

CONFIDENCIAL

**Selección de la Entidad de Referencia de Portabilidad
Numérica Móvil en Costa Rica**

PROPUESTA

Sección 05. Módulo Opcional de Validación Biométrica con Prueba de Vida

p.p. Daniel Alejandri Cerón
Representante Autorizado
Mediafon Datapro, UAB

Oferente: MEDIAFON DATAPRO, UAB
Vilna, Lituania | 2026

Contenido

1. Módulo Opcional de Validación Biométrica – Propuesta Técnica.....	3
1.1. Naturaleza, Alcance y Modelo de Contratación	3
1.2. Modalidad Biométrica y Estándares Aplicables.....	4
1.3. Comportamiento Funcional del Servicio	4
1.4. Especificaciones de Captura del Retrato (Selfie).....	6
1.4.1. Formato de la Fotografía.....	7
1.4.2. Calidad de la Fotografía.....	7
1.4.3. Posición del Rostro Respecto a la Cámara.....	7
1.4.4. Posición y Apariencia Facial	7
1.4.5. Dirección y Visibilidad de los Ojos	8
1.4.6. Brillo y Contraste	8
1.4.7. Iluminación.....	8
1.4.8. Anteojos.....	8
1.4.9. Cobertura de la Cabeza.....	8
1.4.10. Accesorios Faciales	9
1.4.11. Dimensiones del Retrato y Ubicación de la Cabeza	9
1.5. Calidad de Imagen del Documento de Identidad	9
1.6. Obligaciones de Reporte	10
Anexo 1. Tabla de Cumplimiento Sección 8 del Pliego ERP.....	11

1. Módulo Opcional de Validación Biométrica – Propuesta Técnica

1.1. Naturaleza, Alcance y Modelo de Contratación

La solución Numlex™ SIPN propuesta incluye un módulo opcional de validación biométrica que permite que dicho proceso realice de forma totalmente remota, no presencial, ejecutada en su totalidad a través del dispositivo del usuario final, sin requerir hardware dedicado ni terminales propietarias. El módulo es integrable mediante SDK nativo (Android / iOS), SDK híbrido (Cordova, React Native, React Native Light), SDK Web JavaScript o API REST, y puede desplegarse on-premise (Docker) o como SaaS en la nube Microsoft Azure de VU.

La plataforma combina reconocimiento facial pasivo con verificación pasiva de prueba de vida, contando con certificación iBeta PAD Level 2 conforme a ISO/IEC 30107-3. Se incorporan múltiples capas nativas contra el fraude y la suplantación: un servicio de antispoofing facial basado en modelos de Machine Learning entrenados para detectar prints, máscaras 3D, fakes, videos, malware y ataques man-in-the-middle; un modelo de Deepfake Detection on-demand desplegado como capa de seguridad adicional dentro del flujo de verificación de identidad; lógica de Replay Attempt que descarta validaciones cuyo score de comparación biométrica sea exactamente 100% (indicador de comparación de una imagen consigo misma); validación frame a frame durante la captura para detectar cambios sospechosos de píxeles consistentes con intercambio de rostro; y aleatorización opcional de gestos en modalidad de prueba de vida activa para casos de uso de mayor riesgo.

Toda la captura biométrica se realiza de forma multicanal sobre el dispositivo del propio usuario, sin necesidad de hardware adicional. Los canales soportados son: SDK nativo Android (mínimo Android 5, targetSdk 29 o superior), SDK nativo iOS (mínimo iOS 11, Swift 5.2 o superior), SDK híbrido (Cordova / React Native / React Native Light), SDK Web JavaScript (cualquier navegador moderno con acceso a cámara) y API REST para integraciones server-to-server. La captura utiliza la cámara frontal del dispositivo, y los frames se procesan en tiempo real para verificar centrado, encuadre, presencia de un único rostro y prueba de vida antes de ser enviados al backend para la validación biométrica.

La solución biométrica soporta nativamente los documentos de identidad de Costa Rica mediante templates dedicados: la cédula de identidad costarricense con imagen holográfica (emitida desde septiembre de 2016) — template VU-CRI-ID-02 — y la cédula de identidad costarricense moderna (emitida desde agosto de 1998) — template VU-CRI-ID-03. Los datos extraídos por OCR incluyen nombre, apellido, nacionalidad, número de cédula, fecha de vencimiento y fecha de nacimiento. La solución es además agnóstica al documento por diseño: se agregan nuevos templates de documento a la biblioteca tan pronto como hay una cantidad suficiente de muestras para entrenar los modelos de Machine Learning subyacentes, permitiendo extender la cobertura a pasaportes, permisos de residencia y otros documentos de identidad a solicitud. La verificación se realiza comparando los datos biométricos capturados en vivo del usuario contra el documento de identidad presentado durante la misma sesión — un proceso totalmente autocontenido que no requiere integración con el TSE ni con la Dirección General de Migración y Extranjería.

