



DOCUMENTO TECNICO

VALIDACIÓN BIOMÉTRICA FACIAL

Versión 1

CONTENIDO

1. BIOMETRÍA FACIAL.....	3
1.1. PRODUCTO VERIFACE	4
1.2. PRODUCTO VERID	5
1.3. VERIFICACIÓN DATA BIOGRÁFICA.....	6
1.4. CAPACIDADES	7
1.5. COBERTURA CASOS DE USO.....	8
1.6. FLUJOS DE ONBOARDING FACIAL	10
1.7. FLUJOS DE AUTENTICACIÓN RECURRENTE FACIAL.....	11
1.8. CONDICIONES MÍNIMAS DE FUNCIONAMIENTO	11
1.9. MÉTODOS DE INTEGRACIÓN	13
1.10. PARAMETRIZACIÓN.....	13
1.11. DISEÑO DE INTEGRACIÓN.....	15
1.12. DESCRIPCIÓN DEL PROCESO.....	16
1.16. TRANSFERENCIA DE DATOS BACK ANTIFRAUDE	23
2. CONFIDENCIALIDAD.....	31
3. PROPIEDAD DE OLIMPIA IT.....	32

1. BIOMETRÍA FACIAL

Solución de Validación de identidad a través de biometría facial, que tiene la capacidad de realizar capturas a través de biometría, con el objetivo de validar la identidad de los clientes, evitando la captura de rostros falsos, algunos de los alcances de la solución son:

- **Verificación de presencia viva (Liveness):** Incluido en el producto VeriFACE, asegura que la persona que está realizando la validación es una persona real y no una falsificación o suplantación.
- **Verificación de Documentos de identidad (VerID):** Permite verificar los documentos de identidad presentados.

Adicionalmente, contamos con un diferencial de alto valor para nuestros clientes:

- **Central facial y de alertamiento del ecosistema Olimpia:** Manteniendo en colaboración con nuestros clientes y con la autorización de los ATDP, esta central permite agilizar los procesos, reduciendo tiempos y aumentando la seguridad que proveemos con nuestras soluciones.

Olimpia IT con la plataforma dispone una solución de biometría facial en la cual tiene diferentes componentes que robustecen la seguridad de la solución en nuestro producto de validación facial, integramos las soluciones de identificación a través de **integración API, SDK y WEB.**

La solución de validación de Identidad facial cuenta con la opción de consulta para diferentes tipos de documento como lo son: Cedula de ciudadanía, Cedula de extranjería, Pasaporte, PPT (Permiso por Protección Temporal) y PEP (Permiso Especial de Permanencia).

Nota: La solución de Biometría Facial asociada a la RNEC será suministrada por Olimpia IT una vez se habilite el procedimiento de certificación como operador biométrico Nivel 2, así como el acceso a las bases de consulta en producción, provistos por la Entidad (RNEC). Surtido lo anterior, Olimpia IT procederá a entregar las tarifas, previa determinación de las condiciones (costos) asociados a su habilitación como Operador Nivel 2.

1.1. PRODUCTO VERIFACE

Nuestro producto está diseñado para mitigar el riesgo de ataques de presentación en canales digitales con un apetito de riesgo alto, ya que son no asistidos o autogestionados a través de internet. Este producto cuenta con la acreditación iBETA 1 e iBETA 2, lo que respalda su cumplimiento con altos estándares internacionales de seguridad y fiabilidad.

Igualmente mejora la experiencia de usuario y la conversión de clientes, ya que, facilita el acceso a productos y servicios a través de un flujo simple similar a la captura de una selfie y facilitando la autogestión y la multicanalidad de la plataforma y la gestión asistida en oficina.



Para realizar este proceso de consulta y cotejo facial se debe tener en cuenta las siguientes consideraciones.

- En atención a la normatividad de Protección de Datos Personales, se aclara que cada cliente debe firmar un ATDP (Autorización Tratamiento Datos Personales) al momento de iniciar el proceso, que deberá incluir la autorización para la validación de su identidad, así como la consulta en bases de datos biométricas públicas o privadas disponibles para la corroboración de su identidad.
- Cada aprobación se da por una única vez y ésta debe realizarse cuantas veces el cliente realice el proceso con nuestros servicios. Por tanto, cada proceso debe contar con su ATDP único. Así mismo, todo tratamiento de datos personales se regirá por la Ley 1581 de 2012, sus decretos reglamentarios y la regulación que sobre la materia se expida.

Si el cliente NO brinda su autorización para la consulta, el proceso no se podrá llevar a cabo, así se cuente con la información.

1.2. PRODUCTO VERID

Producto que mitiga el riesgo de ataques de posibles suplantaciones de identidad basados en presentación de documentos falsificados en canales digitales.



Importante: Para validación de documentos diferentes a la cédula de ciudadanía colombiana, integramos tecnología de proveedores de clase mundial con altos estándares de calidad y cobertura.¹

1.3. VERIFICACIÓN DATA BIOGRÁFICA

Es un servicio de validación del documento de identidad que cuenta con la validez jurídica requerida por la legislación colombiana para llevar acabo un modelo de consulta a la base de datos de la RNEC – (Data biográfica). Olimpia IT ha desarrollado un modelo de validación partiendo del número de identidad y la fecha de expedición de la cédula de un ciudadano colombiano mayor de edad.

La consulta de Onboarding – Data Biográfica se realiza a través de un Servicio Web publicado por Olimpia IT desde el cual y a petición del cliente, se envían los

¹ Es importante analizar la cantidad de transacciones estimadas que involucran documentos diferentes a la cédula de ciudadanía colombiana, ya que esto requiere una integración y valoración específica según el caso de uso.

números de cédulas de ciudadanía colombianas y de esta manera hará la consulta a la base de datos dispuesta.

