Épica Solicitud de Screening APIS – CustomerCheck

Yo como: Usuario de negocio

Quiero que: el banco disponga de una capacidad institucional de screening integrada con Tetharay, operando a través de un servicio interno (passthrough) y un mecanismo seguro de callback, que asegure evidencia auditable, control del ciclo de vida de alertas y continuidad operativa ante fallas.

Para asegurar que todas las validaciones de clientes y transacciones contra listas restrictivas se ejecuten bajo un esquema controlado, auditable y resiliente, cumpliendo con los requerimientos regulatorios vigentes y las políticas internas de gestión de riesgo.

Criterios de aceptación:

Envío de Solicitud (Passthrough Controlado)

- Todas las solicitudes de screening deben enviarse exclusivamente a través del servicio interno del banco.
- Cada solicitud debe generar un **RequestId / CorrelationId único**.
- Debe registrarse:
  - ❖ Fecha y hora de envío.
  - ❖ Tipo de screening ejecutado (customer / investigation / transaction).

- No debe permitirse invocación directa al proveedor desde canales externos.

Recepción de Resultado (Callback Seguro)

- El endpoint de callback debe:
  - ❖ Validar autenticidad (token, firma o mecanismo definido).
  - ❖ Implementar control de idempotencia.

- El sistema debe:
  - Actualizar el estado del caso.
  - Registrar fecha/hora de recepción.
  - Almacenar el payload recibido completo solo si aplica y es necesario.

- Si el Core no responde, debe existir mecanismo de reintento automático.
- No debe generarse duplicidad de casos ante múltiples callbacks.

Trazabilidad y Auditoría

- Debe poder consultarse el historial completo por:
  - ❖ Cliente
  - ❖ RequestId
  - ❖ Fecha
  - ❖ Estado
- Debe almacenarse:
  - ❖ Decisión final aplicada
- La información debe conservarse conforme a política de retención definida por Cumplimiento.

Resiliencia y Continuidad Operativa

- Debe existir:
  - ❖ Timeout configurado.
  - ❖ Política de reintentos.
  - ❖ Manejo controlado de errores.
- Si el proveedor no responde:
  - ❖ Debe existir mecanismo de consulta posterior.

Seguridad

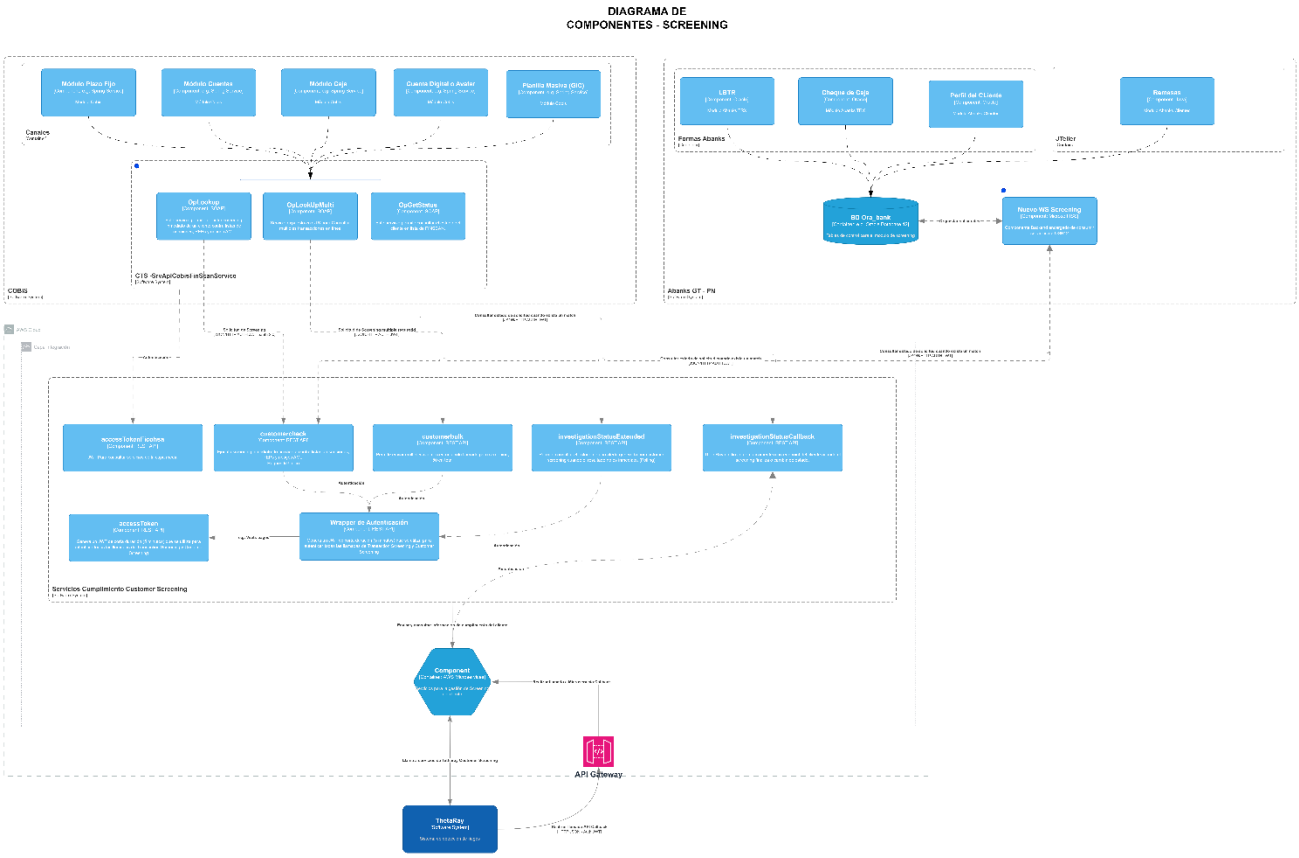
- La comunicación con Tetharay debe ser segura (HTTPS + autenticación).
- El endpoint de callback no debe ser público sin validación.
- Debe evitarse exposición de datos sensibles en logs.