1.2. Modalidad Biométrica y Estándares Aplicables

La modalidad biométrica implementada es la validación facial pasiva combinada con detección pasiva de prueba de vida. El rostro capturado en vivo del usuario durante la sesión se compara algorítmicamente contra el retrato extraído del documento de identidad presentado, mediante el motor de análisis facial, que realiza comparación 1:1 con métodos de similitud configurables (cosine, euclidean, mahalanobis y métodos propietarios v1 a v4) y adicionalmente puede ejecutar comparación 1:N contra registros previos para detección de duplicados. El componente de prueba de vida pasiva certifica que la captura proviene de una persona real y viva, físicamente presente al momento de la transacción, sin requerir gestos activos por parte del usuario. No se incluyen otras modalidades biométricas — huella dactilar, escaneo de iris ni reconocimiento de voz — salvo acuerdo por separado.

La prueba de vida pasiva está certificada iBeta PAD Level 2 conforme a ISO/IEC 30107-3, y VU se encuentra actualmente postulando a la certificación Level 3. iBeta Quality Assurance es un laboratorio acreditado por NVLAP bajo el NIST National Voluntary Laboratory Accreditation Program, por lo que las pruebas se realizan bajo el marco metodológico reconocido por NIST.

Detalles de la certificación: producto certificado Secure Onboarding Process versión 1.2.5.1, servidor versión 1.29.0; normas ISO/IEC 30107-1 e ISO/IEC 30107-3 (Information technology — Biometric presentation attack detection); nivel PAD Level 2, que cubre ataques de presentación de mayor sofisticación, incluyendo máscaras 3D y pantallas; laboratorio iBeta Quality Assurance, Denver, Colorado, EE. UU. La carta oficial de confirmación de iBeta está disponible bajo solicitud para su incorporación al expediente de la oferta.

La captura del retrato Entendemos, aceptamos y cumplimos con las recomendaciones de ISO/IEC 19794-5 y las estructuras de datos definidas en ISO/IEC 39794-5, referenciadas en el Código Nacional de Tecnologías Digitales del MICITT de 2024. Las imágenes capturadas incluyen encuadre completo de cabeza y cuello superior, rostro centrado que ocupa el 70–80% de la imagen, vista frontal con mirada directa a la cámara, ambos lados del rostro visibles, expresión neutral con labios cerrados, sin objetos ni accesorios que cubran rasgos del rostro, fondo blanco o gris claro sin sombras, e iluminación adecuada sin reflejos ni efecto de ojos rojos. Las referencias a los puntos característicos del rostro utilizadas por los algoritmos de comparación siguen los Parámetros de Definición de Rostros establecidos en ISO/IEC 14496-2 (MPEG-4), garantizando compatibilidad con modelos de landmarks faciales reconocidos internacionalmente.

La funcionalidad de análisis de rostro soporta umbrales de aceptación configurables a través de más de 90 parámetros expuestos por el SDK, de manera que la False Acceptance Rate (FAR) y la False Rejection Rate (FRR) puedan ajustarse a la tolerancia al riesgo acordada por las partes. Los valores detallados de FAR y FRR serán propuestos formalmente con base en el perfil de desempeño de la solución y acordados en coordinación con el CTPN-M y la ERPN seleccionada antes de la activación del módulo. El motor se encuentra desplegado en producción en más de 27 países y ha protegido a más de 350 millones de usuarios a la fecha, con experiencia comprobada en los sectores de Telecomunicaciones, Petróleo y Gas, Salud, Juegos On Line, Banca y Gobierno.

1.3. Comportamiento Funcional del Servicio

La solución de proceso de enrolamiento seguro cubre íntegramente los cuatro requerimientos del comportamiento funcional dentro de un único flujo de validación:

(a) correspondencia entre rostro y documento: el motor de análisis de rostro realiza la comparación 1:1 entre la “selfie” en vivo del usuario y la foto del titular extraída del documento por OCR (photo crop), devolviendo un score de similitud con métodos configurables (cosine, euclidean, mahalanobis y métodos propietarios v1 a v4);

(b) prueba de vida pasiva (Prueba de Vida) certificada iBeta PAD Level 2 conforme a ISO/IEC 30107-3, complementada opcionalmente con prueba de vida activa basada en gestos (sonrisa, guiño, ojos cerrados, giro de rostro) con aleatorización de gestos para casos de mayor riesgo — garantizando que el usuario es una persona viva que realiza la acción en tiempo real y no una foto, video replay, máscara 3D, screenshot o deepfake generado por IA. La solución de proceso de enrolamiento seguro dispone adicionalmente del componente Government Proxy REST y de la funcionalidad TrustHub para conectar con fuentes de datos externas (por ej. gobiernos, TSE) y verificar el estado del titular del documento, lo que permite a la ERPN validar que el usuario no se encuentra fallecido;

(c) autenticidad del documento y protección contra deepfakes: el servicio ID Anti-Spoofing aplica modelos de Machine Learning entrenados sobre muestras auténticas y fraudulentas para detectar si la imagen del documento es real, una foto impresa o una fotocopia, y si el documento ha sido alterado parcialmente para ocultar información; el módulo Antispoofing Face in Document analiza específicamente la fotografía dentro del documento para detectar intervención o reemplazo; y el modelo de Deepfake Detection on-demand añade una capa adicional contra ataques de medios sintéticos generados por IA. En conjunto, estas tres capas brindan protección integral frente a todas las categorías principales de robo de identidad y fraude remoto.