1.4.CAPACIDADES

AUTENTICACIÓN BIOMETRÍA FACIAL

Tipo	Detalle	Propio	Integrado
Facial	Captura en vivo: Android / iOS / componente web	X	
	-Liveness activo tipo selfie (para Android / iOS) iBeta 1 y 2		
	-Liveness activo tipo selfie web (multiplataforma) pendiente iBeta 2		
	-Liveness activo multiplataforma (retos de movimientos) iBeta 1		
Fuente de confianza	Central Facial Olimpia / Rostro de documento / foto referencia externa	X	X
	Matcher acreditado NIST 1;1 y 1;N		
Tipo de integración	Formulario Web (Webvalidador) / componente web/ SDK / API	X	
Consola	Gestión de parametrización de convenios (Aspecto UX, flujo de validación, umbrales)	X	
	Gestión administrativa: Revisión de transacciones y reportes	X	
	Envío de URL del proceso : SMS /email o whatsapp		X

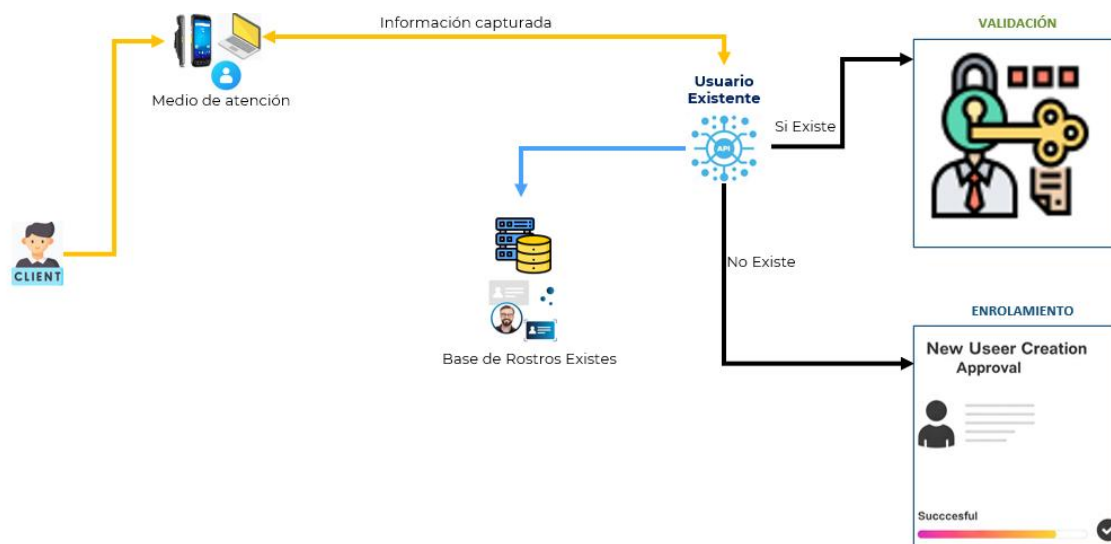
VERIFICACIÓN DOCUMENTO DE IDENTIDAD

Tipo	detalle	Propio	Integrado
Verificación y registro de Doc Identidad	Captura en vivo de imagen de documento: Android / iOS / API / componente web	X	
	-Mayor calidad y seguridad		
	-Auto recorte		
	-No permite API		
	Cargue de imagen de documento almacenada: Android / iOS / API / componente web		
	-Riesgo ante adulteración digital		
	-Cargue API	X	X
	OCR (SDK con mejor calidad de captura y feedback / En web tiene captura limitada)		
	- Extracción imágenes textos, fechas y números		
	- Extracción de fotografía		
	- Extracción de Barcode (PDF417 /MRZ)		
	- Verificación estructura del documento		
	- Verificación de calidad chequeo iluminación y calidad		
	Registro en Central facial (enrolamiento de data)	X	
	-Fotografía rostro de documento		
	-Fotografía de documento (front / back)		
	-Información Biográfica desde el documento		
Consola web	Puede incluir el paso en el flujo de convenio para onboarding o para autenticación	X	

CAPACIDAD VERIFICACIÓN FUENTES DE DATOS

Tipo	Detalle	Propio	Integrado
Data biográfica RNEC (CC)	Verificación estado de cédula colombiana ANI – (Verificación no suministro de data)		X
	ESTADO (Vigente vigente con novedad Cancelado Pendiente)		
Data biográfica (CE.PPT,CE)	Consulta de data y vigencia documentos colombianos diferentes a CC		X
	CE: Cédula de extranjería		
	PAS: pasaporte		
	PPT: Permisos de Protección temporal		
Confirmación OTP	Envío y confirmación de OTP (One Time Password) en canales suministrados (SMS / Mail / WhatsApp)		X
PSD	Preguntas sociodemográfica de comportamiento financiero & comercial		X
	(BURO)		

1.5.COBERTURA CASOS DE USO



El proceso de validación facial dependiendo del modelo de operación estará integrado en el flujo de negocio del cliente y en el momento que sea invocado nuestro servicio, este inicia el proceso de validación facial.

El proceso incluye las siguientes actividades:

- Datos de entrada del usuario consumidor.
- Recepción de un mensaje de texto SMS y en simultaneo un correo electrónico con el link.
- También se puede configurar la plataforma para que el link se reciba por WhatsApp para seguir el proceso de validación de identidad.
- En caso de que el dispositivo no permita el acceso a la cámara o no cuente con la misma, el sistema le permitirá redirigen su experiencia hacia otro dispositivo móvil mediante el escaneo de un código QR.

*El texto que se recibe en la notificación (SMS/correo electrónico/WhatsApp) y el look & feel es personalizable.

Cuando el cliente consumidor reciba esta notificación podrá realizar el proceso desde cualquier dispositivo tecnológico entiéndase por móvil Android/iOS o PC Windows/MAC.

