



REGISTRADURÍA
NACIONAL DEL ESTADO CIVIL

Documento técnico para el “Fortalecimiento, mantenimiento y sostenibilidad de la plataforma PMT II”, así como la adquisición de insumos para la expedición de documentos de identidad en los formatos establecidos por la Registraduría Nacional del Estado Civil

Octubre, 2022

OT Ver 45

Tabla de contenido

1 / Presentación de IDEMIA	5
1.1 > Resumen de la compañía	5
1.2 > Ingresa al mundo de la Identidad Aumentada	6
1.3 > Nuestras fortalezas	8
1.3.1 > Liderando identidades de confianza para un mundo digital en crecimiento	8
1.4 > Sirviendo clientes en 180 países	10
1.5 > Nuestra tradición de innovación	11
1.6 > Soportando 6 principales segmentos	11
1.6.1 > Instituciones financieras	11
1.6.2 > Operadores Móviles	13
1.6.3 > Objetos conectados	14
1.6.4 > Identidad de Ciudadanos	16
1.6.5 > Seguridad Pública	17
1.6.6 > NORAM Identity & Security	18
2 / Resumen ejecutivo	20
3 / Robustecer la plataforma tecnológica	22
3.1 > Insumos para cédula física en policarbonato	22
3.1.1 > Tarjetas en policarbonato pre - personalizadas con tecnología LASINK para documento de Identidad	23
3.1.2 > Entregable	26
3.2 > Ampliación de Capacidad para la Emisión de Unidades de Cédulas digitales.	27
3.2.1 > Generación de Cédulas Digitales adicionales	28
3.2.2 > Entregable	28
3.3 > Ampliación del flujo de transacciones del MBSS facial	29
3.3.1 > Descripción de la solución	29
3.3.2 > Funciones del MBSS facial	30
3.3.3 > Dimensionamiento transaccional Diario	32
3.3.4 > Entregable	33
3.4 > Caso de Uso	33
3.4.1 > Portal web de Gestión de Cédula Digital	34
3.4.2 > Módulo de interoperabilidad	35

3.4.3 > App móvil de Verificación	36
3.4.4 > Evolución de los sistemas operativos de smartphone (ANDROID – iOS)	37

4 / Suministro de EIS para el sistema de atención integrado de identificación 39

4.1 > EIS: Estación Integrada de Servicios	40
4.1.1 > Funciones	41
4.1.2 > Componentes de Hardware	47
4.1.3 > Entregables	49
4.2 > Servicios para EIS	49
4.3 > Entregable	50

5 / Mantenimiento y sostenibilidad de la plataforma tecnológica PMT II del sistema de identificación y registro civil a nivel nacional 51

5.1 > Alcance del proyecto	51
5.2 > Actividades de Mantenimiento y Sostenimiento	52
5.2.1 > Actividad 1: Realizar mantenimiento de la plataforma PMT II	54
5.2.2 > Actividad 2: Ofrecer la disponibilidad de la plataforma PMT II.	57
5.2.3 > Actividad 3: Disponer de un soporte técnico a usuarios	61
5.2.4 > Actividad 4. Cargar la información del trámite del colombiano	62
5.2.5 > Actividad 5. Validar la información del trámite	63
5.2.6 > Actividad 6. Producir documentos de identificación	63

6 / Insumos TESLIN® para TI y CC 66

6.1 > TESLIN® SP1000 TS Preimpreso	66
6.2 > Laminados holográficos y claros	68
6.3 > Entregable	69

7 / Robustecimiento de la App Cédula Digital Colombia 70

7.1 > Características de la Arquitectura	70
7.1.1 > Características Mínimas Ofrecidas para los Centros de Datos en Cloud	71
7.1.2 > Características Mínimas de la Capa de Seguridad	72
7.1.3 > Características Mínimas de la Capa de Monitoreo	73
7.1.4 > Características Mínimas de la Capa de Red y Balanceo de Aplicativos	73
7.1.5 > Características Mínimas de la Capa Interconexión	74
7.1.6 > Características Mínimas Requeridas de los Centros de Datos en Colombia	74