Antes de capturar o procesar cualquier dato biométrico, la solución permite la integración de pantallas de consentimiento (a desarrollar por el integrador) que se muestran antes del inicio de la captura. El paso de consentimiento registra datos del dispositivo (fingerprint del dispositivo, modelo, sistema operativo, IP) y un sello de tiempo vinculado al operation GUID de la sesión, dejando una evidencia auditable del consentimiento explícito del usuario para utilizar una fotografía de su rostro para compararla con el documento capturado y, según corresponda, para iniciar el proceso de portabilidad numérica. No se recolecta ni procesa dato biométrico alguno sin este paso de consentimiento afirmativo. El mecanismo de consentimiento es compatible con GDPR y genera un registro de consentimiento con sello de tiempo como parte de la pista de auditoría de la sesión, accesible a través del backoffice de la solución.

La interfaz de captura brinda retroalimentación visual e instruccional en tiempo real al usuario durante todo el proceso de captura de la selfie. El SDK valida en vivo que sólo haya un rostro en cuadro, que el rostro esté centrado, que ocupe al menos el 50% del encuadre (configurable hasta el 80%), que haya iluminación suficiente y que el fondo sea adecuado, antes de capturar la imagen final. Los mensajes en pantalla guían al usuario para ajustar posición, distancia, iluminación o encuadre hasta que la imagen capturada cumpla los umbrales de calidad requeridos para un procesamiento de reconocimiento facial exitoso, contribuyendo a una alta tasa global de éxito por sesión.

El componente de captura de documento incluye la ID-Analysis-API con procesamiento OCR sobre documentos de identidad, ejecutándose sobre dos motores intercambiables (Microsoft Cognitive Services OCR y Cognitive Services de la propia solución). El conducto de procesamiento

incluye un Document Normalizer que identifica y recorta el documento dentro de la imagen, estandariza rotación e inclinación, facilita la lectura OCR y produce el photo crop del titular; alineación con template específico de cada documento; OCR parsing con clasificación de áreas por patrones y detección de áreas por color de template; y normalización de campos (formatos de fecha, nombres, números).

Los datos personales — nombre, apellido, nacionalidad, número de cédula, fecha de vencimiento y fecha de nacimiento — se extraen automáticamente y se entregan vía API al backend de la ERPN sin requerir reingreso por parte del usuario. También se soportan MRZ Reader y Barcode Reader (PDF417) cuando están presentes, aunque el PDF417 de la cédula costarricense está encriptado por el TSE y no se decodifica. La información operativa no contenida en el documento de identidad — específicamente el o los números telefónicos a registrar a través del proceso de portabilidad y el correo electrónico del usuario — se ingresa manualmente por el usuario mediante campos de formulario claramente etiquetados con validación de formato, que residen en la capa de aplicación del SIPN que invoca a proceso de enrolamiento seguro.

La verificación de autenticidad del documento se realiza automáticamente dentro de cada sesión mediante el servicio ID Anti-Spoofing, basado en modelos de Machine Learning entrenados sobre documentos auténticos y fraudulentos. El servicio aplica reconocimiento sin necesidad de templates (cualquier cédula puede ser analizada independientemente del país emisor) en conjunto con reconocimiento de marcas de seguridad específicas de cada tipo de documento. Para documentos costarricenses esto incluye la imagen holográfica de la cédula nueva, el escudo en oro, el mapa del país en el fondo y el área del PDF417, aplicando las mejores prácticas de la industria para detección de alteraciones, falsificación y fotocopias. El módulo Antispoofing Face in Document analiza específicamente la fotografía dentro del documento para detectar intervención o reemplazo. Los documentos que no superan las verificaciones de autenticidad son rechazados y marcados con un motivo de rechazo específico en el log de la sesión.

