó y entregó sin diligenciar.

- Recuerde que la mejor forma de asegurar un contacto permanente es actualizando su información básica, como correo, numero celular, y demás datos relevante, contáctenos.

- Recuerde que Skandia no recibe aportes en efectivo a través de Financial Planners, ni de agencias comerciales autorizadas ni en ninguna de sus oficinas a nivel nacional.

- Skandia le recomienda revisar el estado de cuenta de su(s) contrato(s) por lo menos una vez al mes. Para esto, consúltelo en el Portal de Clientes, ingresando con su usuario y contraseña a través de **www.skandia.com.co** o comunicándose personalmente a nuestro Contact Center o directamente en nuestras oficinas a nivel nacional.

- Los correos sospechosos, generalmente contienen información con errores en redacción y elaboración de texto o palabras mal escritas.

- Recuerde que cuando sean solicitados cambios de sus datos personales o se realicen transacciones, Skandia siempre realizará notificación de sus operaciones en línea vía SMS y correo electrónico registrado. En caso de no haber solicitado cambios de datos o haber realizado transacciones por favor **infórmelo de inmediato** nuestras líneas de atención al cliente o a los siguientes correos: **cliente@skandia.com.co - prevenciondefraude@skandia.com.co** y **ciberseguridad@skandia.com.co**

Si sospecha que es víctima de fraude, puede comunicarse inmediatamente con nuestro Contact Center Skandia en la línea 658 4000 / 484 1300 o 01 8000 517 526 a nivel nacional. También puede escribirnos a **prevenciondefraude@skandia.com.co** y **ciberseguridad@skandia.com.co**

Seguridad en Internet

- No utilice enlaces (links) dentro de un correo electrónico para ingresar a los portales transaccionales de Skandia, para llegar al sitio escriba **www.skandia.com.co** en la barra de direcciones del navegador.

- Skandia le enviará mensajes con enlaces a sitios informativos que No le solicitan información personal. En el caso de notificaciones de transacciones que estén cifradas, estas podrán tener un enlace en el cual usted podrá leer el contenido de su mensaje después de ingresar la contraseña seleccionada.

- Sospeche de cualquier correo electrónico que soliciten de manera urgente alguna información. Tenga en cuenta lo siguiente:
    - A menos que los correos vengan firmados digitalmente (Garantía del emisor por medios electrónicos), no se puede estar seguro si es un correo falsificado.
    - Usualmente los correos fraudulentos vienen con anuncios o alarmas con el fin de crear pánico y hacer reaccionar a las personas inmediatamente.
    - Usualmente los correos fraudulentos solicitan información como nombres de usuario, claves, números de tarjetas de crédito, números de cédula, etc.
    - El correo electrónico fraudulento generalmente no es personalizado ni viene dirigido a una persona como sí lo son los correos recibidos de los Bancos.
- Evite llenar formas de texto en correos electrónicos que solicitan información financiera y /o personal.
- Verifique que en la página visitada, se encuentre el ícono del "candado" en la barra de estatus del Navegador de Internet. Esto significa que la pagina cuenta con un Certificado digital que autentica y asegura la información que es transmitida.
- Ingrese frecuentemente a sus contratos en línea y verifique su información del contrato. No deje más de un mes sin revisar cada una de sus cuentas. Si nota algo sospechoso, contacte inmediatamente a Skandia.
- Asegure que su computador y su navegador de Internet se encuentran al día con las últimas actualizaciones de seguridad.
- Proteja su sistema de cómputo. Los sistemas para acceder a Internet deben incluir lo siguiente:
    - Tener instalado un Software Antivirus actualizado.
    - Tener instalado un Software de Control de acceso al PC (Firewall de Red o Personal) para protección de accesos no autorizados desde Internet.
    - Tener instalado Software para protección de instalación de programas espías (Spyware).
- Considere instalar una barra auxiliar para el Navegador Web para ayudar a proteger de sitios Web fraudulentos.
- Manejo de Claves Secretas o Passwords.
- Utilice claves diferentes en todos los servicios que tenga, como por ejemplo la de su correo electrónico.