- Mensaje informático y ATDP (Autorización del Tratamiento de Datos Personales), si el usuario consumidor no señala este **Check** no podrá continuar con el proceso dado que es una medida obligatoria para proteger la integridad del proceso de validación de identidad.
- El cliente consumidor deberá superar las indicaciones que la plataforma le indique para validar su identidad.
- El cliente consumidor procederá a escanear los documentos; una vez subidos, la plataforma realizará el análisis de los datos.
- Al final del proceso se tendrá un resultado de **Aprobado** o **Rechazado** sobre el cual ahora el cliente procederá a continuar con el proceso del flujo de negocio.

Nota:

- El proceso descrito en este apartado es solo un ejemplo, la cantidad de validaciones depende de la configuración de componentes que se asocien al caso de uso.

A continuación, se describen los flujos posibles de OnBoarding y autenticación.

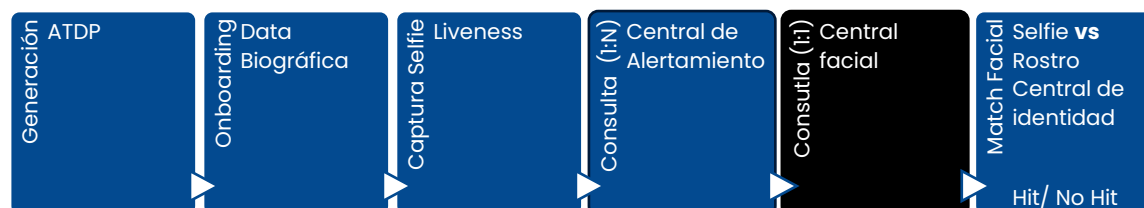
1.6. FLUJOS DE ONBOARDING FACIAL

OnBoarding con verificación en central de alertamiento para reducir riesgo a través de alertamiento facial del ecosistema Olimpia. Aumenta la seguridad d con alertas en coincidencias al rostro de la selfie en vivo.



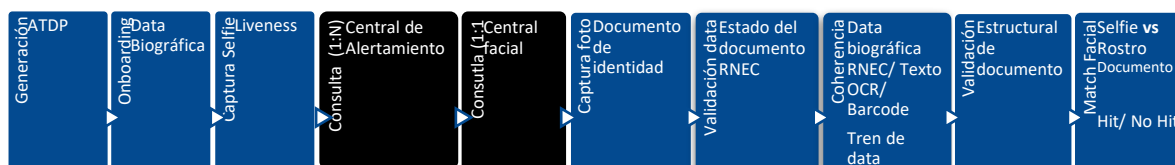
Flujo Onboarding con alertamiento.

OnBoarding con verificación en central facial, búsqueda en la central facial del ecosistema Olimpia para agilizar el proceso de onBoarding y reducir la solicitud de la captura de documento. Reduce los pasos y aumenta la rapidez.



Flujo OnBoarding con central facial.

OnBoarding Match facial versus Documento VeriFACE + VerID, onBoarding de alta seguridad que incluye los diferenciales del ecosistema Olimpia, central de alertamiento 1:N, central facial, Liveness tipo selfie, estado del documento RNEC y verificación de coherencia de data biográfica de documento capturado.



Flujo OnBoarding VeriFACE + VerID.

1.7. FLUJOS DE AUTENTICACIÓN RECURRENTE FACIAL

La autenticación recurrente con los diferenciadores de Olimpia, como la central facial y el sistema de alertamiento, es una solución que ofrece un alto nivel de seguridad y agilidad en las operaciones y procesos digitales. Esta solución está diseñada específicamente para entornos con un apetito de riesgo alto y en los que los usuarios consumidores ya están enrolados, proporcionando una autenticación continua y robusta que facilita la protección y la eficiencia en los procesos digitales.



Flujo Autenticación recurrente VeriFACE y estado de documento.

1.8. CONDICIONES MÍNIMAS DE FUNCIONAMIENTO

Condiciones de escena para la captura

- Luz natural o iluminación que permita ver detalles del rostro (> 300 lux – aprox.).
- No uso de accesorios como gafas, pasamontañas, tapabocas entre otros objetos o accesorios que bloquen la captura de estos detalles del rostro como: distancia pupilar, raíz, labios u otros puntos de la biometría del rostro.
- Fuente de luz principal hacia el rostro (evitando luz trasera Backligh) que generan sombras que pueden afectar la captura.
 - **Para la captura del documento (especialmente cédula de ciudadanía colombiana)**
- No usar flash o luces artificiales que puedan generar brillos que eviten su lectura.
- Usar una superficie estable para colocar el documento mientras realiza la captura.
- Evitar recortes.

Dispositivo de captura:

- Cámara de 2 Mpx. con una resolución de fotografía de 1080p.
- Para SDK nativo
- Android versión vigente (para 2024 la vigente más antigua vigente es la versión 10) aproximadamente con 3 años de antigüedad.
- iOS versión 14 (Desde el 2020) aproximadamente con 3 años de antigüedad.

Calidad de imagen

La baja calidad de la imagen capturada, recortes, desenfoques, múltiples rostros, capturas de documentos diferentes a los solicitados entre otros criterios que afecten las características de extracción de biometría del rostro o las validaciones del documento podrían ser causal de rechazo.

1.9. MÉTODOS DE INTEGRACIÓN

Estos flujos de la solución de biometría facial de Olimpia están disponibles para ser integrados de acuerdo con las necesidades y capacidades de integración del cliente a través de 3 métodos:

Integración por Componente web

- Integración generica (marca blanca)
- Personalización Básica (paramétrica)
- Requiere poco desarrollo
- Implementación rápida (acompañamiento inicial entre 20 y 40 horas)

Integración vía API

- Flexibilidad en frontend a cargo del Cliente
- Alta personalización
- Requiere desarrollo (tecnología web)
- Tiempo de implementación medio (acompañamiento < 80 horas)

Integración por SDK

- Flexibilidad en frontend a cargo del Cliente
- Alta personalización a cargo del cliente
- Cada actualización requiere desarrollo (tecnologías movil nativas Android y iOS)
- Tiempo de implementación medio (acompañamiento < 80 horas)

1.10. PARAMETRIZACIÓN

Los servicios del portafolio tanto de los productos de VeriD como de VeriFACE tienen opciones de parametrización para su adaptación a los casos de uso y los flujos definidos para la situación actual del cliente.