Mediafon Datapro mantiene una política de actualización evolutiva continua que se incluye sin costo adicional dentro del servicio contratado. Los componentes cubiertos por el ciclo de mejora continua incluyen: el motor biométrico Face Analysis (con actualizaciones periódicas de modelos, nuevas redes neuronales y reentrenamientos); los modelos de antispoofing facial (reentrenados con nuevas muestras de ataques observadas en producción); el modelo de detección de deepfakes (actualizado conforme a la evolución del estado del arte en IA generativa); el componente de OCR (con nuevos templates y mejoras al Document Normalizer); y el servicio de prueba de vida pasiva (recertificaciones iBeta periódicas). Operativamente, las actualizaciones se despliegan en modalidad hot-swapping desde el ambiente de pre-producción, con políticas de rollout incremental y capacidad de rollback ante eventuales fallos. Los cambios significativos se notifican al cliente con antelación, y las release notes detalladas por componente se publican en el portal de documentación técnica. El SLA del servicio es de 99% de uptime anual fuera de las ventanas de mantenimiento programado.

1.4. Especificaciones de Captura del Retrato (Selfie)

La interfaz de captura del proceso de enrolamiento seguro Entendemos, aceptamos y cumplimos punto por punto con las especificaciones de calidad del retrato definidas en los requerimientos. Las siguientes subsecciones describen cómo cada requerimiento es atendido por el motor Face Analysis y el SDK del proceso de enrolamiento seguro.

1.4.1. Formato de la Fotografía

El proceso de enrolamiento seguro (en adelante, PES) captura la imagen a color (24 bits, espacio de color RGB) y la entrega en formato JPEG (ISO/IEC 10918-1) por defecto — el formato que ofrece el mejor balance entre calidad y peso para transmisión en redes móviles. También se soportan los formatos de salida JPEG-2000 (ISO/IEC 15444-1) y PNG (ISO/IEC 15948:2003), configurables para cumplir con los requerimientos específicos de la integración con el SIPN. La captura se entrega en dos resoluciones simultáneas: estándar (640×480) y alta calidad (~2 MPx, dependiendo de la cámara del dispositivo), utilizadas diferencialmente por los módulos de matching biométrico y antispoofing. La captura de la selfie produce adicionalmente un GIF corto que registra el movimiento de captura, brindando una capa adicional de evidencia verificable de prueba de vida.

1.4.2. Calidad de la Fotografía

PES implementa múltiples validaciones automáticas de calidad al momento de la captura. Una verificación de balance monocromático detecta imágenes en blanco y negro o con tonos monocromáticos (indicador de manipulación o impresión). Una validación de saturación de canales RGB rechaza imágenes con baja varianza en los canales de color, garantizando al menos 7 bits de variación de intensidad (al menos 128 valores únicos) en la región de la imagen. Una validación de patrones de pantalla descarta fotografías de pantallas. La captura se realiza en alta resolución (~2 MPx), preservando detalles faciales finos como arrugas, lunares y textura de piel para uso del motor de comparación biométrica. El enfoque se valida mediante el feature “blurry” de Face Analysis, y se capturan y promedian 10 frames base para evaluar el rostro y filtrar capturas no nítidas.

1.4.3. Posición del Rostro Respecto a la Cámara

El SDK de PES valida en tiempo real, antes de capturar la imagen final: la posición frontal de la cabeza (head pose estimation con ángulos Euler controlados); la mirada hacia la cámara mediante detección de orientación de los ojos; y la apariencia natural, tomando 10 frames base esperando que el usuario no esté sonriendo, no tenga los ojos cerrados ni el rostro girado. Los rangos angulares detectables son leftRight de -90° a +90° y upDown de -70° a +70°, con tolerancias configurables para definir lo que se considera una pose válida.

1.4.4. Posición y Apariencia Facial

Las directrices oficiales de captura de imagen de PES Entendemos, aceptamos y cumplimos este requerimiento punto por punto: la imagen debe reflejar la cabeza entera y la parte alta del cuello; ambos lados del rostro deben estar completamente visibles; el rostro debe estar alineado con el eje vertical de la imagen; la vista debe ser frontal con el rostro dirigido al lente; los features “mouthSlightlyOpen” y “smiling” se detectan automáticamente para asegurar labios cerrados y expresión neutral; el head pose estimation rechaza inclinaciones excesivas (arriba/abajo, izquierda/derecha); y el sistema verifica que sólo haya un rostro en cuadro antes de iniciar la captura.

1.4.5. Dirección y Visibilidad de los Ojos

Face Analysis detecta la apertura de cada ojo de manera independiente mediante las etiquetas “leftEyeClosed” y “rightEyeClosed”, y rechaza capturas en las que alguno de los ojos esté cerrado (salvo durante el gesto de prueba de vida activa de ojos cerrados). Durante la captura del frame neutro, el sistema verifica la apertura simultánea de ambos ojos, la visibilidad de la región ocular sin oclusión por cabello (validado mediante análisis facial y los features “heavyMakeup”/cobertura de cabello) y la apertura natural (apoyada por las directrices visuales mostradas en la pantalla de captura).