- No utilice claves que sean fácilmente identificables como fechas de nacimiento, teléfonos, direcciones, nombres de familiares.
- No revele por ningún motivo sus claves.
- No apunte sus claves, memorícelas.
- Cambie periódicamente sus claves.
- Ingrese su clave de manera confidencial de forma que no pueda ser vista por otras personas que están a su alrededor.
- No revele su información personal ni financiera en cualquier página de Internet o correo electrónico, cuide la confidencialidad de sus datos.
- No abra correos electrónicos sospechosos (enviados desde cuentas de correo que no pertenezcan a Skandia o que no esté esperando), 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.
- Acceda al portal digitando siempre **https://www.skandia.com.co** nunca lo haga a través de un link o enlace. Siempre verifique que en el navegador este la palabra **HTTPS**
- Nunca utilice la opción recordar clave en los navegadores personales y públicos.
- Mantenga actualizado el software de su computador, antivirus en su computador personal y dispositivos móviles
- Proteja su clave del portal web, recuerde que su uso es personal, no las comparta con nadie incluso con funcionarios de la entidad. Recuerde cambiarla con frecuencia o cuando sienta que alguien tuvo acceso a ella
- 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.
- Para obtener información acerca de Skandia, de nuestros productos o para realizar cualquier consulta, comuníquese con nosotros a la línea nacional: 01 8000 517526 **PBX:** (1) 658 4000 / 484 1300 **E-mail:** cliente@skandia.com.co

Seguridad para Retiros de Fondos

Los retiros de fondos de sus contratos deben ser directamente realizados por los clientes y diligenciando un formato de retiros dispuesto por Skandia para tal fin.

Su clave es su firma electrónica y no debe confiarla a nadie. En lo posible haga sus transacciones acompañado de otras personas (plena confianza), pero que el

acompañamiento sea activo, es decir mientras la persona realiza la transacción el otro u otros están atentos a detectar situaciones o personas sospechosas.

Skandia no realiza retiros de fondos de contratos de clientes en efectivo ni en cheques de cuentas personales.

Skandia no deposita en efectivo retiros de fondos en cuentas de clientes. Todas nuestras transacciones de retiros son realizadas a través de transferencias entre cuentas vía ACH principalmente o en cheques Skandia.

En sus desplazamientos verifique que no esté siendo seguido por personas, vehículos o motos sospechosas, si detecta esto trate de llegar a un sitio que le ofrezca seguridad.

Seguridad en Portal de Clientes: Manejo de Clave de Acceso

A continuación se presentan las recomendaciones que debe tener en el manejo de la clave de acceso al Portal de Clientes:

- Recuerde que el suministro de claves para el uso de Internet es la primera instancia de seguridad que debe ser muy bien administrada.
- **Si usted ha registrado una cuenta de correo electrónico en su afiliación o la ha solicitado posteriormente, recuerde que su clave de acceso al Portal de Clientes la puede obtener a través del Sistema de Audio Respuesta o través de la línea de servicio a clientes.**
- Si usted periódicamente recibe información de Skandia a través de su correo electrónico y este proceso es suspendido, le recomendamos verificar que su cuenta de correo electrónico sea la misma que usted ha registrado, si encuentra alguna anomalía contáctenos de inmediato.

Por su seguridad, Skandia a través del área de Servicio al Cliente contacta a sus clientes para confirmar las solicitudes de transacciones como retiros y transferencias en sus contratos y solicitudes de cambio de datos.

Modalidades de Fraude en la Red

Pesca (Phishing)

Este fraude se realiza enviando un correo electrónico con un mensaje muy convincente que invita a la persona a ingresar, mediante un enlace (link) a la supuesta página de su entidad o empresa de servicios, donde deberá escribir su usuario y clave.

La página que se presenta es muy similar o casi idéntica a la página original, razón por la cual cualquier persona escribirá en forma desprevenida su usuario y clave de la manera acostumbrada; pero debido a que es una página falsa no podrá ingresar y en algunos casos recibirá un mensaje de error invitando a intentarlo más tarde.

En ese momento los datos de la persona ya han sido robados y con ellos el delincuente podrá hacer todas las operaciones autorizadas al cliente original.

¿Cómo prevenirlo?

- Skandia Colombia no envía correos electrónicos solicitando datos del usuario por este medio
- Digite en la barra de direcciones del navegador las URL del grupo **www.skandia.com.co** y que al momento de realizar la transacción compruebe que tenga un icono de candando (dar click para comprobar el certificado), el cual indica que es el certificado digital y que la pagina es segura

Suplantación de Sitios Web o Email (Spoofing)

Es una técnica que seduce a los usuarios para que accedan a sitios Web falsos mediante e-mail o software espía instalado en los computadores, en la cual se abren páginas que pueden ser copia total de la imagen del sitio al que se quiere ingresar pero al intentar hacerlo, comienzan a solicitar información financiera o simplemente cuando se ingrese los datos de usuario y clave secreta el ingreso falla y se muestra una página de error.

