trycore | BANCA

PREVENCIÓN

Blindaje Transaccional y Prevención de Fraude

Multi-canal en una entidad financiera

Entidad financiera dominicana con 60 años de historia, líder en servicios hipotecarios, corporativos y digitales con enfoque sostenible.



DIAGNÓSTICO CRÍTICO

Identificación de Vulnerabilidades

Como parte de su estrategia de protección, la entidad detectó una brecha de seguridad determinante:

La suplantación de identidad en Contact Center, IVR y App Móvil.

Se carecía de un motor centralizado de retos para neutralizar estas amenazas.



EL ANTES

Puntos de quiebre

El diagnóstico inicial revelaba una brecha importante entre la situación actual y el blindaje requerido. El proyecto se encontraba en **"punto cero"** tras la disolución de un equipo previo.

Retos de negocio y operación

- Suplantación de identidad constante en Contact Center, IVR y App Móvil.
- Ausencia de un flujo centralizado de retos de seguridad (OTP/preguntas) dinámico por riesgo.
- Inexistencia de código previo tras la disolución del equipo anterior.

Retos técnicos y arquitectónicos

- Necesidad crítica de integrar proveedor internacional de evaluación de riesgos.
- Debate técnico con perfiles senior sobre la escalabilidad del sistema.
- Fragmentación de criterios de seguridad entre canales, creando silos de riesgo.



Retos de equipo y talento IT

1. Proyecto detenido por la **disolución del equipo previo**, sin código y bajo alta presión.
2. Necesidad de un líder autónomo para el **backend**, capaz de actuar sin guía arquitectónica.
3. Talento para **defender decisiones técnicas** ante seniors y proponer escalabilidad sólida.

NUESTRA GUÍA Y APORTE

Un aliado estratégico para la construcción del blindaje End-to-End

Para superar estos desafíos, la entidad integró a uno de nuestros Ingenieros de Desarrollo II de People Service, con profunda experiencia en seguridad financiera.

Aprovechando tecnologías como **Node.js, PostgreSQL e integraciones de riesgo**, se implementó una estrategia multi-canal:

Motor de riesgo centralizado

Evaluación en tiempo real de cada transacción para disparar retos de seguridad (OTP) de forma coherente en todos los canales.

Arquitectura flexible

Estructura diseñada para soportar cambios abruptos de requerimientos sin re-trabajo, superando estándares senior.

Cobertura omnicanal

Solución operativa en Caja, Negocios, Servicios y App Móvil, eliminando silos de seguridad previos.



RESULTADOS

Potencial desbloqueado

La entidad pasó de tener un proyecto en "punto cero" y canales vulnerables a contar con un sistema de **blindaje transaccional** robusto operando al 100% en producción. Los resultados se reflejaron en dos frentes clave:



Alto impacto cliente

Bajo impacto operativo

Alto impacto operativo

- **Seguridad multicanal para clientes**
- **Protección contra suplantación**
- **Continuidad de proyectos críticos**
- **Soporte mínimo y omnicanalidad**

Bajo impacto cliente

Resultados que transformaron la experiencia del usuario

Seguridad multi-canal unificada

El usuario final cuenta con un **estándar de seguridad único** ya sea que opere por Contact Center, IVR o App Móvil, protegido por el mismo motor de reglas de riesgo.

Protección ante suplantación en tiempo real

Gracias a los retos inteligentes (OTP y preguntas de validación), el sistema **bloquea intentos de fraude en tiempo real**, garantizando que solo el dueño real de la cuenta autorice movimientos sensibles.

Fricción reducida para el usuario legítimo

La solución **solo actúa cuando el nivel de riesgo lo requiere**, permitiendo que el cliente legítimo opere con fluidez mientras el sistema mantiene un "escudo invisible" contra atacantes externos.



IMPACTO OPERATIVO INTERNO

Eficiencia, estabilidad y reconocimiento

Continuidad y rescate de proyecto crítico

El banco reactivó un proyecto en "punto cero". El impacto interno fue pasar de la incertidumbre técnica a tener una solución robusta y finalizada operando en todos los canales.

Soporte mínimo y estabilidad

La calidad del desarrollo en Node.js permitió que el sistema entrara en fase de "soporte mínimo", liberando al equipo de TI para proyectos estratégicos en lugar de apagar incendios.

Omnicanalidad real de seguridad

El departamento de Riesgos y TI cuenta con un motor centralizado que dispara retos de seguridad de forma coherente en Contact Center, IVR y App, eliminando los silos de protección.

