

## RECOMENDACIONES PARA UN ADECUADO USO DE LOS SERVICIOS ELECTRÓNICOS

El Banco GNB Sudameris cuenta con una moderna infraestructura tecnológica mediante la cual pone a disposición de sus Clientes una variedad de servicios con adecuados niveles de seguridad. Con estas recomendaciones buscamos que usted sea partícipe de esta tecnología y efectúe un uso más seguro de nuestros servicios electrónicos.

### 1. Cuidados con su Clave.

- ✓ Nunca revele su clave; ésta es personal e intransferible.
- ✓ Nunca la digite en presencia de otras personas, ya sean amigos, compañeros de trabajo o familiares.
- ✓ Memorícela y nunca la escriba donde pueda ser leída por otras personas.
- ✓ Cámbiela con frecuencia.
- ✓ Debe seleccionar el periodo de expiración de la clave en el momento del registro por primera vez en la Banca Virtual o si desea cambiarla en otro momento, puede hacerlo dando clic en "personalizar Banca Virtual". Elija periodos cortos (30 días), ya que son más seguros.
- ✓ Si sospecha que alguien más conoce su clave, cámbiela inmediatamente.
- ✓ Algunos navegadores ofrecen la opción de almacenamiento automático de claves; sin embargo, se recomienda que no habilite este servicio, o deshabilítelo si se encuentra activo y borre las claves que tenga almacenadas en éste servicio.
- ✓ En la creación de claves incluya diferentes letras y números. Evite la utilización de palabras o eventos que sean fácilmente relacionados con usted, tales como nombre de familiares, ciudades, mascotas, la marca o placa del vehículo, etc.
- ✓ No atienda correos solicitando claves o información de carácter confidencial. Si nota alguna actividad sospechosa en sus cuentas, puede informarla a través de cualquiera de los siguientes canales:
  - Gerente/Director de Negocios.
  - Línea de Atención al Cliente GNB en Contacto (57) 601 307 7707 en Bogotá o en otras ciudades 018000 910499 / 018000 910660.
  - Línea de Atención al Cliente GNB Premier (57) 601 336 1500 en Bogotá o en otras Ciudades 018000 512236.
  - Línea de Soporte a Canales Electrónicos Persona Natural (57) 601 380 8702 en Bogotá o en otras ciudades: 018000 112751
  - Línea Especializada de Servicios Electrónicos Empresariales (57) 601 210 9573 en Bogotá o en otras Ciudades 018000 516111.

El Banco nunca le solicitará sus claves para soportar procesos y procedimientos internos.

### 2. Ejecución de Transacciones a través de la Banca Virtual.

- ✓ Como medida adicional de Seguridad se recomienda el uso del Token para la autenticación inicial y para la realización de operaciones dentro de la Banca Virtual. Si cuenta con el servicio de Banca Móvil, el uso del Token en la Banca Virtual es obligatorio.
- ✓ Para verificar la validez del sitio, dé doble clic en el candado ubicado en la parte inferior izquierda de la pantalla. Se abrirá una ventana que muestra el certificado digital del Banco a nombre de servicios.sudameris.com.co y su fecha expedición y vencimiento.
- ✓ Cuando realice transacciones, prepare todo lo necesario antes de iniciar la conexión, de forma que no deje su computador solo mientras busca un dato o recibo para continuar.

- ✓ Utilice para su conexión un equipo conocido o “confiable”, como su computador personal o el de su empresa, que tenga instalado un programa de antivirus actualizado, programas conocidos y que la configuración de seguridad del navegador impida que se instalen programas en forma automática cuando está navegando en Internet.
- ✓ Cuando quiera acceder a los servicios que ofrece el Banco GNB Sudameris a través de Internet, no lo realice en un “Café Internet” o desde computadores de acceso público, desconocidos o de poca confianza. Sus claves pueden ser descubiertas y utilizadas con propósitos dolosos.
- ✓ No deje la sesión abierta después de haber ingresado con su usuario y clave, cuando tenga que realizar otras actividades en las que se deba alejar temporalmente del equipo.
- ✓ Evite que personas no autorizadas usen su computador personal.
- ✓ Efectúe todas sus transacciones en la Banca Virtual, haciendo uso del Dispositivo de Seguridad Token físico o del Token virtual activando su servicio de Banca Móvil, el cual le brinda mayores niveles de seguridad.

### 3. Virus y Otros Programas Masivos.

- ✓ Tenga presente que existen programas diseñados para capturar todo lo que se escribe en el teclado, almacenarlo y distribuirlo a sitios desconocidos en Internet o permitir su lectura local (programas espías), éstos generalmente se encuentran ocultos y no se pueden ver a simple vista; por lo tanto, se recomienda instalar en su computador programas de seguridad en internet y antivirus.
- ✓ No abra mensajes de correo de extraños o desconocidos, o con un asunto irregular que invite a abrir el mensaje y los archivos anexos. Si tiene dudas, borre el mensaje sin abrirlo, ya que existen muchas formas de motivarlo a abrir mensajes cuyo contenido puede ser un virus o un programa espía.