1.4.6. Brillo y Contraste

PES incluye una etapa de preprocesamiento que normaliza brillo y contraste como parte del conducto de Face Analysis. Las validaciones de calidad ejecutadas son: normalización de brillo y contraste en escala de grises antes de la comparación biométrica; Cross Background Validation, que compara el fondo de las tres selfies tomadas durante el registro para detectar inconsistencias; validación de nitidez mediante el feature “blurry”; y análisis de histograma de cada canal de color para detectar problemas de saturación.

1.4.7. Iluminación

La captura de PES se ejecuta con la cámara estándar del dispositivo del usuario, sin filtros de polarización ni modificaciones ópticas. El SDK utiliza las APIs nativas de cámara (Android Camera2 / iOS AVFoundation / Web getUserMedia), accediendo directamente al lente del dispositivo. Las validaciones para asegurar buena iluminación incluyen: verificación de luminancia mínima en la región facial antes de la captura; detección de reflejos y sombras por el modelo de calidad de imagen; detección de efecto ojos rojos con descarte automático del frame; y un tutorial en pantalla que indica las condiciones de iluminación recomendadas. La información de textura de piel se preserva en la captura en alta calidad (~2 MPx), permitiendo que los algoritmos de comparación facial y antispoofing extraigan landmarks finos.

1.4.8. Anteojos

Face Analysis incluye la funcionalidad “eyeglasses”, que detecta la presencia de anteojos en la imagen capturada. Por configuración, el flujo puede rechazar capturas con anteojos cuando se requiere máxima precisión. Si se permiten anteojos (configuración estándar), el sistema verifica la visibilidad de los ojos a través de los cristales mediante “leftEyeClosed”/“rightEyeClosed” y rechaza casos con reflejos, cristales oscuros o de color, o gafas de sol. Los reflejos y brillos sobre la superficie del cristal se detectan automáticamente. Una excepción médica declarada puede atenderse mediante un flujo alterno con revisión manual en el backoffice, donde la excepción queda registrada como parte de la sesión y el proceso continúa sujeto a la condición declarada.

1.4.9. Cobertura de la Cabeza

Las directrices de captura de PES establecen que la imagen no debe contener accesorios que cubran rasgos del rostro (pañuelos, barbijos, capuchas, gorras). El motor de Face Analysis adicionalmente detecta máscaras faciales mediante el feature “faceMask”. Las coberturas

religiosas de cabeza se atienden mediante un flujo de excepción: cuando el flujo automático rechaza una captura por este motivo, la sesión puede ser derivada a revisión manual en el backoffice, acompañada del registro de la condición declarada por el usuario. En todos los casos el sistema verifica que la región facial desde la corona hasta la base de la barbilla, los puntos de contacto superior entre cada oreja y la cara, y el punto medio entre la línea del cabello y la frente estén completamente visibles sin distorsión ni sombras.

1.4.10. Accesorios Faciales

PES detecta ornamentación facial y obstrucciones mediante el conjunto de features de Face Analysis (“faceMask”, “heavyMakeup”, “eyeglasses”) y los modelos de detección de landmarks faciales. El comportamiento es: detección automática de máscaras y elementos que cubren el rostro; validación de visibilidad de landmarks de ojos, nariz, boca y línea mandibular; admisión de ornamentación que no obstruye (aretes, piercings faciales discretos, maquillaje no excesivo). El umbral de cada funcionalidad es configurable por el cliente.

1.4.11. Dimensiones del Retrato y Ubicación de la Cabeza

Las directrices oficiales de captura de PES establecen que la cabeza debe ocupar el 70–80% de la fotografía y debe estar centrada tanto en el eje vertical como en el horizontal, alineada con la franja del 74–80% indicada por SUTEL. Las validaciones automáticas del SDK incluyen: verificación de que el rostro esté centrado en el frame antes de la captura; verificación de que el rostro ocupe al menos el 50% del frame (umbral mínimo, configurable hasta el 80%); detección de landmarks faciales conforme a MPEG-4 / ISO/IEC 14496-2 (Face Definition Parameters); y un crop normalizado tras la captura para producir el output con encuadre estandarizado. Los umbrales exactos (45–55% lateral, 30–50% vertical) son configurables a través de los más de 90 parámetros expuestos por el SDK.

1.5. Calidad de Imagen del Documento de Identidad

Las imágenes del documento capturadas durante la sesión biométrica son procesadas por el módulo Document Normalizer de PES, que ejecuta un pipeline de control de calidad automatizado de extremo a extremo antes de que las imágenes sean aceptadas para el procesamiento OCR y la comparación biométrica.

La captura se realiza con la cámara trasera del dispositivo en resolución óptima; el normalizador escala la imagen al tamaño objetivo balanceado para OCR, con parámetros de resolución y peso configurables para alinearse con los umbrales del pliego (72 ppp, peso ideal 200–300 KB, lado más largo ≤ 1.200 píxeles). El normalizador aplica preprocesamiento que ajusta brillo y contraste para maximizar la legibilidad del texto contra el fondo, lo que mejora el desempeño del OCR sobre documentos con fondos complejos como la cédula costarricense (escudo en oro y mapa del país). Los documentos capturados con iluminación deficiente o con reflejos se marcan y se solicita al usuario que vuelva a tomar la captura en mejores condiciones.