Esta parametrización es llevada a cabo en el momento de la implementación a través del equipo de Delivery de Olimpia y validada durante el proceso de entrega.

La configuración incluye el alistamiento de parámetros del caso de uso, según el apetito de riesgo de las transacciones por tipología del cliente-consumidor, líneas de negocio con superficies de riesgo homogéneas (umbrales iguales aceptación de score de riesgo), las cuales son parametrizadas como convenios y subcategorías del cliente entidad.

La parametrización de estos convenios depende del método de integración y están enfocadas en balancear la exigencia del sistema en cuanto seguridad, facilidad y cantidad de pasos.

La parametrización puede incluir de forma limitada:

- Color Interfaz gráfica, botones.
- Mensajes principales (que no afectan los criterios acreditados).
- Umbrales de score de riesgo para definir acidez o permisividad de la prueba facial o umbral de zona gris para el desbordamiento a validación manual.
- Flujos, pasos y secuencia.
- Número de intentos permitidos.
- Inclusión de servicios complementarios de seguridad:
 - Central facial
 - Central de alertamiento
 - Back antifraude

Notas importantes:

Esta parametrización es limitada dado que algunos criterios son de uso exclusivo de la solución, por ejemplo: pasos requeridos en secuencia, tiempos de transacción, rechazo automático, textos relacionados con seguridad, fondos que apoyan la iluminación del rostro, o logos de propiedad, entre otros.

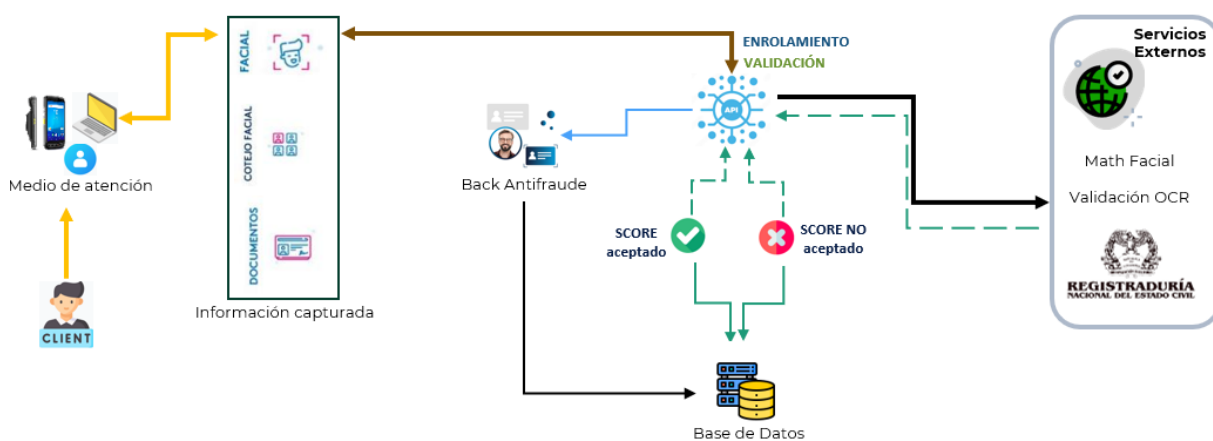
La modificación de criterio de seguridad como umbrales de aprobación requiere una aprobación y responsabilidad por parte del cliente según el apetito de riesgo

de cada caso de uso o parametrización de convenio, algunos de estos umbrales y flujos pueden no permitir que se definan umbrales menores a los mínimos, por lo tanto, existe una corresponsabilidad que debe ser acordada entre las partes para garantizar niveles de usabilidad y seguridad acorde con las necesidades del cliente y del producto.

El análisis estructural y la coherencia de los textos del documento son procedimientos altamente dependientes de la calidad de la imagen, al igual que la calidad del rostro de referencia extraído del documento, por lo tanto, es importante tener en cuenta que el procedimiento no constituye una técnica infalible para detectar documentos que puedan tener posibles alteraciones, desgaste o dificultades de procesamiento, lectura de caracteres y códigos de barras por parte del sistema o ante baja calidad de la imagen.

1.11. DISEÑO DE INTEGRACIÓN

Basados en la necesidad del cliente proponemos el siguiente diseño técnico y funcional de la solución, integración vía API o SDK; sin embargo, estamos prestos a los ajustes que se deban realizar. Esta arquitectura se debe revisar entre las partes para su integración e implementación.



2 Diseño de Integración

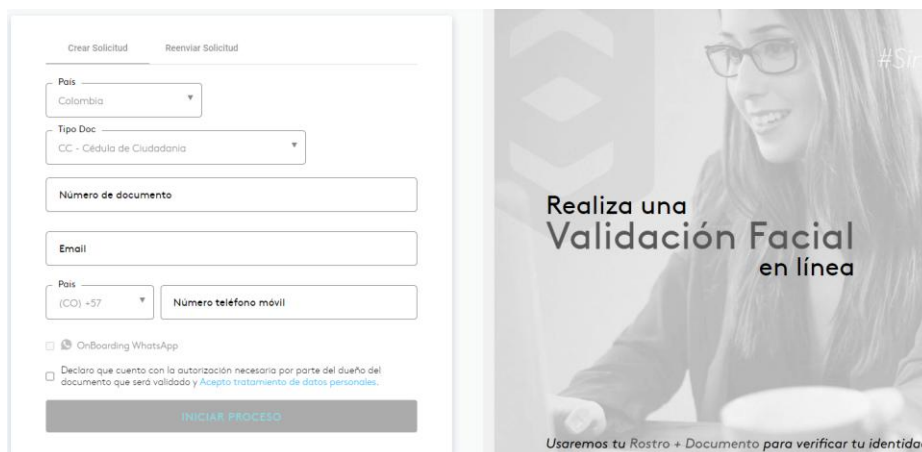
Cada validación genera un % de score de coincidencia parametrizable y el estado del documento.

