



BANESCO PROTEGE SUS OPERACIONES CON DIVERSOS MECANISMOS DE SEGURIDAD

Banesco refuerza sus procesos de seguridad con herramientas de última generación y de estándar internacional que permiten la verificación y autenticación de las transacciones bancarias de sus clientes.

Banesco Banco Universal, institución bancaria de capital 100% venezolano, ofrece diferentes mecanismos de seguridad para proteger las transacciones y operaciones bancarias de sus clientes: la Clave Dinámica Banesco, la Llave Banesco y la Certificación PCI son algunos de los sistemas que convierten a Banesco en una institución confiable y segura.

De manera permanente y sistemática, Banesco refuerza sus procesos para proteger la información y operaciones de sus clientes. De igual manera, actualiza las herramientas de verificación y autenticación para prevenir fraudes, riesgos y amenazas en las transacciones cotidianas.

Clave Dinámica: es un mecanismo de seguridad que consiste en un código numérico que se obtiene en la aplicación BanescoMóvil y cambia cada 30 segundos para una mayor seguridad. Los clientes que realicen transferencias a terceros en Banesco u otros bancos, o al mismo titular en otras entidades bancarias, requerirán de la Clave Dinámica para realizar la transacción. La clave también se solicitará para agregar o modificar datos del directorio de pagos y/o transferencias o para eliminar dispositivos registrados en BanescoOnline.

¿Cómo funciona la Clave Dinámica?

1. Los clientes Banesco deben descargar el aplicativo BanescoMóvil para tener acceso a la Clave Dinámica.
2. En el menú de la pantalla de inicio del aplicativo aparece la opción para solicitar esta clave -abajo a la derecha.
3. La generación de la Clave Dinámica no depende de la disponibilidad de datos móviles o conexión a internet.
4. Tiene una duración de 30 segundos y pasado este tiempo, podrá solicitarse una nueva.

Llave Banesco: es un sistema de seguridad de última generación que valida la identidad de los usuarios de BanescoMóvil al momento de hacer transferencias a otros bancos. Está diseñado para fortalecer la seguridad ante intentos de suplantación de identidad como el *phishing*. Con la Llave Banesco las operaciones son verificadas con cualquier mecanismo de autenticación o desbloqueo que utilice el dispositivo como la huella, rostro o PIN. La Llave Banesco está disponible en la versión actualizada del aplicativo de BanescoMóvil tanto para sistemas operativos iOS y Android.

El usuario de BanescoMóvil debe contar con la versión actualizada del aplicativo. Para activar la Llave Banesco en la banca móvil requiere de estos pasos:

1. Abrir la App BanescoMóvil en el teléfono.

2. Ingresar datos de usuario y contraseña.
3. Crear la Llave Banesco, siguiendo las indicaciones.

Una vez que la Llave Banesco esté creada, el usuario puede consultar su estado en las opciones adicionales del BanescoMóvil (sección Más), ingresando al botón Administrar la Llave Banesco.

Certificación PCI: Banesco tiene la certificación PCI DSS V 4.0 por GM Sectec, un estándar internacional de seguridad de la industria de tarjetas de pago que garantiza la protección de los datos y transacciones de los clientes. Con la certificación Banesco refuerza sus prácticas de seguridad en el negocio de medios de pago, además de lograr estándares internacionales para la prevención de fraudes, riesgos y amenazas en el sistema y procesos del banco.

Clave de Operaciones Especiales: es un método de autenticación en transacciones que requieran un factor de confirmación adicional, así como para usuarios que no tengan el aplicativo BanescoMóvil. En estos casos la Clave de Operaciones Especiales se envía por mensajería de texto o correo electrónico.

Recomendaciones para fortalecer la seguridad digital y financiera:

1. Utilice los canales oficiales de Banesco: [Banesco.com](https://www.banesco.com), BanescoMóvil, Asistente virtual DANI (+58 414-2784473), Instagram (@banescobancouniversal), X @Banesco, Facebook (Banesco Banco Universal), Banca telefónica 0500-BANCO24 (0500-2262624) o (0212) 501.1111.
2. Use contraseñas seguras y no compartidas. Asegúrese de que sean complejas, combinando letras, números y símbolos.
3. No abra enlaces ni archivos adjuntos sospechosos. Los ciberdelincuentes utilizan técnicas como el *phishing* para robar credenciales. Banesco nunca pedirá a sus clientes claves o datos sensibles por estos medios.
4. Monitoree sus movimientos bancarios y transacciones con frecuencia. Reporte inmediatamente cualquier comportamiento inusual a monitoreodefraude@banesco.com o por el (0212) 501.10.29.
5. No comparta su cuenta, productos financieros ni información bancaria personal en plataformas de procedencia desconocida, mensajería de texto en respuesta a mensajes promocionales o llamadas telefónicas.
6. Asegúrese de que su dispositivo (computadora, teléfono inteligente o tableta) tenga un antivirus y un sistema operativo actualizados para protegerse contra malware y otras amenazas informáticas.

La seguridad y confiabilidad son una de las prioridades de Banesco, ofreciendo a sus clientes el más alto estándar de protección bancaria y las mejores herramientas que aseguren sus datos y operaciones.

Encuétranos como