El conducto establecido aplica filtros de denoising antes de la inferencia OCR, eliminando ruido térmico, artefactos granulares y artefactos de compresión para mejorar el reconocimiento de caracteres bajo condiciones de captura sub-óptimas. El Document Normalizer identifica los bordes del documento, lo recorta de la imagen y aplica deskew (corrección de rotación e

inclinación) para alinear el texto horizontalmente, garantizando una entrada óptima al motor OCR independientemente del ángulo en que el usuario haya sostenido el documento durante la captura. Esta corrección geométrica incluye normalización de perspectiva y detección de orientación.

1.6. Obligaciones de Reporte

PES incluye un Backoffice de administración que registra de forma persistente cada transacción biométrica y permite generar reportes operativos detallados. El reporte mensual cubre la actividad completa de validación biométrica dentro del período de reporte e incluye: cantidad total de validaciones exitosas (estado APPROVED); validaciones rechazadas desglosadas por código de motivo — alteración de documento, persona no concuerda (mismatch biométrico), antispoofing fallido, calidad insuficiente y otros (más de 30 códigos de respuesta estandarizados); validaciones derivadas a revisión manual (estado PENDING_REVIEW); y la distribución horaria de las transacciones, que permite identificar el pico máximo de validaciones realizadas en cualquier hora del período de reporte. Los reportes son accesibles directamente a través del portal backoffice de la solución en tiempo real, o pueden entregarse como archivo CSV estructurado de forma mensual, dependiendo de la preferencia del CTPN-M.

PES utiliza el concepto de operación como unidad de transacción, asignando un identificador único (operation GUID) al inicio de cada sesión, antes de cualquier validación. En consecuencia, cada sesión genera una única transacción identificable independientemente del resultado final (APPROVED, REJECTED, EXPIRED, ABANDONED); las sesiones que incluyen múltiples reintentos de OCR, comparación biométrica o prueba de vida se contabilizan como una sola transacción; y el conteo de transacciones se alinea con el criterio del pliego para fines de facturación y reporte. El parámetro de configuración “Enable operation GUID” garantiza la trazabilidad individual de cada sesión dentro del backoffice.

Anexo 1. Tabla de Cumplimiento Sección 8 del Pliego ERP

Pliego §	Requerimiento (resumen)	Estado de cumplimiento	Sección de la propuesta / Referencia
8.1	El SIPN deberá contar con un módulo opcional que permita la validación biométrica remota con algoritmos que permitan constatar que la persona que realiza la gestión está viva. Debe contar con mecanismos para no permitir intentos de fraude o suplantación de identidad.	Entendemos, aceptamos y cumplimos	§1.1 Naturaleza, Alcance y Modelo de Contratación; §1.3 Comportamiento Funcional
8.2	Se requiere que el SIPN pueda realizar validaciones biométricas remotas (no presenciales) con prueba de vida automáticas de la identidad del usuario.	Entendemos, aceptamos y cumplimos	§1.1 Naturaleza, Alcance; §1.2 Modalidad Biométrica
8.3	El servicio de validación biométrica remota (no presencial) se realizará a través del dispositivo utilizado por el usuario final para acceder a la plataforma de Portabilidad.	Entendemos, aceptamos y cumplimos	§1.1 Naturaleza, Alcance y Modelo de Contratación
8.4	La ERP seleccionada deberá presentar un informe mensual de los resultados para las validaciones que realizó el cual indique la cantidad de validaciones exitosas, validaciones rechazadas (con su respectivo desglose como alteración de documentos o persona no concuerda, entre otros), validaciones que requirieron una revisión manual. También deberá incluir un informe que permita determinar la cantidad máxima de validaciones que realizó en 1 hora durante el periodo.	Entendemos, aceptamos y cumplimos	§1.6 Obligaciones de Reporte
8.5	La ERP seleccionada contabilizará una transacción de validación biométrica como una sesión en la que se realice uno o más procesos de revisión de datos personales o de identidad independientemente de si el proceso se completó o no dentro de dicha sesión.	Entendemos, aceptamos y cumplimos	§1.6 Obligaciones de Reporte
8.6	El servicio de biometría en conjunto con la comparación del documento de identidad deberá permitir validar la correspondencia entre ambos, validar que el usuario no está fallecido, realizar la prueba de vida (conocida como Liveness en inglés) y evitar todo tipo de fraudes de suplantación de identidad (como el deepfake).	Entendemos, aceptamos y cumplimos	§1.3 Comportamiento Funcional del Servicio