1.12. DESCRIPCIÓN DEL PROCESO

El proceso de validación está integrado en el flujo de negocio del cliente y en el momento que sea invocado nuestro servicio, este inicia el proceso de validación facial.

Se solicitan los datos de entrada de:

- Tipo de documento
- Numero de documento
- Correo electrónico
- Número de teléfono de Celular



Luego, el cliente recibe un mensaje de texto SMS y en simultaneo un correo electrónico con el link y también se puede configurar la plataforma para que el link llegue por WhatsApp para seguir el proceso de validación de identidad, en caso de que el dispositivo no permita el acceso a la cámara o no cuente con la

misma, el sistema le permitirá redirigen su experiencia hacia otro dispositivo móvil mediante el escaneo de un código QR.



***Texto modificable y personalizable**

Cuando el cliente reciba esta notificación podrá realizar el proceso desde cualquier dispositivo tecnológico entiéndase por móvil Android/iOS o PC Windows/MAC, en el cual procederá a realizar los retos faciales para validar la identidad evitando suplantaciones.

Mensaje informático y ATDP (Aceptación del Tratamiento de Datos Personales), si el usuario no señala este check no podrá continuar con el proceso dado que es una medida obligatoria para proteger la integridad del proceso de validación de identidad.

Información personal

Diligencia tu información personal.

País

Selecciona tu país



Tipo de documento

Número de Documento

Tipo



1130628231



He leído y acepto la **Autorización de Tratamiento de Datos Personales**

Prepara tu rostro para una
fotografía.



Recomendaciones

- ✓ Encuentra un lugar iluminado.
- ✓ Ubica tu cara dentro del marco.
- ✗ No cubras tu rostro con accesorios.

¡Gracias! Por aceptar los permisos
solicitados para verificar tu identi...



**No cubras tu cabeza
con accesorios**



Procesando solicitud

Procesando solicitud de validación



Tu rostro es real

Hemos validado que tu rostro es verdadero



Nota: imagen de muestra



Tu rostro es real

Hemos validado que tu rostro es verdadero

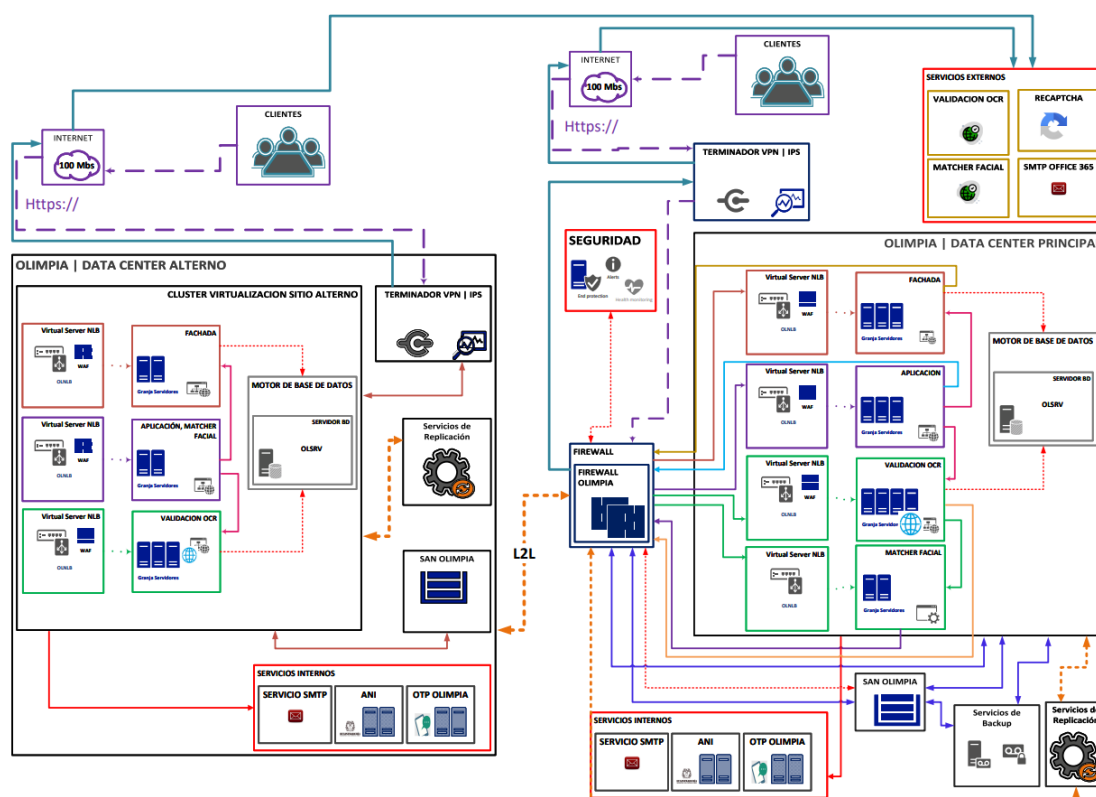
Al final del proceso se tendrá un resultado de **Aprobado** o **Rechazado** sobre el cual ahora **el cliente** procederá a continuar con el proceso del flujo de negocio.