### 4. Navegación (Browser).

- ✓ Nuestra Banca Virtual funciona mejor con los siguientes navegadores de internet:
  - Internet Explorer Versiones Win.11 - Edge o superior.
  - Google Chrome Versiones Win / OS 64.0.3282.186 o superior.
  - Apple Safari Versión 11.0.3 o superior.
  - Mozilla Firefox Versiones OS.58.0.2 (64-bit) o superior.
- ✓ Mantenga actualizado el software de navegación de su preferencia, de acuerdo con las recomendaciones del fabricante.
- ✓ Tenga precaución y desconfíe de los programas o software gratuitos que ofrecen varios sitios de Internet. Verifique cuidadosamente su procedencia y confiabilidad, antes de instalarlos y utilizarlos, ya que puede tratarse de un programa espía.

### 5. Recomendaciones de Seguridad y Cuidados del Dispositivo Físico de Seguridad Token.

- ✓ Dé aviso al Banco en caso de hurto, robo, pérdida y/o fraude del Token, con el fin de efectuar el respectivo bloqueo.
- ✓ Guárdelo en un lugar seguro donde no pueda extraviarse o ser extraído por terceros.
- ✓ Manténgalo en un lugar seco y alejado de las variaciones de temperatura.
- ✓ No permita que otras personas observen la clave que genera el Token.
- ✓ No acepte ayuda de terceros, el Token es personal e intransferible.
- ✓ No lo exponga a campos magnéticos.
- ✓ Evite que sea golpeado o sometido a algún esfuerzo físico.
- ✓ No intente abrirlo, retirar la batería o placa de circuitos, ya que ocasionará su mal funcionamiento.

- ✓ No lo introduzca en agua u otros líquidos.

NOTA: Tenga en cuenta que, al activar la Banca Móvil, el token físico asignado para ingresar y/o realizar transacciones en la Banca Virtual se inactiva, por lo tanto, cuando desee acceder a la Banca Virtual, sólo podrá utilizar el token (código) generado en la Zona Pública de la Banca Móvil.

#### 6. Recomendaciones de Seguridad y Cuidados del Dispositivo Móvil y Token Virtual para el Uso de Banca Móvil.

- ✓ En la creación del PIN. Evite la utilización de números seguidos, (de menor a mayor y viceversa), la recepción del mismo número o eventos que sean fácilmente relacionados con usted, tales como fechas de nacimiento, número de documento de identidad y/o número de placa del vehículo, etc.
- ✓ Memorice su PIN de Banca Móvil, no lo escriba ni la revele a otra persona.
- ✓ Cambie su PIN con frecuencia o si sospecha que alguien más lo puede conocer.
- ✓ Siempre que digite su PIN, hágalo con precaución, sin que otra persona pueda visibilizarla fácilmente.
- ✓ Por su seguridad, la clave y PIN no aparecen en la pantalla de su celular al momento de ser digitadas.
- ✓ Al ingresar su PIN errado más de tres veces, éste será bloqueado y se reactivará automáticamente al día siguiente.
- ✓ Cuide su celular, en caso de pérdida o robo solicite inmediatamente a su operador de telefonía celular el bloqueo del mismo junto con el de la tarjeta SIM.
- ✓ Si desea restablecer el servicio debido al olvido de PIN, podrá solicitarlo a través de la Banca Virtual.
- ✓ En caso que desee restablecer el servicio por extravío o cambio de su número de celular, debe descargar la aplicación "Banca Móvil Banco GNB Sudameris" en el nuevo dispositivo móvil, seleccionar la opción "Ya soy usuario" en la Zona Pública de la Banca Móvil e ingresar los datos solicitados.
- ✓ No permita que otras personas observen la clave que genera el Token Virtual.
- ✓ No acepte ayuda de terceros, el Token Virtual es personal e intransferible.
- ✓ En caso de pérdida de su celular o si sospecha que su línea has sido objeto de SIM Swapping (secuestro del número celular), informe esta novedad a la Entidad, para evitar posibles fraudes con sus productos.

Si requiere información adicional comuníquese con:

Línea de Atención al Cliente GNB en Contacto  
Bogotá: (57) 601 307 7707  
Otras Ciudades: 018000 910499 - 018000 910660  
Horario de Atención: lunes a viernes 7:00 a.m. a 7:00 p.m.  
sábados, domingos y festivos 8:00 a.m. a 5:00 p.m.

Línea de Atención al Cliente GNB Premier (Exclusiva para clientes GNB Premier)  
Bogotá: (57) 601 336 1500  
Otras Ciudades: 018000 512236  
Horario de Atención: lunes a viernes 8:00 a.m. a 5:00 p.m.

Línea de Soporte a Canales Electrónicos Persona Natural  
Bogotá: (57) 601 380 8702  
Otras ciudades: 018000 112751  
Horario de Atención: lunes a viernes 8:00 a.m. a 5:00 p.m.

Línea Especializada de Servicios Electrónicos Empresariales  
Bogotá: (57) 601 210 9573  
Otras Ciudades 018000 516111  
Horario de Atención: lunes a viernes 8:00 a.m. a 5:00 p.m.

Asesor en Línea "Chat" y Buzón Contáctenos en [www.gnbsudameris.com.co](http://www.gnbsudameris.com.co)