
B·MATCH
COMMERCIAL
20

ÍNDICE
Y OBJETIVOS
DE LA SESIÓN

Todas las áreas conocerán a la perfección **qué es B-match,** cuáles son los problemas que resuelve, cómo genera un impacto positivo en el mercado y cuáles son los beneficios que ofrece al usuario final.

01

LÍNEA DE NEGOCIO

B-Match la solución que te protege aprendiendo de ti.

02

PROBLEMA/ SITUACIÓN ACTUAL

Panorama de la industria:

En la actualidad, los **ataques a la banca móvil** se han convertido en el **principal objetivo del fraude online bancario,** esto se debe a que diariamente se enfrentan riesgos de seguridad, derivados de la suplantación o manipulación del usuario mediante **sofisticados ataques contra las aplicaciones bancarias, tales como:**

RAT in the Mobile (RitM) – Malware para acceso remoto al móvil

Smishing - Mensajes de texto dirigidos a los usuarios de telefonía móvil mediante los cuales, alguien intenta obtener información privada.

Screen Overlay – Mensajes que te piden acceder a tus fotos o archivos.

Panorama del usuario:

De acuerdo con información de la propia Condusef, **los tipos de fraude que se presentan con mayor frecuencia en la banca móvil son, principalmente, tres:**

Vishing telefónico

A través de un mensaje telefónico, los delincuentes notifican al usuario sobre cargos hechos en su cuenta y le envían una liga que los dirige hacia un portal falso. Posteriormente, lo llaman por teléfono para darle las indicaciones de los datos que debe ingresar en la misma.

Descarga de App

El delincuente baja la aplicación móvil del banco del que la víctima es cliente e ingresa los datos confidenciales de acceso para generar el fraude.

Smishing

Estafa en la cual, por medio de mensajes SMS, se solicita a los usuarios de la banca móvil datos confidenciales o se les pide que llamen a un número o accedan a página web.