<div>ANTECEDENTES</div> <ul style="list-style-type: none"> Consultas Reporte Consumo Historial de Consultas Consulta Batch Disponibilidad Fuentes <div>GESTIÓN</div> <ul style="list-style-type: none"> Empresas Convenios Usuarios Facturación Reporte de Riesgo Países 	Detalle del proceso Logs Trx Facial Documento Cross check doc 1 Cross check doc 2 Cross Check Facial ATDP							
	ID PROCESO		4e66983f-d378-4284-bfe9-c3818cd90b53					
	PAÍS		Colombia					
	TIPO DOCUMENTO		CC					
	NÚMERO DOCUMENTO		072551771					
	NOMBRE DEL CIUDADANO		JAIME ANDRES MEZA PUENTE					
	TELÉFONO		573178880271					
	CORREO		JAIME.MEZA@OLIMPIAIT.COM					
	USUARIO		jair.yepes - OLIMPIAIT-					
	TIPO PROCESO		VALIDACIÓN					
	FECHA DE CREACIÓN		feb. 13, 2024, 3:40:45 p. m.					
	EN CENTRAL FACIAL		SI					
	RESULTADO		APROBADO					
	ESTADO ANI		Vigente					

Nota: El proceso descrito en este apartado es solo un ejemplo, la cantidad de validaciones depende la configuración de componentes que se asocien al caso de uso.

1.13. ARQUITECTURA

La solución cuenta con una arquitectura híbrida. A continuación, los componentes de red del ecosistema del servicio y sus dependencias que incluye, tráfico de red, infraestructura, base de datos, equipos de seguridad perimetral, plataformas SOC y conexión con terceras partes.



Los **Tiempos Medios de Respuesta – TMO** para este servicio se estiman entre 1,5 segundos y 12 segundos, sin embargo, se debe contemplar la cantidad de componentes de validación configurados para el proceso, lo anterior debido a que se puede realizar la integración de servicios con terceros y también está sujeto a la latencia que se pueda presentar en los sistemas de comunicación y seguridad.

1.14. EVOLUCIÓN Y MEJORAS

Detección de cámaras virtuales y videos generados con IA: Nuestros componentes de liveness facial se están entrenando y mejorando en la detección de este tipo de escenarios, optimizando la detección de diferentes tipos de nuevas tecnologías o escenarios de vulneración con componentes de

profundidad, saturación, movimiento y otros modelos de machine learning con el fin de mejorar el liveness.

Liveness iBeta: Aunque nuestro producto ya incluye la detección de máscaras 2D, máscaras 3D, videos en pantalla, entre otros. Nos encontramos en proceso de acreditación internacional por un laboratorio autorizado por la **NIST en iBeta 1 e iBeta 2** para nuestro algoritmo “liveness activo y pasivo” desarrollado en Olimpia y entrenado con IA. Esto nos permitirá mejorar los procesos de entrenamiento en un algoritmo propio de IA que facilite la identificación de rostros de la región haciendo el modelo más cercano a la realidad del mercado colombiano y de la región.

Validación Mejorada en Cedula de Ciudadanía colombiana: Estamos reentrenando nuestros algoritmos de validación de documentos con los documentos emitidos en Colombia para mejorar las métricas de éxito y detección de manipulaciones, basados en los escenarios identificados por nuestro equipo de dactiloscopia se realizan escenarios de identificación de patrones basados en la cedula holográfica y cedula digital para optimizar la identificación de documentos falsos y documentos legítimos.

Detección de suplantadores: en los modelos de co-creacion con los clientes se plantean escenarios para la identificación de posibles suplantadores y victimas de fraude que pueden ser detectados por otros clientes creando un entorno 360 de seguridad con el apoyo e insumo de nuestros clientes para alimentar la información de los intentos realizados y marcado en listas negras para poder tener alertamiento proactivo de intentos de suplantación por medio de la biometría facial.

Homologación ante la RNEC como OAID Nivel 2 (Operador Facial): Ya estamos preparados técnica y organizacionalmente para ser un operador biométrico

facial de la RNEC, de tal forma que tan pronto salgan los requerimientos definitivos lograremos la certificación y así podremos ofrecer esta funcionalidad de forma inmediata.

1.15. IMPLEMENTACIÓN DEL SERVICIO

A continuación, se describen las etapas del proceso de implementación, los tiempos estimados podrán variar de acuerdo con el cumplimiento de las actividades por las partes; la complejidad y alcance de las integraciones .



El alta del servicio se estimará en conjunto con la entidad, teniendo en cuenta el cronograma que se establezca según los recursos técnicos que la entidad disponga.

A continuación, se presentan los hitos a alto nivel para el proceso de implementación e integración.

<div>      </div>					
Etapa	Firma Contrato	Kick Off	Habilitación Inicial	Marcha Blanca	Entrega a la Operación
Tiempo	5 a 10 días	1 día	5 a 20 días	15 días	
Equipo	Comercial Team	Delivery Team	Delivery Team	Delivery Team	Customer Service Team
Actividades	Firma & legalización del contrato	Reunión de Inicio de la Implementación con cliente Definición del alcance e Identificación de las posibles personalizaciones Identificación de riesgos & factores de éxito Definir fechas reuniones de capacitación técnica y de realización Definición de canales de comunicación	Creación y entrega de credenciales del servicio a implementar Entrega de documentación técnica y funcional del servicio Capacitación técnica y funcional del servicio Entrega de Desarrollos Requeridos (Si Aplica) Realización y definición Seguimiento Periódico Firma Acta Finalización Implementación	Acompañamiento y estabilización en ambiente productivo	Inicio de consumo de servicio
Entregables	Contrato Firmado	Presentación Kick Off actualizada	Credenciales accesos ambientes preproductivo y productivo Manuales / Documentación Técnica Entrega Acta Finalización	Presentación de canales de servicio al cliente (ANS) - Modelo Operativo	Prestación del Servicio

Nota: El tiempo total de la implementación este sujeto al tiempo de desarrollo del Cliente.

