CARTILLA DE SERVICIOS ELECTRÓNICOS

El Banco ofrece al Cliente determinados instrumentos electrónicos que posibilitan el acceso a los servicios del Banco a través de la utilización de medios electrónicos de comunicación o transmisión de datos entre el Banco y el Cliente.

Recomendaciones para el buen uso de los instrumentos electrónicos.

- Utilizar el instrumento electrónico de acuerdo con las condiciones del Contrato.
- Al acceder por primera vez al servicio y ante cualquier duda que se le presente en cuanto a la utilización del instrumento, Ud. deberá requerir al Banco, las instrucciones necesarias acerca de su uso.
- La utilización de los instrumentos electrónicos será realizada en forma personal o a través de las personas que autorice, no pudiendo ceder ni transferir a terceros los derechos emergentes de este contrato, asumiendo la más absoluta y exclusiva responsabilidad por toda operación que pudiera realizar cualquier persona no habilitada ante el Banco con los datos y claves de propiedad del Cliente. El Cliente será el único responsable por la selección de dichas personas y el uso de Identificación, Claves y PIN correspondientes, comprometiéndose a extremar las medidas que resulten necesarias a fin de resguardar la confidencialidad y confiabilidad de las identificaciones electrónicas y claves utilizadas. El Banco quedará expresamente facultado para dar entrada a sus servicios y cursar instrucciones que reciba a través del mismo cuando dichos actos se verifiquen mediante la utilización de las identificaciones electrónicas y claves seleccionadas por el Cliente sin asumir el Banco responsabilidad alguna por cualquier daño o perjuicio que pudiera provocar el uso no autorizado, indebido o fraudulento de los instrumentos electrónicos, identificaciones o claves, por parte de personas autorizadas o terceros.
- El Cliente deberá modificar y actualizar su PIN siguiendo las recomendaciones otorgadas por el Banco. Asimismo se obliga a no divulgar este código de identificación personal u otro código, ni escribirlo en el instrumento electrónico o en un papel que se guarde con él.
- Deberá tomar todas las medidas adecuadas para garantizar su seguridad. El Cliente/Usuario será responsable de guardar el instrumento electrónico en un lugar seguro y de verificar periódicamente su existencia.
- El Cliente es responsable de destruir o entregar al Banco los instrumentos electrónicos vencidos.
- El Cliente no deberá digitar el PIN en presencia de otras personas, ni facilitar el instrumento electrónico a terceros, ya que el mismo es de uso personal.
- El Cliente deberá informar al Banco en forma inmediata sobre: el robo o extravío del instrumento electrónico; aquellas operaciones que no se hayan efectuado correctamente; el registro en su cuenta de operaciones no efectuadas y fallos o anomalías detectadas en el uso del servicio (retención de tarjetas, diferencias entre el dinero dispensado o depositado, etc.).
- En caso de pérdida, hurto o robo del instrumento electrónico, el Cliente se obliga a dar aviso de inmediato al Banco al teléfono 1991, sin perjuicio de suscribir posteriormente el correspondiente formulario ante el Banco.
- El cliente se abstendrá de utilizar los dispositivos electrónicos cuando se encuentren mensajes o situaciones de operación anormales.
- Todo intento de comunicación por medios y formas no acordados con el Banco, no deberán ser respondidos por el Cliente.
- El Banco nunca le solicitará sus claves de identificación personal, por ningún concepto.
- Notificar al Banco inmediatamente a que se produzca cualquier cambio de domicilio, de número telefónico, de la firma registrada y, en general cualquier otro dato que haya experimentado modificación de los que hubiera facilitado con anterioridad a la entidad.

® Marca registrada de The Bank of Nova Scotia, utilizada bajo licencia.

Responsabilidad del Cliente.