7.1.7 > Características Mínimas Requeridas para la Capa de Red a los Centro de Datos en Colombia	77
7.2 > Características de los Servicios	78
7.2.1 > Incluir notificaciones electrónicas certificadas para la activación de la Cédula de Ciudadanía Digital y los mensajes que reciba el usuario en la aplicación.	78
7.2.2 > Incluir la firma digital con Certificado ECDSA	79
7.2.3 > Incluir servicio de firmado de documentos notificados.	79
7.2.4 > Incluir servicio de estampado cronológico en transacciones de firma de documentos.	80
7.2.5 > Incluir el requisito de reconocimiento por parte de Adobe en la lista (AATL, Adobe Approved Trust List).	80
7.2.6 > Incluir la implementación del estándar definido por el Consorcio de Firmado en Nube para la API de Interoperabilidad de servicios de firmado y estampado.	80
7.2.7 > Incluir el aseguramiento del cumplimiento de estándar ISO para proceso de calidad y seguridad.	81
7.2.8 > Incluir aseguramiento del cumplimiento de estándares para el manejo de datos a través de canales de Internet	81
7.2.9 > Incluir la implementación del servicio de guarda y custodia de los documentos firmados en el APP.	82
7.2.10 > Incluir los componentes de aplicación compatibles con IOS y ANDROID	82
7.2.11 > Incluir los servicios bajo el modelo Infraestructure as a Service.	82
7.2.12 > Incluir esquemas de capacidad de emisión de acuerdo con la demanda de la RNEC	82
7.2.13 > Incluir esquemas de seguridad en la capa de transporte de información	83
7.2.14 > Incluir mecanismos para manejo de alta concurrencia.	83
7.2.15 > Incluir la seguridad jurídica de la protección tecnológica sobre los desarrollos realizados.	83
7.3 > Entregables	84
7.3.1 > Primer Entregable	84
7.3.2 > Segundo Entregable	84

8 / Obligaciones generales de IDEMIA	86
8.1 > Obligaciones generales	86
8.2 > Obligaciones específicas de IDEMIA	88
8.2.1 > Realizar el mantenimiento de la plataforma PMT II.	88
8.2.2 > Disponer de un soporte técnico a usuarios	93
8.2.3 > Ofrecer la disponibilidad de la plataforma PMT II	95
8.2.4 > Cargar información del trámite del colombiano	102
8.2.5 > Validar información del trámite	103
8.2.6 > Producir documentos de identificación	104
8.2.7 > Robustecimiento de la App Cédula Digital	104

1 / Presentación de IDEMIA

IDEMIA es líder en identidades de confianza para un mundo cada vez más digital. IDEMIA pone al cliente, al consumidor o al ciudadano como el centro de toda su investigación y desarrollo combinando seguridad, conveniencia, factor humano y continuidad dentro de una sola proposición. Esta capacidad de integración es lo que llamamos la «combinación mágica».

En un mundo que ha evolucionado hacia lo «digital», IDEMIA concibe la seguridad de una manera global manteniendo una perfecta sincronía con los desarrollos tecnológicos mediante la personalización de los sistemas globales en el entorno específico del cliente y la forma en que este utiliza específicamente nuestros productos. En un mundo de intercambios cada vez mayores, la seguridad significa principalmente proteger identidades. Esta es la razón por la que IDEMIA coloca la identidad aumentada en el corazón de sus acciones.

La llegada del Big Data y del Small Data, la agitación económica a gran escala causada por la digitalización de las transacciones y los nuevos riesgos de seguridad que se deben afrontar derivados de los factores anteriores, ha hecho que el mundo mantenga un cambio dinámico en la forma de relacionar gobiernos, entidades y personas, lo que deriva en desafíos para la industria de la identidad digital y, para el caso de la posición de liderazgo de IDEMIA, de la identidad aumentada.

Identificar, proteger y contribuir al progreso de nuestra la sociedad, proporcionar a cada individuo una identidad reconocida y segura, y crear confianza en todos los niveles, como un país, una empresa, un sistema de información o simplemente un Smartphone, son los compromisos asumidos por IDEMIA.

1.1 > Resumen de la compañía

La ambición de empoderar a ciudadanos y consumidores por igual para interactuar, pagar, conectar, viajar y votar gracias a la existencia de un entorno conectado, ha obligado a que nuestra identidad sea la misión crítica en el mundo en que vivimos hoy.

En IDEMIA, aceptamos esta nueva realidad y entendemos las preocupaciones de seguridad que surgen junto a los avances globales en tecnología. Analizamos el mundo a nuestro alrededor y reinventamos el concepto de identidad.