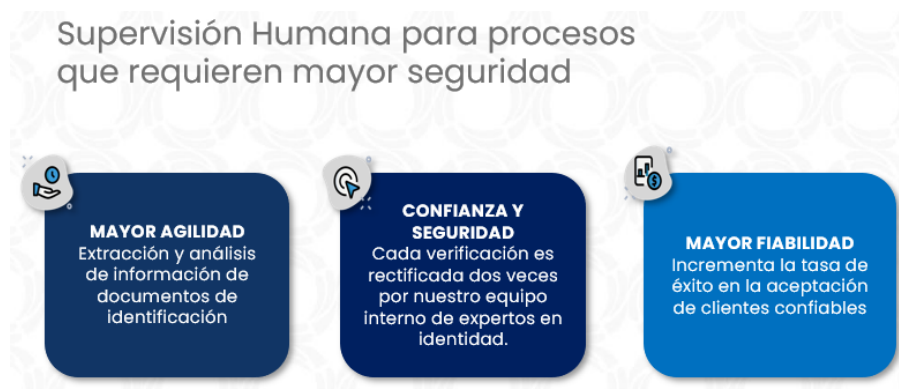
Según el dimensionamiento Olimpia IT apoyará en las siguientes actividades.

1. Planeación.
2. Preparación Técnica ambiente preproducción.
3. Manual técnico.
4. Acompañamiento estabilización de la aplicación.
5. Seguimiento y control.

1.16. TRANSFERENCIA DE DATOS BACK ANTIFRAUDE (VERIFICACIÓN MANUAL – JUICIO DE EXPERTO)

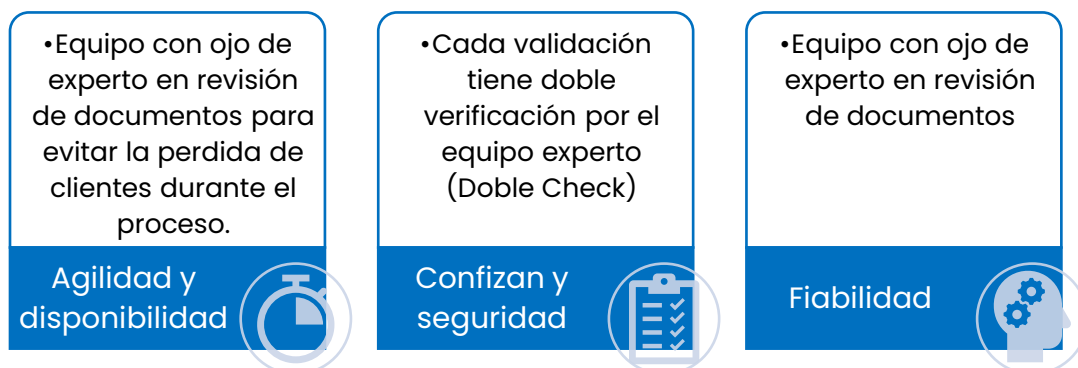
Este servicio complementa el proceso de validación facial y de documento de forma automática que realizan los productos VeriFACE y VerID, para los casos en los que se acuerde un umbral de no decisión automática de Rechazo y se requiera un juicio de experto para Aprobar o Rechazar la validación de identidad.

El proceso de verificación incluye todas las reglas y validaciones de VerID para la cédula de ciudadanía colombiana tanto amarilla como blanca (nueva cédula digital) más el Match del rostro contra central facial y de alertamiento Olimpia, pero con el criterio del experto.



Este juicio de experto genera un alto valor por:

- ❶ **Reduce el impacto en el rechazo** por seguridad y precisión cuando la calidad del documento capturado y la fotografía selfie o de central facial, no haya dado un umbral de comparación aceptable para Aprobar, pero no es tan bajo para Rechazo automático (dada la complejidad de lectura de la cédula de ciudadanía colombiana y sus hologramas).
- ❷ **Capacidad y escalabilidad**, este servicio tiene un grupo de expertos que atienden en horario de servicio según dimensionamiento de transacciones estimadas que les solicite verificar para Aprobar o Rechazar. Es importante que desbordes atípicos sean acordados entre las partes, dado que es un proceso manual y altamente susceptible al volumen y horario de atención de las transacciones solicitadas.
- ❸ **Rechazo como criterio de seguridad**, para no afectar los tipos de la validación, este servicio tiene un tiempo límite para su análisis por parte de cada experto y, posterior a este, por seguridad, la transacción pasa a un Rechazo de forma automática (dado que no aprobó el umbral aceptado por VerID).



Hitos proceso Back Antifraude

- Ofrecemos un servicio de verificación de identidad en el que un equipo de profesionales especializados en este campo realiza un análisis técnico de las imágenes proporcionadas.
- Este servicio se ofrece como un apoyo al flujo de seguridad de cada cliente, garantizando la integridad de sus procesos a través de **APKY WEB**.
- Al finalizar la revisión se dará una respuesta ya sea satisfactoria y rechazada por alguna de las razones que tenemos enumeradas en nuestra plataforma.
- Contamos con un procedimiento para realizar las actividades y gestión de la validación Back Antifraude **“VERIFICACIÓN DE IDENTIDAD BIOMÉTRICA MANUAL”**.

Objetivo

Verificar la plena identidad de las personas de forma manual, mediante el análisis de los elementos recolectados en el momento del registro en la plataforma tecnológica, que por alguna razón no pudieron ser identificados por software.

Alcance

Inicia con la recepción de la solicitud de verificación de identidad biométrica manual y va hasta la emisión del concepto, ya sea favorable o no favorable.