Evidencia para Auditoría

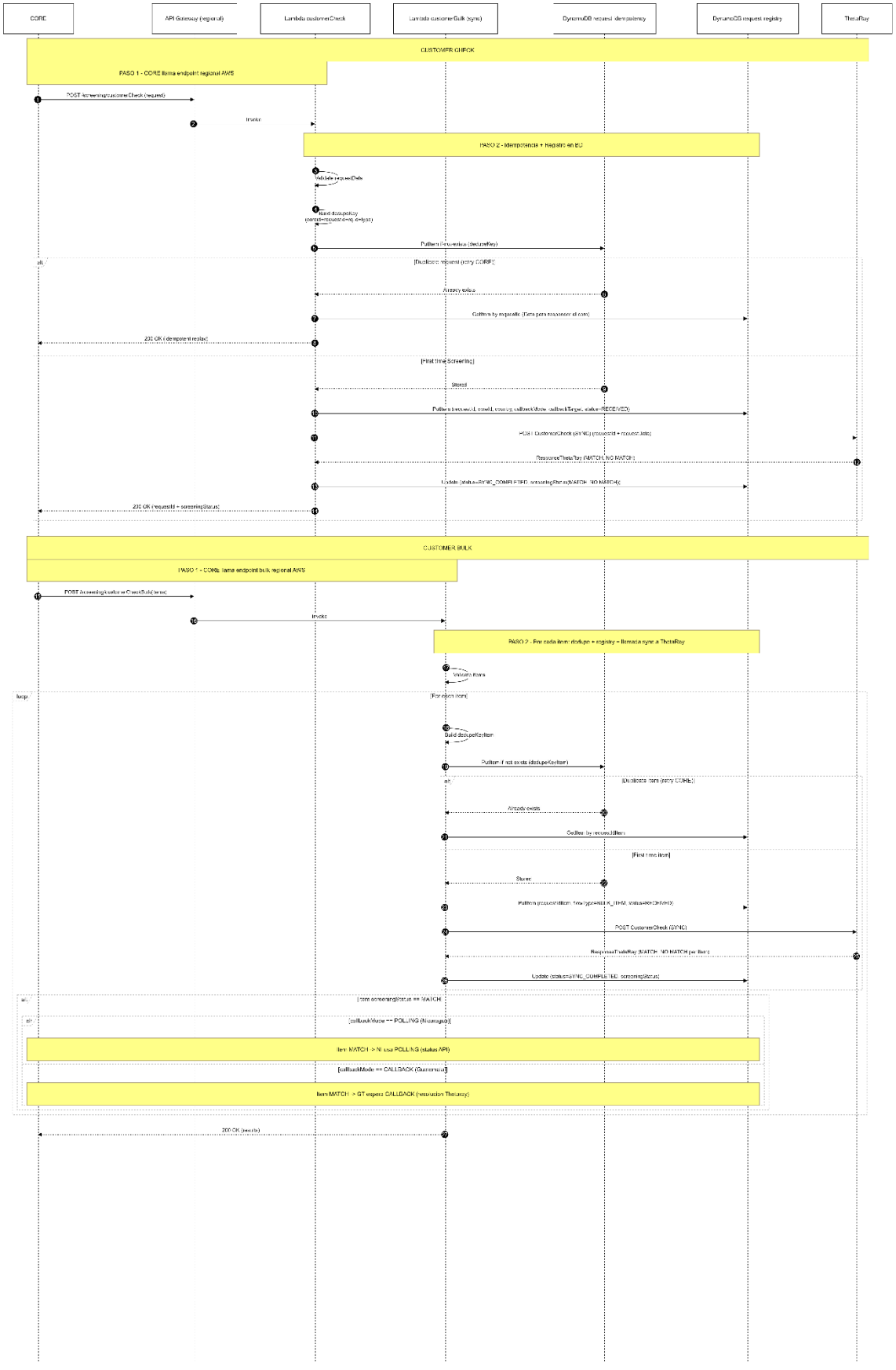
- Debe poder generarse evidencia técnica que permita demostrar:
  - ❖ Cuando se ejecutó el screening.
  - ❖ Qué resultado devolvió el proveedor.
- La evidencia debe poder exportarse en caso de requerimiento regulatorio del tiempo que se decida que persista la data.