¿Cómo prevenirlo?

- Revise que la conexión del sitio Web sea segura (con el ícono del candado en la parte posterior)
- Desconfié de páginas raras o cambiadas. Llame a Skandia y pregunte si el proceso de identificación ha sido cambiado

Software Espía (Spyware)

Al navegar por Internet es posible que sin saberlo se instale Software espía en los computadores. Existen varias empresas que utilizan este tipo de Software para detectar tendencias de navegación o para generar publicidad no requerida (SPAM) directamente en los computadores de los usuarios. En el peor de los casos, hay grupos de delincuentes que utilizan este tipo de Software para capturar información de las personas como números de tarjetas de crédito, números de identidad, etc.

¿Cómo prevenirlo?

- Instale Antivirus y Software de prevención de Anti–Spyware y manténgalos actualizados
- No instale programas de fuente desconocida
- No utilice computadores públicos o poco seguros como en Cafés Internet

Capturadores de Teclado (Keylogger)

Este tipo de Software generalmente se instala de forma "oculta" junto con otros programas que aparentemente tienen otro fin como juegos o tarjetas de felicitación o programas que llegan por e-mail. Su verdadera función es capturar la información que se digita en el computador especialmente contraseñas y números de tarjetas de crédito.

¿Cómo Prevenirlo?

- Instale Antivirus y Software de prevención de Anti–Spyware y manténgalos actualizados
- No instale programas de fuente desconocida
- Utilice el teclado virtual cuando digite sus datos de usuario y clave en el Portal de Skandia Colombia

Swapping

Los estafadores utilizan la ingeniería social (robar información privada de los usuarios) para hacerse pasar por clientes legítimos ante representantes de atención al cliente de compañías telefónicas para obtener una nueva tarjeta SIM con la línea telefónica de los usuarios.

El swapping es un tipo de fraude por medio del cual los delincuentes duplican la SIM card de una persona para acceder a su información. Los celulares y los números telefónicos son cada vez más importantes para las personas y por ende se convierten en elementos atractivos para los criminales.

Cuando los criminales se quedan con la línea telefónica utilizan información importante de las víctimas como la dirección de correo, documentos de identidad, entre otros datos. En los móviles no solo se almacenan los datos de contacto de familiares y allegados, sino también aplicaciones bancarias. Adicionalmente, el número telefónico de los usuarios suele estar registrado dentro de los perfiles transaccionales ante entidades financieras, y se acostumbra a usarlos como canal de autenticación o de validación de identidad.

¿Cómo evitar el swapping?

- Primero que todo cuida tus datos personales
- No utilices como código PIN o código de verificación una fecha o un número que alguien pueda asociar a ti.
- Si cuentas con perfiles en internet, elimina la información personal y borra los perfiles de las aplicaciones que ya no utilices.
- No almacenes toda tu información en el celular y no vincules cuentas bancarias al número de teléfono.
- Instala aplicaciones de seguridad para evitar que terceros puedan acceder a tus datos personales.
- En los casos de hurto de celulares, es preciso solicitar al operador de telefonía bloquear el IMEI del móvil, bloquear el equipo y borrar el contenido de forma remota.

Recomendaciones dentro del Portal Transaccional de Skandia- Portal de Clientes

Una vez ingrese con su usuario y contraseña, en la parte superior derecha podrá comprobar la fecha y hora de la última conexión al Portal de Clientes Skandia, así como la fecha actual de la consulta, confirmada por sus nombres y apellidos completos.

Para solicitar su clave de acceso al Portal de Clientes, debe comunicarse al Contact Center Skandia personalmente. Allí, después de validar sus datos, le asignarán un usuario y contraseña.

Después de ingresar por primera vez al Portal de Clientes Skandia, el sistema le pedirá cambiar la contraseña asignada por una nueva que usted debe definir y recordar para próximas oportunidades.

En caso de bloqueo de su contraseña, debe ponerse en contacto con Skandia personalmente a través del Contact Center, en la línea 658 4000 / 484 1300 o línea nacional 01 8000 517 526.

Para salir de forma segura del sitio, haga uso de la opción “Salida Segura”, ubicada en el menú izquierdo del Portal.