Banesco Banco Universal: Escalando Autenticación Resistente al Phishing a 2,2 Millones de Usuarios

El Desafío de Negocio

Banesco identificó cuatro desafíos de autenticación que afectaban tanto a la seguridad como a la experiencia del cliente:

Exposición al phishing y la ingeniería social. La dependencia anterior de códigos de un solo uso (One Time Passcodes) enviadas por SMS y correo electrónico dejaba a los clientes vulnerables. Los atacantes utilizaban campañas de phishing y vishing para manipular a los clientes y hacer que entregaran sus códigos temporales, eludiendo así los controles OTP sin necesidad de romperlos tecnológicamente.

Fricción en transacciones de alto valor. La autenticación basada en credenciales añadía una fricción innecesaria a los flujos de pago que los clientes utilizaban con mayor frecuencia, incluidos los pagos rápidos P2P y las transferencias de alto valor.

Sobrecarga en la respuesta al fraude. Cuando los sistemas de monitoreo de fraude identificaban actividades sospechosas, la resolución de esas alertas requería la intervención manual del equipo de soporte. Los clientes no tenían un mecanismo de autogestión para resolverlo.

Consistencia omnicanal. Los clientes acceden a los servicios a través de la web y el móvil. Banesco necesitaba un enfoque de autenticación que funcionara de manera consistente en ambos canales sin requerir soluciones temporales específicas para cada uno.

Por qué Banesco Eligió Passkeys (Claves de acceso)

Banesco evaluó sus opciones de autenticación basándose en dos requisitos fundamentales: la solución debía ser resistente a la ingeniería social y debía funcionar de manera consistente en la web y el móvil sin requerir implementaciones separadas por canal.

Los Métodos Tradicionales Dejaban Abiertas Vulnerabilidades Importantes

Los esquemas OTP entregados por SMS y correo electrónico eran la capa de autenticación principal de Banesco. Esos esquemas dependen de un secreto compartido. Un atacante no necesita vulnerar el mecanismo criptográfico; es suficiente con convencer al cliente de que entregue el código. Ningún enfoque basado en OTP podía cerrar esa brecha.

Las Passkeys Ofrecen lo que Otros Métodos No Entregan

Las passkeys utilizan criptografía asimétrica para asegurar que las claves privadas nunca salen del dispositivo del usuario. Esto elimina por completo los secretos compartidos del flujo de autenticación, erradicando el riesgo de ataques de intermediario (man-in-the-middle) que los esquemas OTP no pueden prevenir. El cambio también se alineó con la estrategia del grupo bancario multinacional de estandarizar el uso de passkeys en toda la organización.

Banesco

Banesco Banco Universal es el principal banco privado en Venezuela, con más de 2,4 millones de usuarios mensuales activos en sus plataformas de banca web y móvil. El banco ofrece servicios digitales para pagos entre pares (P2P) y transferencias de alto valor. Banesco opera dentro de un grupo bancario multinacional, y la estrategia de seguridad global del grupo impulsó directamente el cambio del banco hacia una autenticación resistente al phishing.

Resumen de la Implementación

Banesco realizó un despliegue por fases a través de tres etapas que se completaron en siete meses.

Fase 1: Evaluación Técnica. El equipo integró los servidores FIDO con la infraestructura bancaria central y validó la compatibilidad en las plataformas web y móvil antes de cualquier despliegue de cara al cliente.

Fase 2: Piloto en Flujos de Bajo Riesgo. Banesco introdujo las passkeys primero en casos de uso de menor riesgo, estableciendo líneas base de adopción e identificando puntos de fricción antes de un lanzamiento más amplio.

Fase 3: Despliegue Masivo. Una vez completado el piloto, Banesco activó las passkeys para 2,2 millones de usuarios en transacciones de alto valor y pagos rápidos P2P. El banco también integró las passkeys como mecanismo de verificación para las transacciones identificadas por sus sistemas de monitoreo de fraude, permitiendo a los clientes resolver por sí mismos las alertas de fraude sin tener que contactar a soporte.

Resultados e Impacto

Banesco ha observado resultados en adopción, experiencia del cliente y operaciones de fraude desde que completó el despliegue masivo.

Adopción y Volumen de Transacciones

- **2,2 millones** de usuarios se autentican activamente con passkeys de manera regular, lo que representa aproximadamente el 92% de los usuarios activos.
- **12 millones** de transacciones sin contraseña procesadas en el año en curso.
- **8,3 millones** de transacciones de alto valor completadas utilizando passkeys.

Experiencia del Cliente

La autenticación con passkeys redujo la fricción donde los clientes más la sentían: al completar pagos de alto valor y resolver alertas de fraude. Los clientes cuya actividad activa una alerta de fraude ahora pueden verificar su identidad y restaurar el acceso por su cuenta, sin necesidad de una llamada de soporte. Como resultado, los datos de la última encuesta de satisfacción del cliente muestran que los principales impulsores de satisfacción son la seguridad de la banca en línea (73%) y la facilidad de uso (72%), destacando el impacto positivo que las passkeys generan en la experiencia del cliente.

Beneficios Operativos

Trasladar la resolución de alertas de fraude al autoservicio del cliente redujo la intervención manual en el centro de atención al cliente. Los reportes de fraude relacionados con el robo de identidad han disminuido en un 65% desde el despliegue.

Visión a Futuro

Tras el éxito de su despliegue masivo, Banesco ha establecido métricas claras que demuestran la escalabilidad de la autenticación basada en passkeys. Para mejorar la protección y la experiencia digital de sus clientes, la organización tiene la intención de ampliar el uso de las passkeys, extendiéndolas como el principal método de autenticación fuera de banda (out-of-band) en todos los canales, incluida la banca telefónica y las visitas presenciales a las sucursales.

Además, Banesco avanza hacia un marco integral sin contraseñas (passwordless), con el objetivo de eliminar el almacenamiento y uso de credenciales tradicionales dentro de su ecosistema transaccional central.

Recomendaciones

Banesco ofrece estas recomendaciones para las organizaciones que planean implementar passkeys:

- **Priorizar la educación del usuario.** Los clientes deben comprender que los datos biométricos se almacenan localmente en su dispositivo y nunca se comparten con el banco. Abordar esto desde el principio reduce la resistencia durante el despliegue.
- **Comenzar donde la fricción es mayor.** Iniciar con los casos de uso que causan la mayor fricción al cliente, como la resolución de alertas de fraude, hace que el valor de las passkeys sea evidente de inmediato.
- **Utilizar un enfoque por fases.** Realizar pruebas piloto en flujos de bajo riesgo antes de la implementación total da tiempo a los equipos para descubrir casos atípicos sin exponer a toda la base de usuarios.

Perspectiva Ejecutiva

La implementación de passkeys resolvió lo que había sido un compromiso histórico entre una autenticación más sólida y una experiencia del cliente más simple.

> ***"La implementación de FIDO2 y passkeys ha sido un punto de inflexión en nuestra estrategia de ciberseguridad. Hemos logrado el equilibrio ideal: elevar la protección técnica al más alto nivel, al tiempo que empoderamos a nuestros clientes para gestionar su propia seguridad de forma segura y sencilla."***
>
> — Jesús Irausquín, CISO Banesco Venezuela