

## REQUERIMIENTOS A LA SEGURIDAD DE INFORMACIÓN DE LOS DISPOSITIVOS MÓVILES

¡Estimados Clientes!

Para minimizar el riesgo de acceso desautorizado a las Cuentas del Cliente por parte de malechores y minimizar el riesgo de intrusión en la información clave el Banco pide con insistencia a los Clientes cumplir las siguientes medidas de seguridad de información:

- Usar la protección de contraseña en el dispositivo móvil, realizar el cambio periódico de contraseñas. Las contraseñas para el acceso al dispositivo móvil y para el acceso al Sistema Eurolink no deben coincidir.
- Instalar el bloqueo automático del dispositivo al transcurrir un período de inactividad.
- No entregar el dispositivo móvil con la aplicación del Sistema Eurolink lanzada a terceros.
- No comunicar las contraseñas del dispositivo móvil y del Sistema Eurolink a terceros.
- Usar la última versión de iOS accesible para el dispositivo móvil. Instalar las actualizaciones de seguridad de iOS sólo del sitio del productor.
- No se recomienda nada usar el Sistema Eurolink en dispositivos móviles que han sufrido una fractura (el así llamado jailbreak).
- Haciendo el copiado de reserva del dispositivo móvil es obligatorio cifrar las copias de reserva del dispositivo.
- No trabajar en el Sistema Eurolink cuando el dispositivo móvil está conectado a través de las redes Wi-Fi abiertas en lugares públicos (en el café, en el aeropuerto etc.) sin protección del tráfico con el cifrado (deben ser las redes con la protección mínima de WPA/WPA2).
- En caso de que el Cliente detecte operaciones sospechosas en el Sistema Eurolink debe comunicarlo inmediatamente al Banco.
- En caso de que el Cliente pierda el dispositivo móvil es necesario comunicarlo inmediatamente al Banco.
- En caso de venta o entrega del dispositivo móvil a terceros sin falta elimine la aplicación del Sistema Eurolink y realice la restauración de los ajustes de la fábrica (el así llamado hard reset).