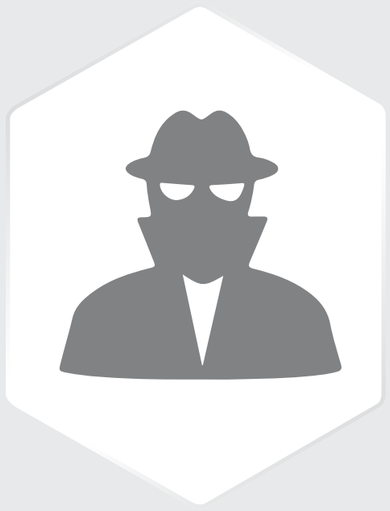
SEGURIDAD EN INTERNET

Para su tranquilidad, a la hora de realizar operaciones a través de nuestro servicio de Banca por Internet, le recomendamos lea atentamente la siguiente información sobre seguridad:

PISHING



Periódicamente se detectan envíos de correos masivos indiscriminados, remitidos desde direcciones electrónicas falsas, con el único objetivo de conseguir información confidencial de los clientes.

A esta técnica se la conoce con el nombre de **"PISHING"**.

En estos mensajes, **con la excusa de mejorar la seguridad de sus cuentas o de consultar una supuesta transferencia recibida a su favor**, se invita a pulsar un enlace incluido en el texto y que, en caso de pulsarlo, les llevará a una página web falsa que suplantan a las páginas originales de las entidades financieras, pudiendo figurar cualquiera de las entidades que componen nuestro Grupo, donde les pedirán sus claves de Banca Electrónica.

Estos intentos son detectados y puestos de inmediato en conocimiento de la Policía Nacional para su investigación. Pero la mejor manera de evitar cualquier posibilidad de estafa, consiste en

NO FACILITAR NUNCA SUS CLAVES A NADIE, PUES NI SIQUIERA NUESTRA ENTIDAD LE SOLICITARÁ DICHAS CLAVES NI POR CORREO ELECTRÓNICO, NI POR TELÉFONO, NI EN PERSONA.

CLAVES PERSONALES

Con el contrato de Banca por Internet se entrega su **clave única e intransferible**: Contraseña que se equipara a su firma caligráfica.

Por todo esto y por su seguridad, **en ningún caso deberá facilitar su clave** a quien se la pida por teléfono, e-mail, personalmente o por cualquier otro medio, incluso aunque manifiesten solicitarla en nombre del Banco, ya que nunca le solicitaremos su clave fuera de la página de identificación de Banca por Internet. Así mismo, es conveniente que su navegador tenga **desactivada la opción de "Guardar contraseñas"** en:

Explorer: Herramientas > Opciones de Internet > Contenido > Información personal > Auto completar > Desactivar nombres de usuarios y contraseñas

Netscape: Editar > Preferencias > Privacidad y Seguridad > Desactivar recordatorios de contraseñas

PÁGINA WEB SEGURA

TRANSMISIÓN DE LA INFORMACIÓN

Las transmisiones de información entre su ordenador y el servidor web de Visión Banco se realizan mediante el protocolo de encriptación SSL de 128 bits, la máxima encriptación que existe actualmente.

ZONA WEB SEGURA

Para comprobar que se encuentra en páginas seguras, la dirección de la página deberá comenzar por https://. Además, en la parte inferior de la pantalla deberá aparecer un "candado cerrado" o una "llave". Nuestro servicio de Banca por Internet está en una zona web segura.

CERTIFICADO DE SEGURIDAD

El certificado expedido por la empresa Verisign garantiza la seguridad de nuestro sistema. Si al acceder al servicio, su navegador no reconoce nuestro Certificado, le indicará que este ha caducado, por lo que deberá actualizarlo en su ordenador haciendo doble clic encima del "candado", que aparece en la parte inferior de la pantalla, y pulsar "Instalar certificado".

Verificar la autenticidad y los datos del certificado haciendo click en los siguientes enlaces que se encuentran en el homebanking:

CertiSur SITIO SEGURO

VeriSign Secured VERIFICAR

TENER EN CUENTA

INFORMACIÓN EN TIEMPO REAL

Si la información que se le muestra no está actualizada, si al realizar cualquier operación no se actualizan los saldos, etc., compruebe que su navegador está configurado correctamente:

Explorer: Herramientas > Opciones de Internet > General > Archivos de Internet > Configuración > Cada vez que se visite la página

Netscape: Editar > Preferencias > Avanzadas > Caché > Siempre

DESCONEXIÓN DEL SERVICIO

Para cerrar las conexiones con las páginas seguras sin que ningún usuario pueda acceder a ellas sin identificarse, es recomendable utilizar el botón de "salida", centro superior del encabezado del servicio de Banca por Internet.

VISION Banco

CLAVES Y CONTRASEÑAS

- Su usuario, contraseña, pin de tarjeta, firma, etc., son personales e intransferibles, por lo que no debe revelarlos a nadie bajo ningún concepto.
- Cambie periódicamente sus claves de acceso y contraseñas, en especial cuando tenga la sospecha o duda sobre la confidencialidad de las mismas.
- No utilice las mismas claves y códigos en todas sus entidades financieras, ni use claves vinculadas al usuario (nombres de familiares, mascotas, fechas de nacimiento, teléfonos, etc.).
- Evite la introducción de sus claves en terminales de uso público (cibercafés, aeropuertos, etc.).

PROTECCIÓN DE SU EQUIPO

- La protección de su equipo es clave, por lo que debe disponer de un sistema operativo correctamente actualizado con los últimos parches y mejoras de seguridad recomendadas por el fabricante.
- Instale en su equipo un software antivirus y manténgalo permanentemente actualizado para evitar infecciones de virus o de programas maliciosos.
- Instale un software cortafuegos o 'firewall' personal antes de acceder a Internet y manténgalo siempre actualizado.
- Revise con cierta periodicidad los registros de actividad (ficheros de 'log') que generan estas herramientas en busca de anormalidades o eventos no comunes.
- Desactive en su navegador las funciones de almacenamiento automático de claves en “caché”.
- Elimine periódicamente las cookies y archivos temporales.
- Realice con cierta frecuencia una copia de seguridad de los archivos de su PC.

NAVEGACIÓN Y E-MAILS

- Navegue únicamente por sitios conocidos que le inspiren confianza. Debe ser prudente al visitar webs desconocidas, sobre todo si le invitan a que se descargue ficheros y programas.
- No abra mensajes de correo electrónico si tiene alguna duda sobre su procedencia o si contienen títulos sin sentido o inesperados.
- No utilice enlaces incorporados en e-mails o páginas web de terceros.
- Sea cauteloso al leer e-mails.
- No ingrese datos confidenciales cuando e-mails de desconocidos lo soliciten. Recuerde que el Banco no le enviará mails solicitando el ingreso de información personal o claves.
- No ingrese a vínculos de páginas web recibidos por e-mail.
- Analice con antivirus los e-mails que contengan tarjetas virtuales, promociones o descuentos, verificando su procedencia.

VISION Banco