Diagrama de Arquitectura

1. Diagrama de Componentes



2. Diagrama de Componentes



Criterios de aceptación

1. Operaciones customerCheck

1.1. Campos De Entrada de la API

Method: POST : screening/customer/check

Campo	Descripción	Requerido	Tipo/Formato
Nivel Raíz (Request)			
country	string enum ["NI","GT","PA"]	Sí	String
coreId	identificador lógico del core	Sí	string
callbackMode	string enum ["POLLING","CALLBACK"]	Sí	string
requestId	Identificador único de la solicitud. Debe ser único entre todas las solicitudes.	Sí	String (20–200 caracteres)
requestData	Objeto que contiene la información del cliente a evaluar.	Sí	Object
profile	Perfil de screening a aplicar. Si no se envía, se aplican las configuraciones por defecto.	No	String
saveForRescreening	Flag para habilitar Ongoing Monitoring (rescreening).	No	Boolean
rescreeningProfiles	Lista de perfiles para rescreening cuando saveForRescreening = true.	No	Array[String]
Objeto requestData			

Campo	Descripción	Requerido	Tipo/Formato
id	Identificador único del cliente.	Sí	String (20–200 caracteres)
type	Tipo de entidad a evaluar. Valores permitidos: individual, company, merchant, agent.	Sí	String (enum)
fullName	Nombre completo de la entidad o persona.	Sí	String (1–255 caracteres)
addresses	Lista de direcciones asociadas al cliente. Debe contener al menos un valor.	Sí	Array[String] (mínimo 1)
sex	Sexo (solo aplicable a individual o agent). Valores permitidos: m, M, f, F.	No	String
nationalities	Lista de nacionalidades en formato ISO 3166-1 alpha-2.	No	Array[String]
dateOfBirth	Fecha de nacimiento. Formatos permitidos: YYYY-MM-DD, YYYY o YYYY/YYYY.	No	String
placeOfBirth	País de nacimiento en formato ISO 3166-1 alpha-2.	No	String
identityDocuments	Lista de documentos de identidad. Cada objeto debe contener al menos el campo "number".	No	Array[Object]
bic	Código BIC (relevante para company). Longitud 8–11 caracteres.	No	String (8–11 caracteres)
datesOfRegistry	Fechas de registro (aplicable a company o merchant).	No	Array[String]
placesOfRegistry	Países de registro en formato ISO 3166-1 alpha-2 (company/merchant).	No	Array[String]
Objeto identityDocuments			
number	Número del documento de identidad.	Sí (si se envía el objeto)	number

***Validaciones**:*

1. Se deben mantener las mismas validaciones que se realizan de cara al proveedor aquellas validaciones que no pueden ser controladas por la capa intermedia es decir validaciones de negocio.