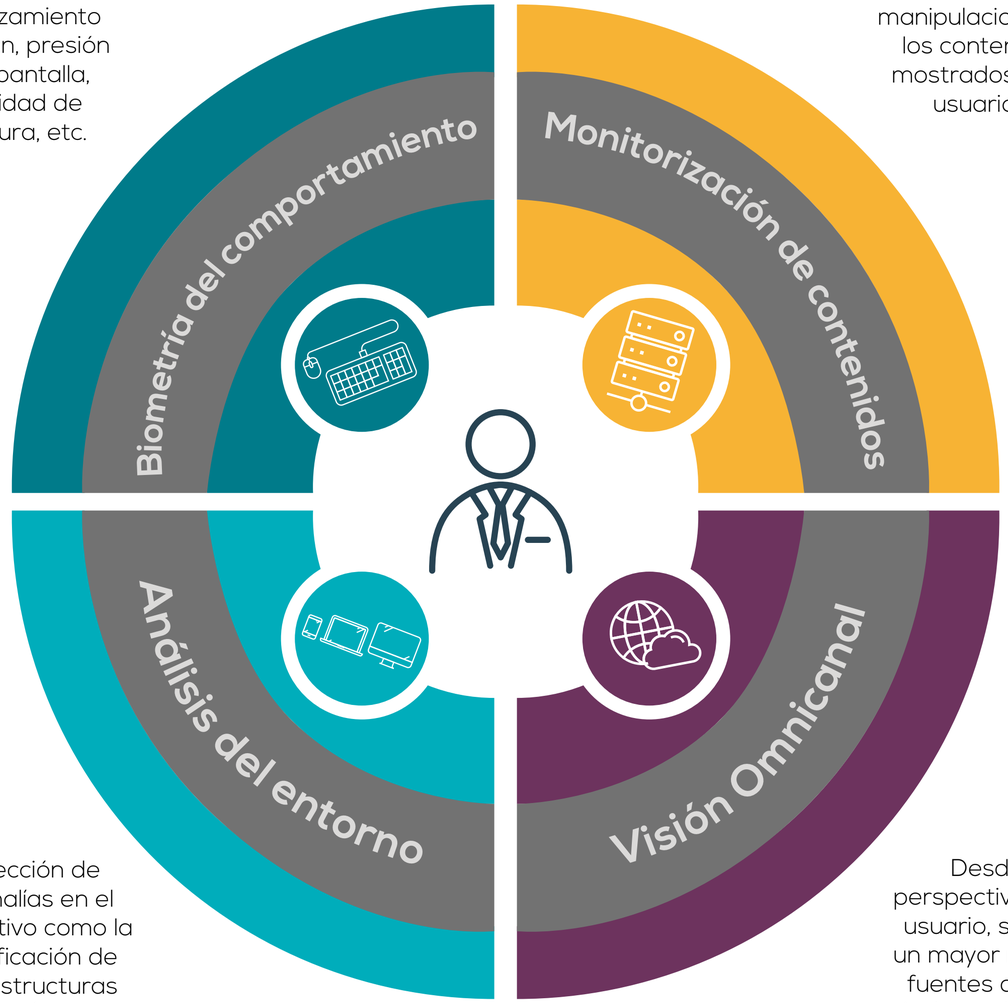
03

PRODUCTO/ DEFINICIÓN

B-match es un software para web y móvil que protege al usuario final de posibles fraudes, ya que a través de algoritmos conocidos como "deep learning", con tan solo 5 inicios de sesión **es capaz de analizar el comportamiento del usuario desde que entra a su banca móvil hasta que finaliza sus transacciones** y puede ofrecer la información precisa para alertar sobre las sesiones sospechosas.

Movimientos del teléfono móvil, desplazamiento del ratón, presión de la pantalla, velocidad de escritura, etc.

Permite detectar manipulaciones en los contenidos mostrados a los usuarios.



Detección de anomalías en el dispositivo como la identificación de infraestructuras maliciosas (redes tor, C&C, proxis anónimos, etc) o una falsa geolocalización y/o red de conexión.