Identidad Aumentada: una identidad que asegura privacidad, confiabilidad y que garantiza transacciones seguras, autenticadas y verificables. Una identidad tan mejorada y adaptable que permite disfrutar de la vida, porque proteger nuestra identidad es la clave para hacer de nuestro mundo un lugar más seguro.

Dado que creemos en la Identidad Aumentada, reinventamos la forma en que pensamos, producimos, utilizamos y protegemos este activo, ya sea para individuos o para objetos. Garantizamos la privacidad y la confianza, así como la garantía en transacciones seguras, autenticadas y verificables para clientes internacionales de sectores financieros, de telecomunicaciones, de identidad, de seguridad y del Internet de las cosas.

1.2 > Ingresamos al mundo de la Identidad Aumentada

Proporcionamos soluciones personalizadas en un mundo que evoluciona y avanza más rápido que nunca. Hoy en día, la información viaja rápidamente alrededor del amplio espacio de las comunicaciones digitales, desafiando los límites y rompiendo los códigos tradicionales de seguridad.

→ Liderando hacia el futuro

Ser un líder significa mantenerse al tanto de las innovaciones disruptivas que impactan nuestro entorno de seguridad. Entendemos que el crecimiento exponencial de los objetos conectados promueve una ruta hacia la necesidad urgente de mejorar y garantizar la seguridad de las personas en sus mundos físicos y digitales, incluyendo los objetos con los que interactúan. Sabemos que, en nuestra sociedad globalizada, el número de intercambios entre pares, viajes y cruces fronterizos está creciendo extraordinariamente. Somos conscientes de que la digitalización de la economía genera una ola de nuevos modelos de negocio.

También somos conscientes de la tendencia de consumo de la tecnología y de cómo esta impacta nuestra identidad y la protección de la privacidad.

→ Empoderando a las personas para que disfruten la vida a través de identidades de confianza

En IDEMIA acogemos esta nueva realidad y entendemos las preocupaciones de seguridad que van de la mano con los avances tecnológicos. Analizamos el mundo que nos rodea y reinventamos el concepto de identidad. Lo llamamos identidad aumentada – una identidad que garantiza privacidad y confianza y garantiza transacciones seguras, autenticadas y verificables. Una identidad que es tan mejorada, adaptable, fortalecida y auto soberana que nos permite disfrutar verdaderamente de la vida, porque asegurar nuestra identidad es clave para hacer nuestro mundo un lugar más seguro.

Nuestra promesa es simple: Con nuestras tecnologías e innovaciones solo tú puedes ser tú.

→Una identificación más fluida y segura

Ahora usamos nuestra identidad para pagar, viajar, cruzar fronteras, intercambiar todos los días, divertirnos, abrir una cuenta bancaria, buscar atención médica y utilizar nuestros dispositivos conectados – y esta lista continuará expandiéndose significativamente en los próximos años. Dada la vasta gama de entornos y usos, asegurar nuestra identidad se ha convertido en misión crítica en el mundo en el que vivimos hoy en día. Sin embargo, reconocemos que incluso las medidas de seguridad más estrictas son inútiles si éstas son complejas al momento de utilizarlas, consideramos que las medidas de seguridad deben ser convenientes y fáciles de usar, afines a lo intrínseco de nuestra naturaleza, en lo que somos a través de la biometría.

También observamos que nuestros estilos de vida exigen un nivel de continuidad nunca visto antes. De hecho, necesitamos nuestra identidad para viajar con nosotros sin problemas – ya sea en el mundo físico o digital o para usos gubernamentales, civiles o comerciales.

→Sólo tú puedes ser tú

Nuestra promesa es simple: con nuestras tecnologías e innovaciones sólo tú puedes ser tú.

En el diseño de nuestras soluciones líderes en el mercado, contamos con la verificación más física, natural y auténtica: los datos biométricos propios de nuestro cuerpo. Tu identidad puede ser verificada con una simple mirada o con el toque de un dedo – lo que significa que tu identidad no puede ser robada, imitada, comprometida o alterada. Estarás en control directo de tu información personal.

