Recomendaciones de Seguridad

1.1. PORTAL TRANSACCIONAL/BANCA MÓVIL

- ✓ La Clave Principal y Segunda Clave es personal e intransferible, no se puede compartir con nadie. Dar a conocer las claves generará riesgos de fraudes.
- ✓ Preferiblemente y para un mejor funcionamiento, tener instalado en su PC un navegador como Internet explorer 9, Firefox 40, Chrome 45, Safari 9 y Opera 35 o superiores.
- ✓ No escriba la clave en ningún lado, memorícela.
- ✓ LA ENTIDAD nunca solicitará el cambio de la clave principal a través de correo electrónico o mensajes de texto.
- ✓ Cuando defina “las preguntas de seguridad”, evite ingresar respuestas obvias o que sean conocidas por terceras personas, utilice contraseñas fáciles de recordar para usted, no utilice fechas de nacimiento, número de documento de identidad, dirección o teléfonos, memorícelas y no las escriba en ningún lugar.
- ✓ Realice cambios de clave de manera preventiva, por lo menos una vez por mes.
- ✓ El uso de su usuario y contraseña de acceso al sistema es responsabilidad de usted, no permita que otra persona las utilice.
- ✓ Realice sus operaciones y/o transacciones únicamente desde equipos de uso personal, en su casa u oficina, evite el uso de equipos ubicados en sitios públicos que no sean de absoluta confianza como un café internet, salas universitarias o lugares donde extraños puedan tener acceso a su información confidencial.
- ✓ Nunca preste su cuenta para recibir fondos cuyo origen usted desconoce, delincuentes utilizan este método para la transferencia de dinero de procedencia ilícita.
- ✓ Nunca ingrese a través de enlaces en correos electrónicos falsos (phishing), que puedan llevarle a sitios fraudulentos. Recuerde que la ENTIDAD no solicita información confidencial por este medio.
- ✓ Instale y mantenga actualizado su computador con herramientas de seguridad informática (antivirus, antispyware, firewall personal y actualizaciones del sistema operativo), lo cual le protege contra espionaje y robo de información.
- ✓ Mantenga los navegadores actualizados a su última versión.
- ✓ Si utiliza un computador portátil, le recomendamos no acceder al PORTAL TRANSACCIONAL/BANCA MÓVIL desde una conexión inalámbrica (WiFi) pública, por ejemplo, en aeropuertos o parques.

- ✓ Usted debe tener total confidencialidad con la información de los usuarios y claves de acceso al PORTAL TRANSACCIONAL/BANCA MÓVIL.

- ✓ Una vez termine sus operaciones y/o transacciones en el PORTAL TRANSACCIONAL/BANCA MÓVIL debe asegurarse de realizar el cierre de sesión de forma segura.

- ✓ Si le llega un reporte de una transacción que usted no ha realizado debe proceder de inmediato a bloquear el canal del PORTAL TRANSACCIONAL/BANCA MÓVIL, comunicándose con LA ENTIDAD.

- ✓ Cuando ingrese a la página web de la ENTIDAD verifique siempre que la imagen del candado en la parte superior de su navegador, aparezca y se encuentre cerrado.

- ✓ Cuando realice compras por Internet, cerciórese que sean páginas seguras (verificando que esté presente el candado de seguridad en la parte inferior, o muestre en la dirección el prefijo https) de lo contrario no estará segura la confidencialidad de sus datos personales y financieros.

- ✓ Evite descargar e instalar programas de fuentes desconocidas, estos pueden contener programas escondidos o virus que pueden comprometer su información.

- ✓ Mantenga actualizado su computador con herramientas de seguridad como antivirus, antispyware, firewall personal, y actualizaciones del sistema operativo, con el fin de protegerse de programas maliciosos que sustraigan su información.

- ✓ Evite proporcionar datos personales a través del perfil de las redes sociales (Facebook, Twitter, Pinterest, etc.)

- ✓ Evite diligenciar formularios en sitios web para suscribirse a boletines en línea o participar en rifas.

- ✓ Evite diligenciar formularios físicos donde le solicitan actualizar datos a cambio de algún beneficio.

1.2. BANCA MOVIL

- ✓ Mantenga el teclado de su teléfono celular bloqueado, No lo deje desatendido, no lo preste a desconocidos.

- ✓ Utilice una clave de acceso al celular que no sea obvia y no la comparta.

- ✓ Recuerde cambiar regularmente la contraseña de Banca Móvil.

- ✓ No almacene nunca las contraseñas de acceso al móvil o a los servicios financieros en los listines del móvil o en archivos dentro del mismo. En caso de que así lo requiera haga uso de programas para cifrado de datos.

- ✓ No descuide su celular. En caso de pérdida o robo de su teléfono celular, comuníquese inmediatamente con su operador e inhabilite su número, también informe a LA ENTIDAD para el bloqueo del canal.

- ✓ Si acostumbra instalar o bajar aplicaciones (programas) en su equipo móvil hágalo solo de sitios conocidos que garanticen la no presencia de programas maliciosos (malware, spyware, virus), valide las condiciones de uso antes de aceptar la instalación.

- ✓ No navegue en sitios desconocidos con su móvil. Podría tener ataques similares a los que se tiene en el PC.

- ✓ Si su equipo móvil requiere de mantenimiento o actualizaciones nunca entregue las claves de acceso al personal de mantenimiento. Además valide que no le hayan instalado programas o aplicaciones diferentes a las que usted normalmente utiliza.

- ✓ No habilite por defecto los puertos bluetooth. Solo hágalo para conectarse a los dispositivos que utiliza con el móvil. Configure la autenticación para dichos puertos evitando que un desconocido se pueda conectar a su móvil sin su conocimiento.

- ✓ Si hace uso de conexiones WIFI en su móvil utilice protocolos seguros (WPA, WPA2) y no se conecte a redes desconocidas. No mantenga activa la conexión WIFI.

- ✓ Si su móvil tiene opciones de seguridad adicionales (caso de blackberry, Iphone, equipos de alta gama y algunos de media) haga uso de ellas y conozca con detalle las funcionalidades que prestan.

- ✓ Si acostumbra hacer backup del software de su móvil y de los datos guardados en él, hágalo en una estación (PC) conocida y asegúrese de que sólo usted tenga acceso a dicha información. Utilice programas para protección de su móvil, si éste cuenta con los aplicativos para ello. Hoy existen para determinados equipos soluciones de antivirus y similares