8.7	Según corresponda, el servicio de validación biométrica con prueba de vida obtendrá el consentimiento del usuario para utilizar una fotografía de su rostro para compararlo con el documento capturado. Según el Código Nacional de Tecnologías Digitales del MICITT (Ministerio de Ciencia, Tecnología y Telecomunicaciones) del 2024, el oferente deberá señalar la forma en la cual cumple o supera las recomendaciones para la captura de retratos según la normativa ISO/IEC 19794-5 y Estructuras de datos ISO/IEC 39794-5. El sistema de captura deberá brindar retroalimentación en tiempo real al usuario para garantizar que la fotografía permita llevar el proceso de reconocimiento facial. Se deberá considerar lo siguiente:	Entendemos, aceptamos y cumplimos	§1.3 Comportamiento Funcional; §1.2 Estándares; §1.4 Especificaciones de Captura del Retrato
8.7.1 / 8.7.1.1	Debe ser “pasiva” y cumplir con los estándares del NIST e ISO 30107-3.	Entendemos, aceptamos y cumplimos	§1.2 Modalidad Biométrica y Estándares Aplicables
8.7.1.1.1	La fotografía debe ser a color, centrada y enfocada, para su formato se puede utilizar una de las siguientes codificaciones <ul style="list-style-type: none"> a. Formato JPEG (ISO/IEC 10918-1) b. Formato JPEG-2000 (ISO/IEC 15444-1) c. Formato PNG (ISO/IEC 15948:2003) 	Entendemos, aceptamos y cumplimos	§1.4.1 Formato de la Fotografía
8.7.1.1.2 8.7.1.1.2.1 8.7.1.1.2.2	La fotografía tiene que ser neutral en cuanto al color y el reflejo natural del color de la piel, para lograr una foto de calidad no debe de haber saturación, todos los canales RGB deben tener al menos siete bits de variación en la intensidad, es decir, que abarque un rango de al menos 128 valores únicos en la región de la imagen. Todas las fotografías deben tener el enfoque y profundidad suficientes, la cámara debe ser capaz de representar con precisión los detalles faciales finos como arrugas y lunares.	Entendemos, aceptamos y cumplimos	§1.4.2 Calidad de la Fotografía
8.7.1.1.3 8.7.1.1.3.1	Posición del rostro con respecto de la Cámara La foto tiene que mostrar a la persona mirando directamente al lente de la cámara, la fotografía tiene que guardar el aspecto natural del rostro.	Entendemos, aceptamos y cumplimos	§1.4.3 Posición del Rostro Respecto a la Cámara
8.7.1.1.4 8.7.1.1.4.1	Posición y aspecto del rostro La imagen en la fotografía debe reflejar la cabeza entera y la parte alta del cuello, los lados derecho e izquierdo del rostro deben estar completamente visibles. La persona fotografiada debe mirar directamente el lente de la cámara, la expresión del rostro debe ser natural y los labios deben estar cerrados. El rostro debe estar mirando fijo el lente de la cámara, la posición de la	Entendemos, aceptamos y cumplimos	§1.4.4 Posición y Apariencia Facial

	cabeza no puede estar torcida, no puede estar de perfil, no puede tener inclinaciones hacia arriba o abajo, debe estar en una posición horizontal con respecto del lente de la cámara.		
8.7.1.1.5 8.7.1.1.5.1	Dirección y visibilidad de los ojos Los ojos deben mirar directamente hacia el lente de la cámara, ambos ojos deben de abrirse de forma natural, claramente visibles, no forzarse al abrirlos, no pueden estar cubiertos por cabello.	Entendemos, aceptamos y cumplimos	§1.4.5 Dirección y Visibilidad de los Ojos
8.7.1.1.6 8.7.1.1.6.1	Brillo y contraste El rostro en todas las partes tiene que ser reflejado de manera nítida y con el contraste adecuado, en general el retrato debe tener brillo y buen contraste entre cara, cabello y fondo.	Entendemos, aceptamos y cumplimos	§1.4.6 Brillo y Contraste
8.7.1.1.7 8.7.1.1.7.1	La iluminación (luz) El rostro debe estar bien iluminado, se tienen que evitar reflejos, sombras en el rostro y el efecto de ojos rojos. No se utilizarán filtros de polarización lineal delante de la lente de la cámara, ya que interfieren con las cámaras de enfoque automático y reducen o eliminan la piel, información de textura que podría ser utilizada por los algoritmos de comparación de imágenes faciales.	Entendemos, aceptamos y cumplimos	§1.4.7 Iluminación
8.7.1.1.8 8.7.1.1.8.1	Personas con anteojos Los ojos tienen que estar bien visibles, el borde de los cristales y los marcos no pueden cubrir los ojos, los anteojos no pueden tener cristales de color u oscuros, los cristales no pueden reflejar la luz, no se pueden utilizar gafas de sol o gafas con filtros de polarización, se aplica una excepción cuando el sujeto afirma razón médica.	Entendemos, aceptamos y cumplimos	§1.4.8 Anteojos
8.7.1.1.9 8.7.1.1.9.1	Cubiertas de cabeza La persona fotografiada no puede tener la cabeza cubierta salvo sea por razones religiosas, pero inclusive en esos casos debe ser visible sin distorsión ni sombras, desde la corona hasta la base de la barbilla, desde el punto de contacto superior entre la oreja izquierda y la cara, desde el punto de contacto superior entre la oreja derecha y cara, desde borde medio entre pelo y frente.	Entendemos, aceptamos y cumplimos	§1.4.9 Cobertura de la Cabeza
8.7.1.1.10 8.7.1.1.10.1	Accesorios faciales La ornamentación facial que oscurece el rostro no es permitida, es permitida aquella que no interfiera en el rostro.	Entendemos, aceptamos y cumplimos	§1.4.10 Accesorios Faciales