Hemos reunido conocimientos y tecnologías complementarias que nunca antes se habían combinado. Nuestra tecnología no sólo ayuda a los consumidores a viajar con pasaportes y a pagar con smartphones, sino que te ayuda a identificarte con seguridad y sin esfuerzo. Y con cada disrupción tecnológica, nos adaptamos para satisfacer las nuevas y evolutivas demandas de seguridad del hoy y del mañana.

1.3 > Nuestras fortalezas

1.3.1 > Liderando identidades de confianza para un mundo digital en crecimiento

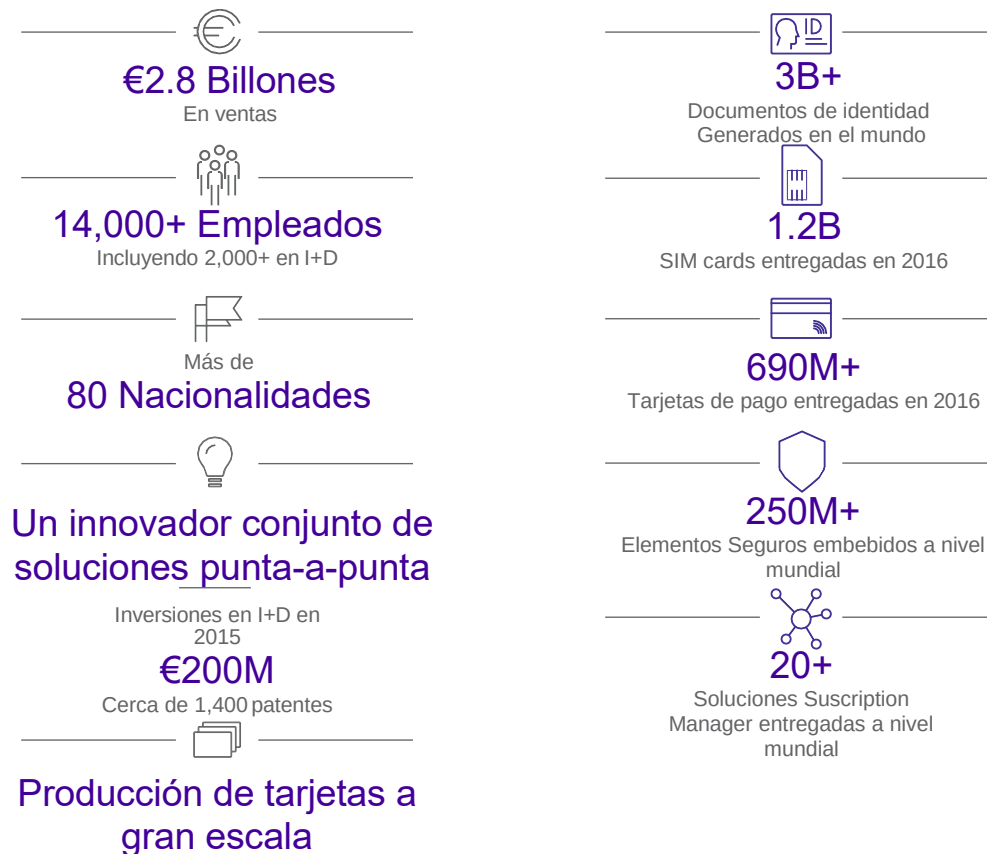


Ilustración 1: Nuestras fortalezas



Bien posicionados en nuestros mercados

#1 en sistemas
biométricos policiales

Confianza en **1,800**
instituciones financieras

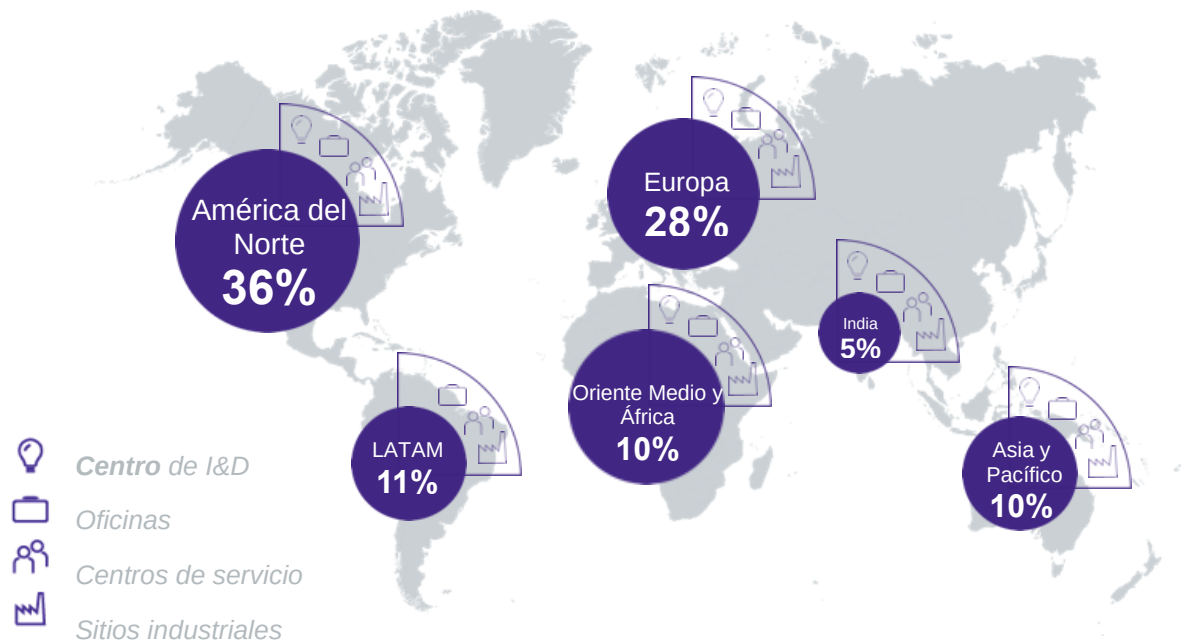
#1 en soluciones de identidad civil

Confianza en **500+**
operadores móviles

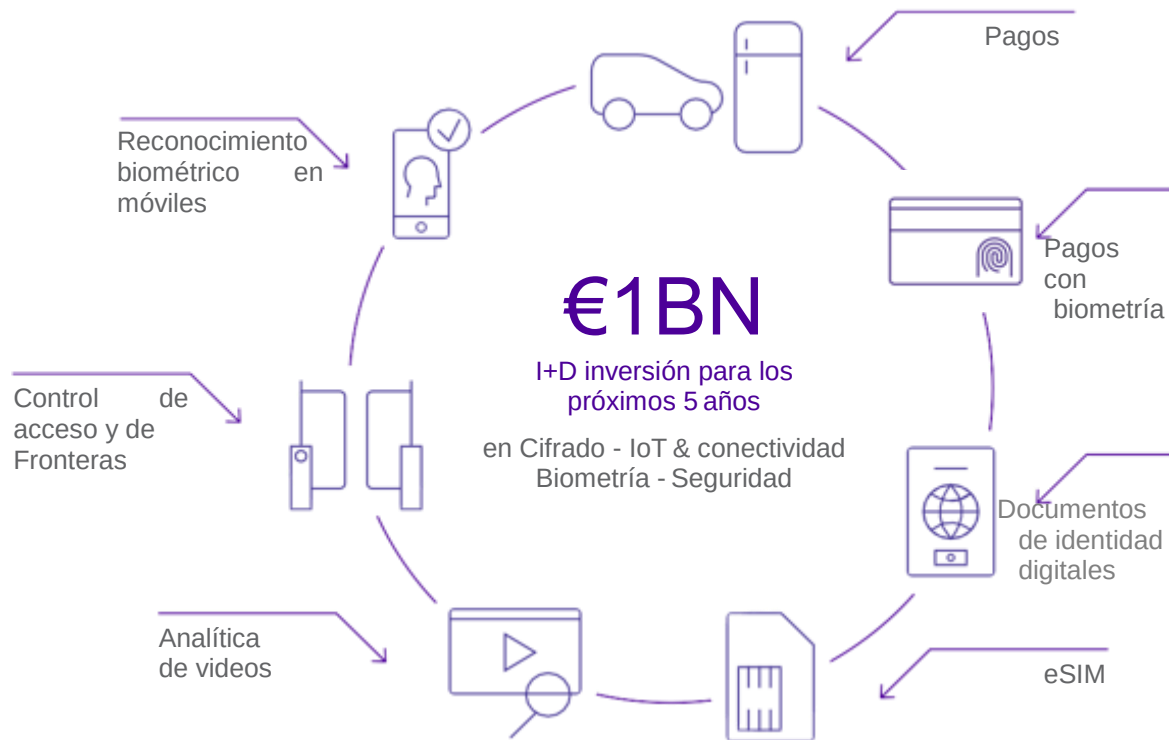
Confianza en los **principales**
fabricantes industriales (OEMs)

