

Caso de estudio

//ABANCA

Implantación e integración de la tecnología de localización para la detección de fraude por medio del perfilado de la identidad y el comportamiento de los lugares de operación de los usuarios de la banca online.

Cuando hablamos de transformación digital en el sector financiero estamos hablando de una nueva reconversión necesaria para el sector, **ABANCA** no solo mantiene el compromiso de ser parte de esta transformación digital de una manera innovadora y segura, si no que apuesta por el crecimiento de los clientes que utilizan los canales digitales y las aplicaciones móviles mejorando su experiencia de usuario y seguridad.



Sobre Abanca

ABANCA, una de las diez primeras entidades financieras españolas por volumen de activos, es un banco con sede en Galicia que cuenta con una red de alrededor de 700 oficinas distribuidas por España y otros 9 países. **ABANCA** apuesta por una nueva forma de hacer banca, basada en lo que denominan Sentir Común, y unos valores muy claros: responsabilidad, confiabilidad, calidad e innovación.

La entidad ha seguido desarrollando su modelo omnicanal para ajustarse a todos los tipos de clientes, combinando la proximidad de una red comercial formada por oficinas cada vez más digitales, sostenibles y accesibles, con un servicio de banca a distancia cada vez más potente y avanzado, tanto en el segmento de particulares como de empresas. Este 2021 la banca móvil superó por primera vez el nivel del millón de usuarios a principios del ejercicio, hasta situarse en más de 1.100.000 a cierre de 2021, y las transacciones digitales suponen ya el 69,6% del total.

Desafíos

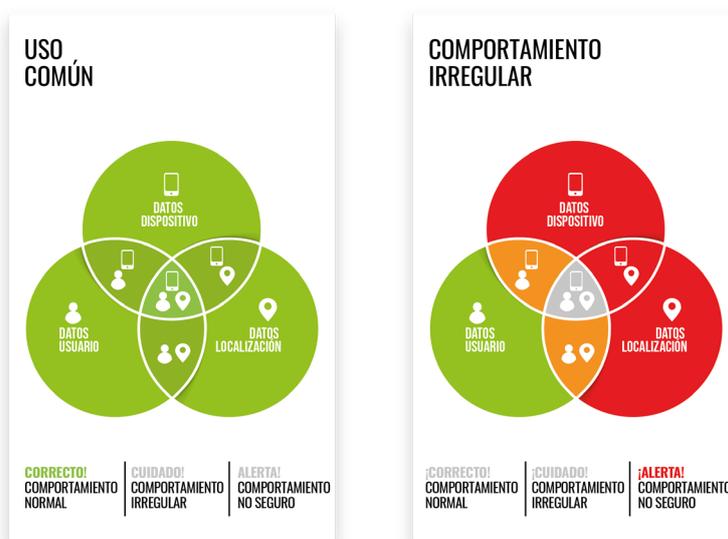
Con la evolución de las tecnologías de la información y la comunicación, además de los cambios de comportamiento de consumo a partir de la pandemia, el sector financiero enfrenta constantemente desafíos de riesgo cibernético, al ser la banca una de las industrias con mayores índices de digitalización. Se estima que en España entre el 50% -70% de los usuarios de la banca son digitales.

Solución

Ironchip proporciona a **ABANCA** una herramienta que le permite conocer si algún usuario de su red, en este caso estaríamos hablando de clientes finales de **ABANCA**, está teniendo un comportamiento anómalo o no. Dicho comportamiento está basado en los datos del usuario en cuestión, en el dispositivo asociado al mismo y en sus localizaciones frecuentes, las cuales son obtenidas a partir de las ondas radioeléctricas circundantes a un lugar y asociadas a los lugares habituales de los usuarios. Estos tres parámetros, determinan de manera muy precisa los comportamientos que llevan a cabo los usuarios, permitiéndonos tomar decisiones más rápidas y perfilar a los usuarios como fraudulentos o no.

Este nuevo paradigma de seguridad basado en localización, abre la puerta a buscar la manera de que el lugar en el cual se encuentra un usuario sea una prueba de identidad clave que nos permita no solo identificar al 95% de los usuarios de manera que no se puedan suplantar, sino que seremos capaces de identificar comportamientos que no se ajusten a identidades reales de dichos individuos y podamos así detectar a entes maliciosos en tiempo real; incluso pudiendo llegar a localizarlos en un futuro no muy lejano.

Esta casuística viene representada en la ilustración que viene a continuación, en la cual se muestran dos comportamientos diferentes: uno completamente en verde que representa el comportamiento natural de un usuario que, empleando su dispositivo habitual está iniciando sesión desde una de sus zonas comunes, mientras que en el otro caso estaríamos ante una conducta irregular, que permite identificar un posible caso de fraude debido a que, en este caso, ni el dispositivo ni el lugar son los habituales del usuario y, obviamente la relación entre ambas informaciones no coinciden:



El fin principal es implementar la geolocalización (GPS) y localización por ondas en las aplicaciones de banca móvil de **ABANCA** como mecanismo para detectar de manera muy ágil comportamientos fraudulentos, para ello la solución consta de los siguientes tres apartados:

1. Permiso de localización:

La petición de permisos de localización se ha de considerar un requisito indispensable y parte fundamental del proyecto. Esto afecta a parte del negocio y las encuestas proyectan que dependiendo del mensaje empleado las aceptaciones del permiso varían entre 65 - 82%, pero existen muchos criterios para la petición del permiso. En el Anexo 1 detallamos y explicamos cómo sería el flujo de petición ideal con el conocimiento unificado y validado de ABANCA e IRONCHIP.

2. Integración de la API:

Contemplamos varias maneras de proporcionar la información a los clientes de ABANCA:

- Integración en la lógica de negocio del BPM o SIEM vía API Rest HTTP.
- Creando un canal de stream para recibir datos en tiempo real.

3. SDK/librería móvil:

Una librería instalada en la aplicación móvil de la entidad distribuida de manera natural una vez la aplicación solicite alguna actualización. Esta librería es la encargada de proporcionar los datos, cuenta y localización del usuario cuando ABANCA considere que es oportuno hacer la petición.

A su vez, se esperan alcanzar otros objetivos claves que consolidan la apuesta tecnológica y de seguridad de **ABANCA**:

- Mejora de la seguridad de la aplicación móvil.
- Concienciación/fomento de los usuarios en la importancia de la seguridad.
- Alineación con la digitalización e implementación de PSD2.