Ítems de reconocimiento del cliente — Perfil: Ingeniero de Desarrollo II

1. **Impacto real en reducción de fraude**
   Éxito en OTP y preguntas de seguridad.
2. **Capacidad de propuesta técnica**
   Autonomía en Node.js y PostgreSQL.
3. **Asesoría de confianza**
   Aliado estratégico con bases técnicas.
4. **Calidad en entrega final**
   Solución operativa y blindada.

"No llegamos a implementar una herramienta. Llegamos a construir desde cero un blindaje multi-canal real — OTP, validación de identidad, arquitectura sólida — que cerró una vulnerabilidad crítica de fraude... Eso es lo que significa un desarrollo que defiende el negocio."

— Ingeniero de Desarrollo II

★★★★★

Autodiagnóstico de match

Lee cada pregunta y marca con un **SÍ** aquellas que resuenen con tu situación actual. Sé honesto: identificar el problema es el primer paso para resolverlo.

- [ ] ¿Tu plataforma sufre intentos constantes de suplantación de identidad?
- [ ] ¿Sientes que tu sistema de autenticación es rígido y no se adapta al nivel de riesgo de cada transacción?
- [ ] ¿Te preocupa que un atacante pueda saltarse tus validaciones por falta de un flujo de "retos" (OTP, preguntas de identidad) centralizado?
- [ ] ¿Tienes proyectos críticos que se quedaron a medias o en "punto cero" por falta de equipo?
- [ ] ¿Te cuesta encontrar desarrolladores que no solo "piquen código", sino que debatan y mejoren tu arquitectura con fundamentos sólidos?
- [ ] ¿Tu aplicación móvil actual se siente pesada o difícil de actualizar debido a una alta deuda técnica?
- [ ] ¿Tardas demasiado en lanzar nuevas funcionalidades móviles porque no tienes una librería de componentes reutilizables?
- [ ] ¿Tu operación se detiene cuando falta un especialista porque tu equipo no tiene versatilidad para aprender y entregar en un nuevo stack?
- [ ] ¿Tu equipo de soporte gasta demasiado tiempo arreglando fallos de estabilidad en lugar de desarrollar nuevas mejoras?
- [ ] ¿Buscas un partner de Staffing que se adapte a tu cultura organizacional y horaria sin fricciones de comunicación?

Suma tus respuestas afirmativas y descubre qué tan cerca estás de transformar tu operativa:

Descubre tu diagnóstico estratégico en la siguiente página.



Sistema de scoring y resultados

Cantidad de Sí	Clasificación	Tu Diagnóstico Estratégico
8 a 10	**Match Estratégico (100%)**	Tu empresa es el gemelo operativo de este caso de éxito. **Tienes retos críticos de seguridad y escalabilidad que ya hemos resuelto.** Estamos listos para replicar este éxito contigo de inmediato.
5 a 7	**Alta Compatibilidad (75%)**	Compartimos retos similares. **Tu estructura presenta cuellos de botella que nuestra metodología puede destrabar.** Podemos optimizar tu arquitectura y acelerar tus entregas móviles.
2 a 4	**Potencial de Mejora · 40%**	Hay áreas de oportunidad claras. **Nuestras capacidades en arquitecturas robustas y componentes reutilizables pueden fortalecer puntos específicos de tu IT para evitar crisis futuras.**
0 a 1	**Exploratorio · 10%**	Salud técnica estable. **Tu infraestructura parece bajo control, pero podemos asesorarte para mantener esa vanguardia técnica y optimizar tus costos operativos de desarrollo.**

¿Te suena familiar? Hablemos

Si este checklist describe tu realidad actual, tu infraestructura está lista para evolucionar hacia una arquitectura de alto rendimiento. En este proyecto, demostramos que la clave del éxito es la apropiación técnica. Entramos en el código para optimizar procesos y acelerar la salida a producción.

Separarme un espacio. Agendemos una sesión técnica para revisar tu hoja de ruta y definir cómo podemos desbloquear tu backlog de forma inmediata.

Match estratégico

Equipo listo para replicar el blindaje transaccional de inmediato en tu organización.

Alta compatibilidad

Metodología adaptable para destrabar tus vulnerabilidades de seguridad rápidamente.

Exploratorio

Capacidades en arquitecturas robustas para fortalecer áreas y prevenir fraude futuro.

Agendemos una sesión técnica

Conoce más sobre nuestro servicio