#1 en emisión de licencias de
conducir en Estados Unidos

1.4 > Sirviendo clientes en 180 países



1.5 > Nuestra tradición de innovación



1.6 > Soportando 6 principales segmentos

1.6.1 > Instituciones financieras

Nuestra misión es asegurar la diversidad de pagos. IDEMIA es el líder indiscutible, que configura el futuro para una necesidad humana esencial: posibilitar el intercambio sin fricción entre las personas mediante los pagos.

En muy poco tiempo, los avances en la tecnología digital han cambiado la forma en que vivimos. En el pasado reciente, olvidar tu billetera significaba devolverse a casa. Hoy, con unos pocos gestos tales como deslizar, tocar o pulsar la pantalla táctil de tu smartphone,

usted puede probar su identidad, hacer una transferencia de dinero, firmar un contrato bancario, pedir que te transporten, ir de compras y cenar fuera con los amigos. La confianza de los consumidores es la base de cualquier forma de transacción. Pero, ¿cómo podemos asegurar que estas operaciones sencillas desde su smartphone caigan en las manos equivocadas?

→Estudiando el mundo que nos rodea

Mientras diseñamos las soluciones de IDEMIA, aprovechamos nuestra propia curiosidad y observamos a nuestro alrededor para obtener fuentes de inspiración. Observamos que las instituciones financieras actuales están pasando por una transformación masiva del comercio minorista a la banca digital y se encuentran en la búsqueda de estrategias multicanal para proteger las relaciones con los clientes. Para satisfacer sus necesidades, IDEMIA ha desarrollado ofertas que ayudan a las instituciones financieras a incorporar la movilidad y la digitalización, abordando el viaje hacia el futuro de la banca y pagos digitales.

Nuestras tecnologías de gestión de claves secretas se han convertido en misión crítica para las empresas más grandes del mundo. Hemos trabajado para reducir el fraude de pagos – tanto en línea como en las tiendas y estamos conduciendo la migración de pagos EMV, NFC y móvil en todo el mundo. También ayudamos a desarrollar la banca digital, así como también la seguridad móvil y soluciones de pago para IoT/M2M sobre una combinación de servicios de pago innovadores y un conjunto fantástico de tecnologías de autenticación digital, lo que nos permite crear las soluciones de pago de mañana.

→Modelar el futuro de una verdadera necesidad humana

El compromiso de IDEMIA con la Identidad Aumentada y la seguridad en diversos mecanismos de pagos nos han ayudado a convertir a IDEMA en el líder indiscutible del mercado, dando forma al futuro de una verdadera necesidad humana. Nuestras identidades están dentro de cada uno de nosotros. Al aprovechar la biometría, por ejemplo, hemos avanzado de una manera que garantiza una experiencia de pago altamente segura en tanto en la tienda como en línea, proporcionando una experiencia fluida y mejorada para el tarjetahabiente.

En resumen, hacemos de nuestra misión asegurar que nuestros clientes tengan soluciones ágiles y altamente adaptables – custodiadas por medidas de seguridad irrefutables – a su alcance cuando y donde lo necesiten. Después de todo, la conveniencia y la fluidez no son nada si no están acompañadas de la paz mental.

- > 1.800 instituciones financieras (incluyendo la mayoría de los bancos más grandes del mundo) confían en nosotros
- > 1 millón de tarjetas digitales por mes en las 3 principales carteras digitales
- > #1 dominando los mayores proyectos de adquisición y verificación biométrica en el mundo

1.6.2 > Operadores Móviles

Nuestro objetivo es asegurar la movilidad y más allá. IDEMIA es un actor líder en el mercado de las telecomunicaciones, acelerando la revolución digital para proporcionar a sus clientes experiencias seguras y convenientes.

El número de usuarios de smartphones excederá los 6 mil millones en el 2020 (Ericsson's Annual Mobility Report) – y por una buena razón. Estos dispositivos móviles ponen una increíble cantidad de información en la palma de nuestras manos: nuestros horarios, detalles bancarios, correos electrónicos, y cualquier otra cosa que podamos necesitar. Si bien la tecnología responde a los nuevos desafíos y oportunidades de conectividad, en particular con el creciente mercado de IoT, la protección de nuestras identidades digitales se necesita más que nunca.