Desde una perspectiva 360º del usuario, se detecta un mayor número de fuentes de fraude, incluyendo intentos de evasión de medidas de seguridad.

04

VENTAJAS COMPETITIVAS

Basado en una **tecnología innovadora de Inteligencia Artificial y Deep Learning, B-MATCH es capaz de perfilar biométricamente** y de forma única a cada usuario de la manera más precisa, rápida y completa, por lo que puede identificar cualquier intento de ataque o posible anomalía en tiempo real.

Permite una **integración rápida,** sencilla y sin impacto en los sistemas bancarios.

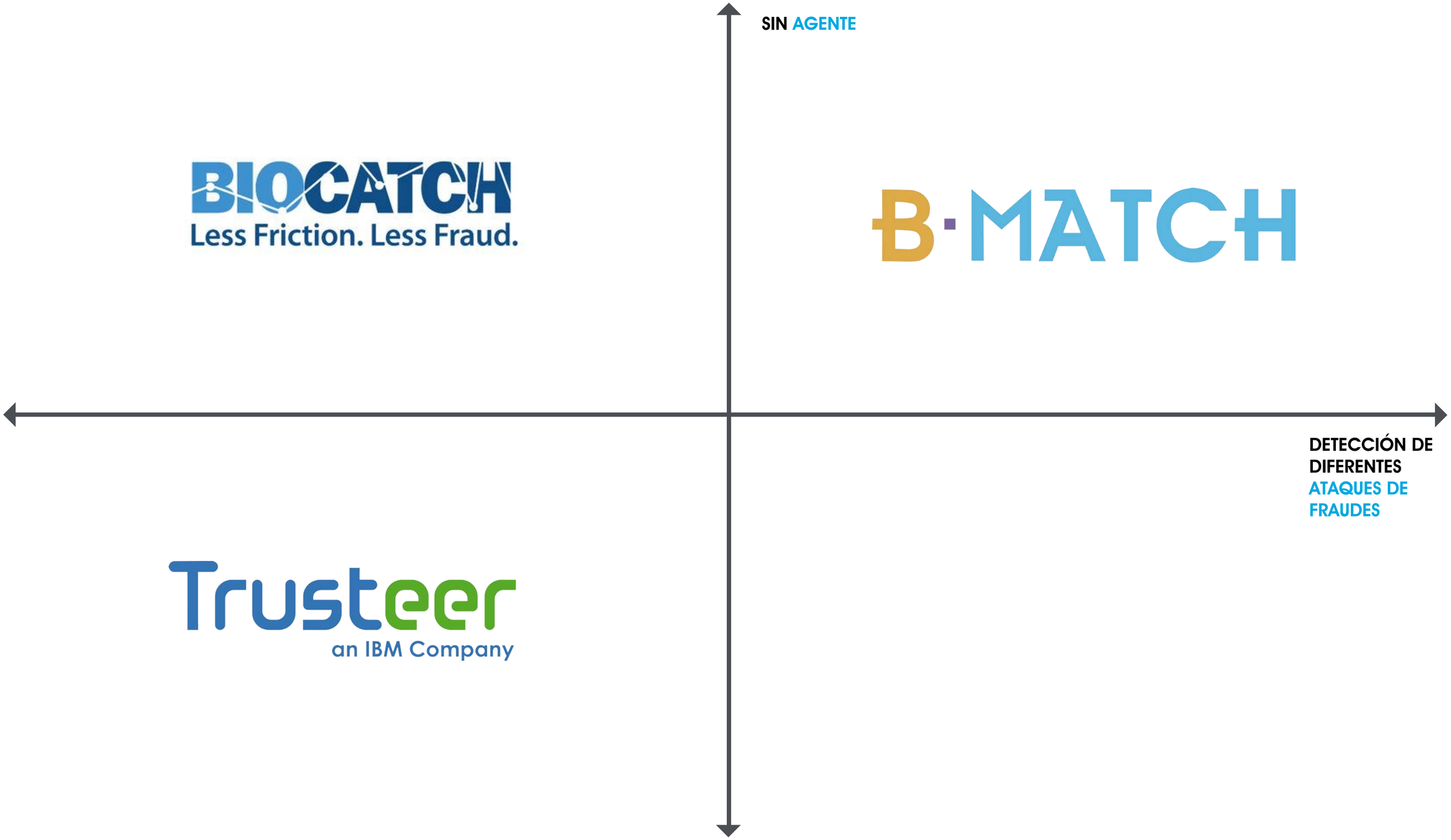
B-match **mejora la experiencia del usuario final,** debido a la reducción de los retos de autenticación y del proceso de Onboarding.