8.7.1.1.11 8.7.1.1.11.1	Dimensiones del retrato y ubicación de la cabeza La cabeza debe estar centrada en el retrato, como se describe, la imagen debe estar entre el 74-80% de la foto, con respecto de la línea horizontal ocular. La distancia entre el borde izquierdo y el punto medio de la cara debe estar entre 45-55% y la distancia vertical entre el borde superior y el centro de la cara debe estar entre el 30- 50% del centro de la boca. Los puntos característicos referidos se describen en ISO/IEC 14496-2.	Entendemos, aceptamos y cumplimos	§1.4.11 Dimensiones del Retrato y Ubicación de la Cabeza
8.7.1.2	Según corresponda, el servicio deberá obtener el consentimiento del usuario para el inicio de su gestión de portabilidad numérica y contar con la capacidad para obtener una o varias imágenes claras de su documento de identificación (según corresponda) que le permita al servicio no sólo hacer la lectura y completado de la información correspondiente vía OCR sino hacer una comparación fehaciente con la persona que realiza el proceso. Los oferentes deberán acreditar la forma en la cual cumplen o superan las siguientes características para el servicio:	Entendemos, aceptamos y cumplimos	§1.5 Calidad de Imagen del Documento de Identidad
8.7.1.2.1	El servicio de captura de documentos deberá permitir la obtención de los datos de identificación vía OCR para que los datos personales no tengan que ser ingresados por el usuario.	Entendemos, aceptamos y cumplimos	§1.5 Calidad de Imagen del Documento de Identidad
8.7.1.2.2	Información como el/los números(s) telefónico(s) a registrar y el correo electrónico deberán ser ingresados de manera manual por el usuario.	Entendemos, aceptamos y cumplimos	§1.5 Calidad de Imagen del Documento de Identidad
8.7.1.2.3	Calidad de imagen <ul style="list-style-type: none"> a. Alta resolución: La resolución recomendada para imágenes WEB es de 72 píxeles por pulgada (ppp). El peso ideal de las imágenes es de unos 200-300 kb, y el tamaño del lado largo no debe exceder los 1200 píxeles. b. Relación de contraste y brillo que permita distinguir los caracteres del fondo. c. Eliminar el ruido de la imagen para facilitar la legibilidad para el algoritmo de OCR. d. Corregir la inclinación y orientación de la imagen de modo que el texto quede correctamente alineado. 	Entendemos, aceptamos y cumplimos	§1.5 Calidad de Imagen del Documento de Identidad
8.7.1.3	El servicio deberá ser capaz de hacer la verificación de legitimidad de los documentos de identificación capturados. Deberá verificar si los documentos están alterados de alguna manera considerando las marcas de seguridad según el tipo de documento a validar y la práctica de la	Entendemos, aceptamos y cumplimos	§1.3 Comportamiento Funcional; §1.5 Calidad de Imagen del Documento de Identidad

	industria para descartar si se trata de alguna falsificación o fotocopia.		
8.7.1.4	La Contratista deberá incluir como parte del servicio, las actualizaciones y mejoras que apliquen sobre los algoritmos de biometría con prueba de vida, verificación de documentos y obtención de datos por OCR según las mejores prácticas de la industria.	Entendemos, aceptamos y cumplimos	§1.3 Comportamiento Funcional

E-Signature Certificate

Document ID: 6a18bf0695e44627758a414a


Status: ● Completed

Document: Sección 05 - Mod_Validación_Biométrica

Signer: Daniel Rodrigo Alejandri Cerón (info@mediafon.mx)

Number of Pages: 15

Completion Date: May 28, 2026, 22:18 UTC

Signer	Timestamps	Signature
<p>Daniel Rodrigo info@mediafon.mx Using IP: 187.251.242.165 IP Location: Mexico, Benito Juarez</p> <p>Authentication Method: Email</p>	<div><div>● Viewed May 28, 2026, 22:17 UTC</div><div>● Signed May 28, 2026, 22:18 UTC</div></div>	<div></div>