- El Cliente toma conocimiento y reconoce que la Clave y los distintos medios de identificación o seguridad electrónica son estrictamente confidenciales. El Cliente se hace plenamente responsable por cualquier tipo de orden que el Banco reciba a través de los medios referidos, aún las que fueran realizadas fraudulentamente o por personas no autorizadas. El Cliente acepta que no es obligación del Banco detectar errores en la transmisión o en el contenido de las solicitudes de información o instrucciones impartidas.
- El Cliente será responsable de las operaciones no autorizadas por él, efectuadas con su instrumento electrónico hasta el momento de la notificación al Banco del robo, extravío o falsificación del instrumento electrónico o de su clave personal.
- El Cliente será responsable de indemnizar al Banco todo daño que cause al sistema por el mal uso de los instrumentos electrónicos puestos a su disposición.

Recomendaciones básicas para Clientes que utilizan Internet como herramienta de comercio electrónico

- No responda ningún e-mail donde se le solicite información de tipo financiera o personal sin antes verificar el origen de dicho e-mail con la Entidad correspondiente. Tenga en cuenta que los datos más críticos de sus Tarjetas de Crédito son su Número, Fecha de Vencimiento y Código de Seguridad. Scotiabank Uruguay S.A. nunca le solicitará información específica sobre sus Cuentas, Tarjetas o Claves de Acceso vía correo electrónico ni por páginas electrónicas referenciadas (links) a través de dicho medio. Si recibe un e-mail solicitando este tipo de información favor reportarlo inmediatamente al Servicio de Atención al Cliente, teléfono (02) 1991.
- No acceda al sitio de Scotiabank Uruguay S.A. a través de links insertos en e-mails, le recomendamos agregar la dirección de correo de Scotiabank Uruguay S.A. (www.scotiabank.com.uy) en su lista de favoritos o bien digitarla en la barra de direcciones de su navegador.
- No comparta con nadie y bajo ninguna circunstancia sus claves de acceso a banca electrónica, servicios de Home Banking, PIN de sus Tarjetas de Débito o Crédito.
- Utilice claves de acceso con largos mínimos de 8 dígitos, no utilice secuencias numéricas o alfabéticas obvias, trate de no utilizar nombres propios, fechas (aniversarios, nacimientos, etc.), número de su casa, matrícula de su vehículo o cualquier otro que pueda ser conocido por más personas y relacionado con Ud.. Una buena práctica es utilizar secuencias alfanuméricas que únicamente tengan sentido para Ud. logrando el efecto fácil de recordar difícil de descubrir.
- No utilice computadoras públicas para realizar operaciones por Internet en banca electrónica.
- Mantenga actualizado el antivirus, antispyware, el navegador que utiliza para acceder a Internet y el sistema operativo de su computadora, ponga especial atención en las más recientes actualizaciones de seguridad del mismo, éstas corrigen vulnerabilidades de seguridad detectadas por los fabricantes. Sugerimos fuertemente el uso de firewall personal y Trusteer Rapport en su computadora para aumentar el nivel de protección y la utilización de Tokens para transaccionar en banca electrónica. (*Trusteer Rapport está diseñado específicamente para proteger las transacciones online, evitando el robo de identidad. Esto lo realiza dotando de mayor seguridad al navegador (browser) del usuario, mitigando la probabilidad de que éste sea afectado por malware el cual podría alterar sus transacciones)
- El Token es un dispositivo creado para prevenir el riesgo de fraude electrónico cuando realizas operaciones con el banco vía Internet (Scotia en Línea). El Token genera distintas claves numéricas de 8 dígitos que sustituirán al PIN para la autorización de las transacciones.
- No descargue software a su computadora de sitios desconocidos o que le merezcan sospechas.
- Antes de realizar compras en Internet, busque información sobre el sitio en el que pretende realizar transacciones para tratar de verificar dentro de lo posible que se trata de una Empresa seria.
- Lea bien las condiciones de la compra antes de efectuarla, ya que muchos sitios utilizan modalidades de cobro mediante las cuales Ud. paga todos los meses una cuota por el servicio o producto, lo cual podría no ser lo que finalmente pretendía.
- Verifique antes de realizar transacciones que el sitio en el que se encuentra es seguro, en caso de no serlo evite ingresar información confidencial. Le recordamos que las páginas de Scotia en Línea de Scotiabank Uruguay S.A. son seguras manteniendo un adecuado nivel de encriptación entre su computadora y nuestro sitio. Por mayor información sobre el Certificado Digital SSL utilizado por Scotiabank Uruguay S.A. haga click sobre el sello VeriSign Secured desplegado en las páginas seguras del Banco, las que podrá identificar al visualizar el protocolo HTTPS en lugar de HTTP en la barra de direcciones o navegación de su navegador, una vez que comience a transmitir datos cifrados su navegador mostrará símbolos que le permitirán identificar que la comunicación está encriptada,