La herramienta B-MATCH **cuenta con una consola de monitoreo que despliega el porcentaje de coincidencia del usuario final,** adicional realiza el análisis del comportamiento de las operaciones que ejecuta tanto en su banca digital como en su banca móvil

La **prevención del fraude** es tanto para la banca digital como para la banca móvil

05

COMPETENCIA


SIN AGENTE
BIOCATCH
Less Friction. Less Fraud.
B·MATCH
DETECCIÓN DE DIFERENTES ATAQUES DE FRAUDES
Trusteer
an IBM Company

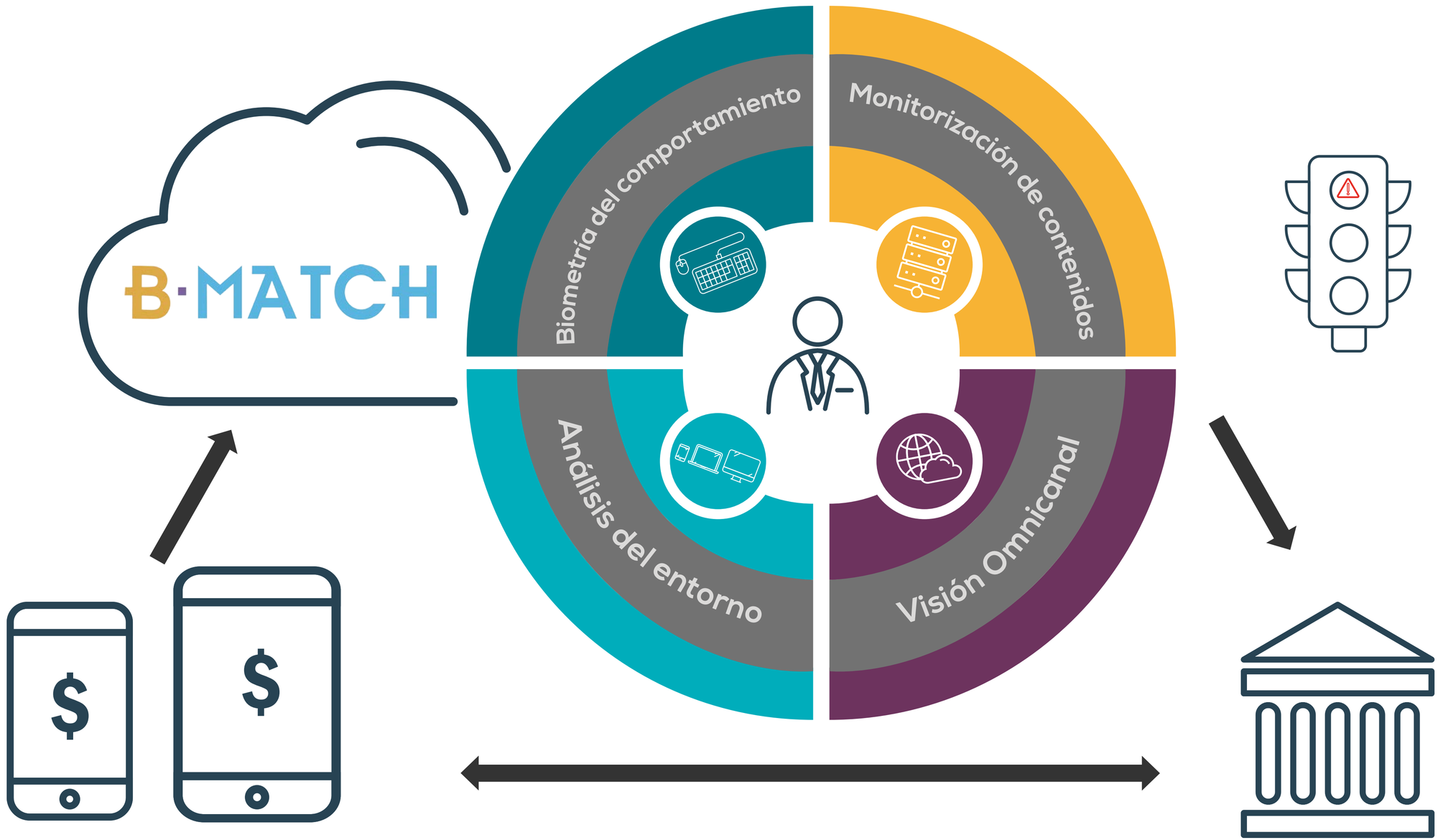
06

MODELO DE NEGOCIO

PRODUCTO	INGRESO	PAQUETES
B·MATCH	Se cobra una suscripción anual por plataforma (mínimo 5 millones de usuario)	Mobile
		Web
		Mobile + Web
		Precio total en base a número de usuarios totales

07

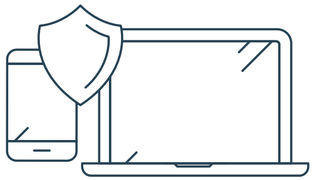
MODELO OPERATIVO


B·MATCH
Biometría del comportamiento
Monitorización de contenidos
Análisis del entorno
Visión Omnicanal
$
$

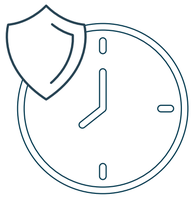
Protección
completa de sesión

Análisis de la biométrica del comportamiento del usuario

Máxima detección de Accout takeover (ATO)



Protección multicanal web y movil



Detección en tiempo real

Detección de new account fraud (NAF)

Sin fricción de UX y fácil despliegue

Fraudster hunting

Detección de malware en el endpoint

REQUERIMIENTOS TECNOLÓGICOS MÍNIMOS

PLATAFORMA PARA INTEGRACIÓN DE APIs

PROCESO DE ONBOARDING

fintspace

Conexión FINTSPACE

Obtener la documentación y especificaciones del API

Solicitar una ventana de certificación

El tiempo de pruebas es de 80 horas

Visto bueno interno con la documentación de liberación

08

FAQS

¿Qué es Deep Learning?

R= Son algoritmos basados en inteligencia artificial capaces de analizar escenarios, problemas o situaciones complejas con un gran número de variables y posibilidades, de forma rápida y precisa, brindando respuestas o alternativas con soporte y criterios claros de análisis.

¿Qué riesgos mitiga B-match?

R= Principalmente evita riesgos derivados de la suplantación o manipulación del usuario mediante sofisticados ataques contra las aplicaciones bancarias.

¿Qué es un Perfil Biométrico del usuario?

R= Es un estudio para el reconocimiento inequívoco de personas basado en uno o más rasgos que se basa en conocer un gran número de parámetros de comportamiento y físicos, (en este caso el del usuario en relación al uso de una aplicación financiera) para establecer mediante Deep Learning un perfil de su actuar digital durante una sesión.

¿Qué tipos de parámetros analiza B-match?

R= Analiza y genera un amplio número de parámetros basados en movimientos del teléfono, presión sobre la pantalla, gestos, fluidez en la escritura, geolocalización, comportamiento dentro de la aplicación bancaria, entre muchos otros.

¿Cómo se comercializa B-match?

R= B-match se comercializa con base a los usuarios por tipo de canal, esto es:
Usuario de Canal Móvil
Usuario de Banal Web
Usuario de Canal Móvil y Web

¿Qué información sensible del usuario recaba B-match?

R= Ninguna, no recaba ni almacena ninguna información confidencial o privada del usuario.

¿Cuánto tiempo requiere B-match para conocer el comportamiento de un usuario?

R= Con tan solo 5 inicios de sesión es capaz de analizar el comportamiento del usuario desde que inicia sesión hasta que la finaliza.


B·MATCH