→Rompiendo fronteras

Cuando IDEMIA miró este desafío, identificamos la necesidad de salvaguardas y servicios que aplican a todo tipo de uso móvil. Optimizamos nuestros servicios, conectando muchos más objetos para habilitar los servicios verticales. Desde el apoyo a la conectividad a través de tarjetas SIM, hasta el uso de dispositivos móviles como portales de entrada biométrica para autenticarnos a nosotros mismos, pasando por el desarrollo de servicios de monederos digitales, nos aseguramos de que los individuos puedan tener el uso completo y sin preocupaciones de sus teléfonos móviles, mientras que sus identidades móviles son salvaguardadas con el más alto nivel de protección.

→La conectividad conveniente de IDEMIA

Como actor líder en el campo de las telecomunicaciones, IDEMIA está a la vanguardia de la revolución digital y estamos comprometidos a aportar experiencias protegidas y convenientes a nuestros clientes los operadores móviles. Diseñamos herramientas para vincular la autenticación fuerte con elementos seguros y plataformas de servicio para garantizar la conectividad simple y el acceso al servicio por parte de los usuarios finales en cualquier lugar y en cualquier momento. El despliegue de tarjetas SIM es crucial para que los operadores móviles obtengan un punto de entrada a los servicios críticos de valor agregado móvil. También apoyamos a nuestros clientes a través de la gestión disruptiva de suscripciones a través de plataformas dedicadas, así como tarjetas SIM embebidas o extraíbles y chips optimizados.

Por encima de todo, es la misión de IDEMIA proporcionar un uso seguro móvil sin inconvenientes. Nuestro papel fundamental es permitir que más personas ingresen con seguridad en el mundo digital e ir más allá de la conectividad para monetizar los servicios que tienen disponibles.

- > 500 operadores de telefonía móvil en todo el mundo (incluidos los principales operadores a nivel mundial de telefonía móvil) confían en nosotros
- > 20 + soluciones entregadas de gestión de suscripciones
- > 100 + plataformas OTA desplegadas en todo el mundo

1.6.3 > Objetos conectados

A través de este segmento, conectamos y hacemos realidad la seguridad en el Internet de las cosas (IoT). Combinamos seguridad embebida y biometría avanzada.

Hemos experimentado tremendos avances tecnológicos en los últimos tiempos. Los dispositivos electrónicos que una vez fueron aislados están ahora conectados y pueden ser operados desde cualquier parte del mundo. Y ya no sólo los humanos interactúan con la tecnología, los equipos electrónicos ahora interactúan con otros equipos.

Desde prendas tecnológicas--wearables y ordenadores personales hasta electrodomésticos y maquinaria industrial, la conectividad está cambiando nuestras vidas y nuestro mundo.

→Creciendo con el mercado del IoT

IoT es un mercado en auge, en rápida expansión. A medida que los nuevos verticales aparecen en la escena, las dinámicas y las aplicaciones evolucionan: el suministro de conectividad es ahora sin fricción y lo que solía ser un producto sencillo es ahora un servicio – todos los desarrollos exigen total seguridad. Sin un nivel de autenticación aumentado, las marcas de los fabricantes y la privacidad de los clientes pueden verse seriamente comprometidas por la piratería informática.

Con estas tendencias en mente, las soluciones de IDEMIA combinan seguridad y conveniencia para permitir a los fabricantes (OEM—Original Equipment Manufacturer) y a los proveedores de servicios de IoT gestionar la conectividad y seguridad de una amplia gama de dispositivos en todo el mundo y para desplegar y mantener servicios críticos de valor agregado durante el ciclo de vida completo del dispositivo.

→Embebiendo seguridad en el campo del IoT

Nuestra experiencia en este campo está soportada por nuestra incomparable capacidad de combinar seguridad embebida y biometría avanzada para imprimir confianza en el campo del IoT. Estamos comprometidos en proporcionar soluciones punta-a-punta para transformar y optimizar el viaje del usuario final. Nuestros hogares pueden ser asegurados y monitoreados remotamente con unos pocos clics en nuestros smartphones. Los automóviles conectados pueden salvar nuestras vidas cuando llaman a servicios de emergencia en caso de que necesitamos ayuda. Los dispositivos móviles seguros y convenientes se han convertido en indispensables para nuestra vida cotidiana – utilizados para realizar pagos, en el transporte y en la identificación.

