

RECOMENDACIONES DE PREVENCIÓN DE FRAUDE Y CIBERSEGURIDAD PARA EL USO DEL PORTA EMPRESARIAL

Implemente estas 4 prácticas para operar con confianza y fortalecer la protección de su organización. **¡Contamos con usted!**

- **Gestione usuarios y accesos:** Asigne permisos según roles y necesidades específicas.
- **Use contraseñas seguras:** Actualícelas regularmente y no las comparta.
- **Monitoree transacciones:** Revise movimientos y notificaciones en tiempo real.
- **Autenticación avanzada:** Active mecanismos como OTP o doble factor.

1 Cuidado con el “Phishing”, método que utilizan los ciberdelincuentes para engañar y obtener información personal y financiera que puede llevar a robo de identidad, contraseñas, datos bancarios y hasta afectar equipos electrónicos con algún tipo de virus.

Estos ciberdelincuentes aprovechan cualquier situación y han creado métodos que emiten a sus víctimas a través de correos electrónicos, WhatsApp, Facebook, entre otros. Skandia nunca solicitará información personal y financiera a través de correos, mensajes de texto SMS, WhatsApp y Facebook.

2 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: - negociosfiduciarios@skandia.com.co prevenciondefraude@skandia.com.co y ciberseguridad@skandia.com.co**

3 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.

4 Vigile todos sus productos financieros, compruebe regularmente sus extractos y asegúrese de acusar recibo de todas las transacciones realizadas.

5 Skandia nunca solicita información confidencial vía correo electrónico, SMS o llamada telefónica como: Producto, número del producto, fecha de expedición de su documento, número de documento, contraseñas o passwords.

6 Desconfíe de las llamadas que ofrecen promociones y requieren este tipo de información confidencial, cuelgue inmediatamente y notifique a Skandia sobre estas situaciones, esto nos permitirá identificar y proteger a nuestros clientes de personas mal intencionadas o grupos criminales.

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.

7 Acceda al portal digitando siempre <https://www.skandia.com.co> y el portal corporate <https://corporate.skandia.com.co/> nunca lo haga a través de un link o enlace. Siempre verifique que en el navegador este la palabra HTTPS.

8 Nunca utilice la opción recordar clave en los navegadores personales y públicos.

9 Mantenga sus dispositivos personales (computador, tabletas, celulares, etc) actualizados con los últimos parches de seguridad y con antivirus.

10 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.

11 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.

12 Si sospecha que su correo ha sido comprometido, cambie sus contraseñas inmediatamente, active el doble factor de autenticación (2FA), verifique la opción y datos de recuperación, escanee su dispositivo en busca de malware, informa a tus contactos.

13 Las medidas básicas para proteger el correo electrónico son:

- Tener una contraseña segura
- Habilitar el segundo factor de autenticación,
- No abrir correos de remitentes desconocidos,
- No abrir enlaces desde correos.
- No ingresar al email desde dispositivos que no son de confianza

14 Evite realizar transacciones financieras desde redes WIFI gratuitas, públicas o desconocidas (como aeropuertos, cafés, bibliotecas, etc).

15. Nunca comparta sus contraseñas ni otros datos confidenciales por correo electrónico, mensajes o teléfono.

Skandia le podrá enviar mensajes vía correo electrónico con enlaces a sitios informativos de la Compañía; en los mismos, nunca se solicitará el ingreso de información y/o claves personales. En caso de encontrar alguna irregularidad, agradecemos que la misma sea reportada a ciberseguridad@skandia.com.co. Para conocer nuestra política de tratamiento de datos, ingrese aquí. Recuerde que puede enviar sus consultas a cliente@skandia.com.co. Por favor no responda este correo electrónico. La información contenida en este e-mail es confidencial y sólo puede ser utilizada por la persona a la cual está dirigida. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje está prohibida y será sancionada de conformidad con las leyes aplicables. Si por error recibe este mensaje, por favor elimínelo de manera inmediata.