busque en la barra inferior de su navegador un candado o una llave dependiendo del tipo de navegador que utilice, ante cualquier inconveniente que pueda surgir recuerde que el número telefónico del Servicio de Atención al Cliente de Scotiabank Uruguay S.A. es (02) 1991.

Recomendaciones de Scotiabank Uruguay S.A. para el uso seguro de sus tarjetas

- Firme su tarjeta en el momento que la reciba de Scotiabank Uruguay S.A., de esta manera los Comercios donde la utilice podrán comparar su firma con la de su documento de identidad, evitando que otras personas puedan hacer uso de la misma.
- No proporcione su número de tarjeta, la fecha de vencimiento de la misma y/o el código de seguridad a ninguna persona que se lo solicite en forma telefónica, aunque su interlocutor mencione que la información se solicita por razones de seguridad o verificación, a menos que esté totalmente seguro de la identidad de la persona que le está llamando y de la Entidad a la que representa.
- Proteja sus tarjetas como si fuese efectivo, nunca las deje fuera de su vista, manténgalas a buen recaudo.
- Memorice su PIN, no lo lleve impreso junto a su tarjeta, evite usar claves obvias.
- Verifique siempre que en los comprobantes de venta esté impreso el monto correcto de la compra antes de firmarlos, guarde las copias de sus comprobantes y compare con los estados de cuenta mensuales para asegurarse que no existan cargos no autorizados.
- No permita que los cajeros o vendedores anoten su dirección en los recibos de la transacción (salvo que el mismo sea impreso por el mismo sistema de facturación del Comercio), ni el número completo de su tarjeta, éste deberá aparecer enmascarado en los recibos electrónicos generados por terminales de tipo POS o bien sistemas del propio Comercio, no así en los manuales donde se imprime el relieve del plástico, tampoco deberá permitir que su código de seguridad sea impreso bajo ningún concepto, esta información no es necesaria para el Comercio, únicamente se utiliza para gestionar la autorización de la compra por parte del Emisor de la tarjeta.
- Limite el número de tarjetas y otra información personal que lleva en la cartera, bolso o billetera, en caso de pérdida o robo, reporte el incidente inmediatamente a nuestro Centro de Autorizaciones Teléfono (02) 1991 para evitar que se realicen consumos posteriores al reporte.
- Recuerde que su tarjeta es para exclusivo uso personal, si desea extender las ventajas y beneficios de la misma solicite adicionales sin costo.
- Mantenga a buen recaudo sus Estados de Cuenta, en los mismos existe información de interés para alguien que quiera robar su identidad.
- Mantenga sus datos actualizados para que podamos ofrecerle un mejor servicio.

Consultas y Reclamos: El Banco cuenta con un servicio de atención de consultas y reclamos en todas sus oficinas de atención al público o a través del teléfono 1991, donde el Cliente podrá efectuar cualquier consulta o reclamo relativo al presente instrumento. Los reclamos también podrán ser remitidos vía electrónica a través de Scotia en Línea: www.scotiabank.com.uy

Supervisión: Esta institución se encuentra supervisada por el Banco Central del Uruguay, por más información Ud. puede acceder a www.bcu.gub.uy

El Cliente suscribe una copia de la presente Cartilla como constancia de la recepción de la misma.

RECIBI(MOS) COPIA.

En la ciudad de _____ el _____ de _____ de 20 _____

Nombre: _____	Nombre: _____
Domicilio: _____	Domicilio: _____
Nº D.I.: _____	Nº D.I.: _____
Firma: _____	Firma: _____