PROTECCION DE DATOS Y SEGURIDAD INFORMATICA
BANQUE HERITAGE (URUGUAY) S.A.

1. Conexión Segura

BANQUE HERITAGE cuenta con las máximas medidas de seguridad para garantizar la confidencialidad de las comunicaciones entre el Banco y nuestros usuarios. El cliente podrá verificar la autenticidad de nuestros servicios web, a través del candado que se muestra a la izquierda de nuestra URL, en la barra de direcciones. Nuestro certificado esta emitido por Thawte, en la pestaña “Detalles” encontrara toda la información acerca de las características de seguridad del mismo.

2. Seguridad de sus claves y contraseñas

Su clave de acceso al e-Banking y su Token son elementos personales y privados. Cada usuario deberá custodiarlos de forma segura. No divulgue las claves ni códigos y tome las medidas adecuadas para garantizar la seguridad de los mismos. Nadie en Banque Heritage conoce sus claves.

Modifique y actualice sus contraseñas y/o claves siguiendo las recomendaciones otorgadas por el Banco. No digite claves ni contraseñas en presencia de otras personas, aún cuando pretendan ayudarlo, ni facilite el token a terceros, ya que son de uso personal. Guarde el token en un lugar seguro y verifique periódicamente su existencia. No entregue el token a terceros.

No utilice los Instrumentos Electrónicos cuando se encuentren mensajes o situaciones de operación anormales. No responda a intentos de comunicación por medios y formas no acordados con el Banco.

En caso de extravío, hurto, robo o falsificación de los Instrumentos Electrónicos o claves o códigos, o de utilización por terceros de la información contenida en los mismos sin autorización de los Clientes, los Clientes se obligan a realizar de inmediato la correspondiente denuncia ante el domicilio del Banco. También se podrá notificar al Banco al teléfono 2 916 0177 opción 1 o enviando un correo electrónico a customersupport@heritage.com.uy.

El navegador en su PC o Smartphone podrá ofrecerle la posibilidad de guardar su contraseña. Le recomendamos que nunca guarde claves de acceso al e-banking u otras contraseñas importantes ya que quedan almacenadas en la memoria de su PC o celular y pueden quedar al alcance de otras personas que utilicen esos dispositivos.

3. Desconexíón de E-Banking

Recuerde que cada vez que finalice su sesión de e-banking deberá cerrarla con la flecha de salida que aparece arriba, a la derecha de la pantalla. De esta forma habrá finalizado de forma segura su sesión en e-banking.

Recomendaciones

- SIEMPRE que reciba una llamada o contacto sospechoso, contáctenos por los canales oficiales.
- RECUERDE que el Banco nunca realizará llamadas telefónicas ni lo contactará por correo electrónico, SMS, Whatsapp o redes sociales para solicitarle contraseñas, pines, números de cuentas o de tarjetas.
- NO INGRESE DATOS PERSONALES en sitios utilizando enlaces que llegan por correo electrónico ya que pueden ser fraudulentos.
- NO RESPONDA A MENSAJES DE AVISO sobre supuestos errores al realizar transferencias bancarias, solicitudes de pago irregulares o cambios en los datos de la cuenta a la que se pide enviar fondos. Ante cualquier duda, siempre comuníquese telefónicamente con el Banco.
- NO BRINDE DATOS PERSONALES relacionados a cuentas (claves, pin, usuarios, token, fotocopia de CI, ni ningún tipo de dato) por mail, teléfono, redes sociales o whatsapp.
- NO acuda al cajero automático, abra la app o acceda a su e-banking si recibe una llamada supuestamente proveniente del Banco.
- NUNCA brinde contraseñas o información confidencial ante llamadas de personas que se PRESENTAN COMO FAMILIARES O PERSONAS DE SU CONOCIMIENTO y que planteen situaciones de ALARMA Y URGENCIA.
- PROTEJA SUS DISPOSITIVOS con contraseñas y en caso de disponer tecnología biométrica, actívela.
- SIEMPRE UTILICE CONTRASEÑAS SEGURAS, que contengan números, letras y signos especiales, con un largo mínimo de 8 caracteres. No deben ser datos obvios como fechas de nacimiento, direcciones o nombres. CAMBIE frecuentemente sus contraseñas.
- Mantenga el token y los dispositivos de autenticación físicamente seguros y bajo control permanente.
- No utilice equipos públicos o dispositivos de otras personas para acceder a sus app, redes sociales o cuentas de uso personales.
- NO USE REDES WIFI PUBLICAS para acceder a sitios que requieran de contraseñas.
- MANTENGA ACTUALIZADO el sistema operativo, antivirus, el navegador y las aplicaciones de sus equipos.
- DESCONFÍE de correos electrónicos que presenten archivos adjuntos, en especial con extensiones .xlsm, .doc, xls o archivos .zip con contraseña. En estos casos verifique la procedencia y autenticidad del mail antes de abrir o descargar los adjuntos.
- ESTÉ ALERTA cuando ingrese en el sitio del banco. Siempre que ingrese a la página transaccional del Banco, verifique que el URL empiece por https y corresponda a la dirección web del Banco.
- NUNCA acceda al sitio del Banco por medio de enlaces que le envíen por correo electrónico.
- LE RECOMENDAMOS ESTABLECER ALERTAS para las compras realizadas con sus tarjetas. Al momento de realizar el pago de las compras asegúrese tener frente a usted el POS utilizado, y verifique que los bordes del mismo estén bien sellados.

- En la medida de lo posible, configure el firewall de la red para que permita la navegación del equipo desde donde se realizan transacciones, únicamente a los portales bancarios.

4. Protección de Datos

BANQUE HERITAGE garantiza la protección de los datos de sus clientes. Es por ello que el sitio web el Banco no reconoce de modo automático ningún dato referente a la identidad de los visitantes de sus páginas. A fin de garantizar la seguridad y confidencialidad de las transacciones, para acceder al e-banking de Banque Heritage, es necesaria la previa identificación y autenticación del usuario en el sistema, por medio de la utilización de claves de acceso y token en determinados casos.

Todos los datos sobre nuestros clientes son tratados con estricta reserva no siendo estos accesibles a terceros para finalidades distintas de aquellas para las que han sido brindados, sin el expreso consentimiento del titular de los datos.