Ejemplo Individual Request:

```
{
  "country" : "GT/PA/NI",
  "coreId" : "1",
  "callbackMode" :"POLLING o CALLBACK",
  "requestId": "582d1c1c-57c8-496a-b6f4-17c8212c552a",
  "requestData": {
    "id": "0ac8ba6f-2ed2-453f-9073-20b8481f40ad",
    "type": "individual",
    "fullName": "John Doe",
    "identityDocuments": [
      {
        "number": 123456789
      }
    ],
    "nationalities": [
      "US"
    ],
    "addresses": [
      "New York, USA"
    ]
  },
  "profile": "DEFAULT",
  "saveForRescreening": true,
  "rescreeningProfiles": [
    "CUSTOM1",
    "CUSTOM2"
  ]
}
```

Ejemplo Company Request:

```
{
  "country" : "GT/PA/NI",
  "coreId" : "1",
  "callbackMode" :"POLLING o CALLBACK",
  "requestId": "myRequestId",
  "requestData": {
    "type": "company",
    "id": "id3456789012345678900",
    "addresses": [
      "North Pasdaran Street, Tehran, Iran"
```

```
    ],
    "fullName": "ANSAR BANK",
    "bic": "ANSBIRTH",
    "placesOfRegistry": [
      "IR"
    ],
    "datesOfRegistry": [
      "1990-01-01"
    ]
  }
}
```


1.2. Campos De Salida de la API

Campo	Descripción	Requerido	Tipo/Formato
Response 200 (CustomerCheck estructura base)			
result	Contenedor principal del resultado del screening	Sí	object
result.checkResult	Resultado del screening. Indica si existe coincidencia en listas	Sí	string (MATCH | NO_MATCH)
result.statusPollingUrl	URL para consultar el estado del caso (cuando aplica seguimiento o revisión manual)	Condicional (normalmente cuando MATCH)	string (URL)
result.matchResults	Lista de coincidencias encontradas	Solo si MATCH	array
matchResults (Solo cuando checkResult = MATCH)			
entityType	Tipo de entidad encontrada en la lista	Sí	string
score	Nivel de coincidencia (matching score)	Sí	string (decimal en texto, ej: "0.84")
list	Nombre de la lista donde se encontró la coincidencia	Sí	string
dateOfPublication	Fecha de publicación del registro en la lista	No	string (date-time ISO 8601)
dateOfUpload	Fecha en que la lista fue cargada en el motor de screening	No	string (date-time ISO 8601)

1.3. Campos De Salida de la API Escenario 1 – NO_MATCH status 200


```
{
  "result": {
    "checkResult": "NO_MATCH"
  }
}
```

1.4. Campos De Salida de la API Escenario 2 – MATCH status 200


```
{
  "result": {
    "checkResult": "MATCH",
    "statusPollingUrl": "https://api/status/123",
    "matchResults": [
      {
        "entityType": "INDIVIDUAL",
        "score": "0.84",
        "list": "INTERPOL",
        "dateOfPublication": "2023-03-20T22:44:36",
        "dateOfUpload": "2023-03-29T14:45:11.721"
      }
    ]
  }
}
```


Error Responses:

Http Status	Description
400	Invalid Request - the request contains validation errors.
401	Unauthorized Request
422	Request cannot be processed - entity type contains an inapplicable field.
500	Internal Server Error
503 Service Unavailable	503 Service Unavailable

Error Message:

Message	HTTP Status
Request ID does not conform, shall be in the range of 20-200 characters 400	400
Request ID value is already used 400	400
Invalid Entity Type, check possible entity type values 400	400
Full Name does not conform, shall be in the range of 1-255 characters 400	400
Gender is not applicable, shall not be provided if Entity Type is different from: Individual,	422
Dates of Birth are not applicable, shall not be provided if Entity Type is different from: Individual, Agent	422
Dates of Registry are not applicable, shall not be provided if Entity Type is different from: Organization, Merchant	422
Countries of Registry are not applicable, shall not be provided if Entity Type is different from: Organization, Merchant	422

Invalid Date, shall be a valid date value/format	422
Invalid Country, shall be a valid ISO 3166-1 Alpha-2 value	422

***Validaciones**:*

- Validar que los campos requeridos no estén vacíos
- Aplicar validaciones de acuerdo a mapeo en CUSTOMER-SCREENING- check y bulk.yml

1.5. Códigos de Error

1.6. Configuración de TimeOut

- Timeout operación: 60 segundos

1.7. Datos de Prueba

Nota: Los datos de prueba para cada Operación se compartirán en un archivo Anexo llamado SWAGGER - Datos de pruebas

1.8. Lógica Importante

Flujo Principal del Servicio (Explicarlo)