Notas:

- Este es un **servicio opcional** que permite continuar aquellas validaciones que por motivos externos a la aplicación no permite culminar la validación o no cumple con los umbrales para aprobarla o rechazarla a través del algoritmo. (baja resolución de las fotos, contra luz, iluminación en el documento, baja conexión internet, información incorrecta en el momento de diligenciar).
- Si las transacciones por temas ajenos al servicio se van a back las mismas serán cobradas como una transacción adicional
- Las modificaciones que solicite la cliente después implementada la solución tendrán un costo adicional, servicios profesionales/hora de desarrollo.
- Contamos con un procedimiento para realizar las actividades y gestión de la validación Back Antifraude **“VERIFICACIÓN DE IDENTIDAD BIOMÉTRICA MANUAL”**. De ser requerido, se presentará el documento en una sesión de trabajo con el cliente, por tratarse de información confidencial para nuestra organización.
- Este proceso puede ser aplicado para los servicios de biometría de huellas y facial.

1.17. DESCRIPCIÓN DEL PROCESO

1	✓	RECEPCION DEL CASO A VERIFICAR
2	✓	ANALIZAR FOTOGRAFIAS
3	✓	COMPROBAR AUTENTICIDAD DEL DOCUMENTO
4	✓	CALIFICACIÓN DEL PROCESO

A continuación, la descripción de las actividades realizadas durante el proceso de validación con el back antifraude.

Realizar requerimiento

El requerimiento se realiza automáticamente por el aplicativo cuando no existe match en las aplicaciones de biometría, basados en los siguientes parámetros.

- **No Registro Facial:** Se realiza cuando no se cuenta en las BD's con el registro facial del ciudadano a validar.

Recibir requerimiento

Recibir requerimiento de acuerdo con la generación automática del aplicativo o la solicitud a la mesa de servicios cuando la verificación de identidad manual ha sido aplazada, por no contar con información suficiente para finalizar la verificación.

Abrir requerimiento y verificar identidad

Abrir requerimiento y realizar verificación de identidad de acuerdo con los criterios definidos como:

Fotografía en tiempo real o Rostro Vivo, análisis del documento, comparación de las impresiones dactilares (Documento de identificación Vs Huella latente capturada), validación de la información biográfica del documento con la ingresada, validar otras fuentes.

Emitir concepto

Emitir concepto de verificación de identidad biométrica manual de acuerdo con los siguientes criterios:

- **Aprobado:** Cumple con los requisitos.
- **Rechazado:** Implica que el enrolado defina un nuevo enrolamiento y se ajuste de acuerdo con la causal del rechazo.
- **Aplazado:** No se da concepto final, se solicita algún requerimiento adicional.

El estado **Aplazado**, debe ser definido en la etapa de implementación, dado que conviene solicitar algún documento adicional para apoyar la identificación.

Notificar al Cliente

Notificar al Cliente el concepto dado a la verificación de identidad manual del enrolado.

Una vez realizado el concepto, el sistema de dactiloscopia cierra el proceso.

Nota: en caso de que el cliente requiera ampliar la información acerca del requerimiento se comunicará en primera instancia con la mesa de servicios y en caso de no encontrar solución al requerimiento, la mesa de servicios consultara a la Dirección de Investigaciones (Gestor de Verificación de Identidad).

A continuación, se describen las etapas del proceso de implementación, los tiempos estimados podrán variar de acuerdo con el cumplimiento de las actividades por las partes, a la complejidad y alcance de las integraciones , así como de las personalizaciones contratadas .



El alta del servicio se estimará en conjunto con la entidad, teniendo en cuenta el cronograma que se ha establecido según los recursos técnicos que la entidad disponga. A continuación, se presentan los hitos a alto nivel para el proceso de implementación e integración.

Etapa	Firma Contrato	Kick Off	Implementación	Pruebas & Afinamiento	Marcha Blanca (Transición)	Inicio de operación
Tiempo	5 a 10 días	1 día	5 a 60 días	5 a 15 días	15 días	
Equipo	Comercial Team	Delivery Team	Delivery Team	Delivery Team	Delivery Team	Customer Service Team
Actividades	Elaboración del contrato. Revisión del contrato por las partes. Firma y legalización del contrato.	Alta del servicio Reunión de inicio de la implementación. Definición del alcance e identificación de posibles desarrollos requeridos. Identificación de riesgos y factores de éxito.	Creación y entrega de credenciales del servicio que desea implementar. Entrega de documentación técnica del servicio. Socialización/capacitación técnica sobre los métodos del servicio. Entrega de desarrollos requeridos (si aplica).	Acompañamiento telefónico y por correo al cliente sobre dudas o inquietudes en el consumo/ integración del servicio Reuniones de seguimiento con el cliente	Acompañamiento	Inicio del consumo del servicio
Entregables	Contrato firmado	Reunión de Kick Off.	Credenciales Manuales / Documentación técnica	Reuniones por Teams Correos de seguimiento	Presentación de canales de servicio al cliente	Prestación del servicio

Nota: EL tiempo total de la implementación este sujeto al tiempo de desarrollo del Cliente.

Según el dimensionamiento Olimpia IT apoyará en las siguientes actividades.

1. Planeación.
2. Preparación Técnica.
3. Acompañamiento estabilización de la aplicación.
- 4.** Seguimiento y control.

2. CONFIDENCIALIDAD

El contenido de la presente propuesta, incluyendo todas las tarifas, valores, términos y condiciones estipulados, se considera de carácter confidencial. La información aquí contenida solo será divulgada a las personas asignadas por el Cliente para la evaluación de la propuesta, y no podrá ser utilizada total o parcialmente para propósitos distintos al objeto de esta propuesta sin el consentimiento explícito de Olimpia.

3. PROPIEDAD DE OLIMPIA IT

El presente documento es de carácter **confidencial** y está protegido por las normas de derechos de autor, cualquier reproducción, distribución o modificación total o parcial a usuarios no autorizados o cualquier uso indebido de la información confidencial será considerado un delito conforme a lo establecido por el Código Penal y Leyes vigentes del estado colombiano.