- CORE → AWS (solicitud)
    1) El CORE llama POST ficohsa/screening/customerCheck parametros requeridos
- AWS valida y aplica idempotencia
    1) Lambda lambda-screening-customercheck valida requestData (campos requeridos).
    2) Genera dedupeKey = hash(coreId + requestId+ requestData.id + type)
    3) guardar dedupeKey en ddb-screening-request-dedupe con condición if-not-exists (TTL 15–30 min).
        - ✓ Si ya existe: es un **retry** del CORE a AWS devuelve el mismo requestId y el estado que tenga.
        - ✓ Si no existe: continúa normal.
- AWS registra correlación y estado en BD o RDS (DynamoDb)
    - ✓ inserta/actualiza en ddb-screening-request-registry todo la información del request con un status = RECEIVED
    - ✓ flowType = Check
- AWS Envia request a ThetaRay (ver mapeo en CUSTOMER-SCREENING- check y bulk.yml)
- Thetaray responde de forma inmediata con la respuesta MATCH o NO MATCH (ver mapeo.yml)
- AWS guarda y responde al CORE PassThru: AWS actualiza ddb-screening-request-registry
    - ✓ status = SYNC_COMPLETED
    - ✓ screeningStatus = MATCH|NO_MATCH

- ✓ Guardar Response (solo si es necesario) dejar parámetro para A/D esta función

➢ Si hay Match se define el camino para la resolución de la alerta : (Polling vs Callback)

- ✓ Si screeningStatus != MATCH → termina.
- ✓ Si screeningStatus == MATCH continua al paso siguiente

4) (Polling)
   - ✓ El CORE NI empieza a consultar: investigationStatusExtended dentro de un lapso de 5 min

5) (callback)
   - ✓ El CORE no hace polling.
   - ✓ Espera a que ThetaRay mande: POST/screening/investigationStatusCallback
   - ✓ AWS recibe, dedupea (valida que no exista duplicado), guarda resolución y llama al CORE que este previamente parametrizado su callbackTarget

1.9. Datos Relevante

- Esta capacidad será consumida por Nicaragua (Polling) Guatemala (Callback).
- Se propone utilizar AWS Systems Manager Parameter Store para almacenar parámetros.
- API POST Thetaray : https://apps-pre-screening.ficohsa.thetaray.cloud/screening/customer/check

1.10. Detalles Técnicos de Conexión

Proveedor	Tipo conexión	Tipo aplicación
ThetaRay	HTTPS sobre Internet (TLS 1.2+)	POST API

1.11. Canal que utilizara la capacidad

Canal	Cloud/Onpremise	Observacioes
Abank GT	Cloud AWS	Parametrizar en configuración tema de Callback
COBIS NI	Cloud AWS	Parametrizar en configuración tema de Callback

1.12. Tablas de DynamoDB

```
1) ddb-screening-request-registry almacena lo de customer check y bulk y resolu-
ciones
PK: requestId (string)

Campos mínimos (requeridos)

1)requestId (string)
```

2)flowType (string enum: CHECK, BULK_ITEM)
3)country (string enum: NI, GT, PA)
4)coreId (string)
5)callbackMode (string enum: POLLING, CALLBACK)
6)requestDataFullName (String) viene de requestData.fullName
7)requestDataId (string) — viene de requestData.id
8)requestDataType (string) — individual/entity etc
9)requestDataprofile (string)
10)status (string enum: RECEIVED, SYNC_COMPLETED, RESOLVED, DELIVERED)
11)screeningStatus (string enum: MATCH, NO_MATCH)
12)createdAt (string ISO8601)
13)updatedAt (string ISO8601)
14)expiresAt (number epoch seconds) — TTL
15)latestResolution (string enum: Approve, Block)
16)resolvedAt (string ISO8601)
Campos para BULK (solo si flowType=BULK_ITEM)
17)bulkRequestId (string)
18)itemId(string)

status (operativo) tablas de control
RECEIVED - AWS recibió request del CORE, aún no llamó a ThetaRay
SYNC_COMPLETED - AWS ya tiene respuesta sync de ThetaRay (MATCH/NO_MATCH).
PENDING_REVIEW - hubo MATCH y está en revisión del oficial.
RESOLVED - ya existe decisión final.
DELIVERED . (si aplica) resolución entregada al core por callback (GT).

resolution
Approve
Block
null (cuando aún no está resuelto)

2) ddb-screening-request-dedupe (Idempotencia de entrada CORE a AWS)
PK: dedupeKey (string)

Campos mínimos (requeridos)
dedupeKey (string) --> Recomendado: = hash(coreId + requestId+ requestData.id + type)
requestId (string)
createdAt (string ISO8601)
expiresAt (number epoch seconds) — TTL 15–30 min

3) ddb-screening-callback-dedupe (Idempotencia de callback ThetaRay a AWS)

PK: callbackKey (string)

Campos mínimos (requeridos)

```
callbackKey (string) Recomendado: hast(businessMessageId+result)
businessMessageId (string)
result (string: Approve/Block)
comment (string) opcional la creacion
processedAt (string ISO8601)
expiresAt (number epoch seconds) — TTL 90 días
```