Los dispositivos conectados son parte de nuestra vida diaria. Es la misión de IDEMIA asegurar los servicios digitales actuales y futuros que surjan del IoT aprovechando nuestras ofertas de hardware, software y de servicios sin igual.

- > Principales fabricantes de equipos industriales (incluidos los fabricantes de automóviles y automóviles Premium y los líderes del IoT) confían en nosotros
- > Líder en eSIM y soluciones de gestión de suscripciones remotas en el dispositivo del cliente y en los campos del IoT.
- > 250 millones de elementos seguros (eSE) embebidos vendidos en el mundo

1.6.4 > Identidad de Ciudadanos

Protegemos la identidad en movimiento. Somos el líder en la industria de la identidad, combinando las referencias de los clientes más fuertes y nuestra experiencia en proyectos.

La identidad de una persona es preciosa. Uno podría argumentar que es la segunda cosa más preciosa después de la vida misma. Nos permite existir a los ojos de la sociedad, así como participar activamente en ella: acceder a la educación y a los servicios de salud o abrir una cuenta bancaria. Como tal, a lo largo de nuestra vida, necesitamos una identidad confiable que pueda ser usada en cualquier lugar, en cualquier momento, ya sea en la vida real o en línea.

→Protección de la identidad para la edad moderna

Los servicios de IDEMIA ayudan a proteger las identidades de los ciudadanos en movimiento. Inspirados por los ciudadanos que viajan más que nunca, que están más conectados y digitales que nunca, pero también más conscientes de la privacidad y de las preocupaciones de seguridad, nuestras soluciones garantizan a los ciudadanos y a gobiernos por igual que cada identidad entregada es única y puede ser de confianza, cuando y en cualquier lugar.

→Centro holístico de soluciones de IDEMIA para la gestión de la dentad

Para nuestros clientes – los gobiernos - somos el centro holístico de soluciones que provee todas las tecnologías requeridas para gestionar y asegurar de manera efectiva toda la cadena de valor de la gestión de la identidad desde el registro y verificación de identidades ciudadanas, hasta la emisión para cada ciudadano de Identidades personalizadas resistentes al fraude – ya sea en forma de documentos tradicionales de identificación o Identidades digitales – para gestionar esas identidades de forma segura tanto en el mundo físico como en el digital. También somos un socio en el largo plazo con la capacidad de ofrecerles la tranquilidad de una concesión bien gestionada por el manejo de las complejidades tecnológicas y la financiación.

Basándonos en décadas de experiencia en soluciones de identidad llave en mano, así como en concesiones a gran escala, ofrecemos a nuestros clientes la más amplia gama de

soluciones de identidad. Hoy en día, los ciudadanos pueden proteger sin esfuerzo su identidad – cuando y donde quiera que lo necesiten.

- > #1 en soluciones de identidad civil y comprometidos en el despliegue biométrico más grande del mundo (Adhaar, India)
- > 3Bn+ de documentos de identidad emitidos
- > 135+ programas activos de identidad ciudadana

1.6.5 > Seguridad Pública

Nuestro objetivo es proteger a las personas y a los lugares. IDEMIA es un socio clave para enfrentar los mayores desafíos de seguridad en todo el mundo.

¡Viajar ya no es lo que solía ser! La gente de hoy está en constante movimiento – moviéndose más rápido y viajando más lejos que nunca. Si bien este aumento en el movimiento alrededor del mundo acerca a nuestras sociedades, también genera nuevas demandas de mayor eficiencia y seguridad para las autoridades públicas.

→ Encontrar el equilibrio adecuado

Vivimos en un ambiente desafiante. Hoy en día, los ciudadanos exigen una verificación de identidad eficiente y transparente para crear un mundo más seguro, pero que al mismo tiempo tenga muy poco impacto en su vida diaria. Para cumplir con esta expectativa, las autoridades tienen la tarea de identificar los riesgos y las amenazas y resolver el crimen en menos tiempo que nunca, a menudo con presupuestos y recursos limitados. Y aunque se dispone de mayores volúmenes de datos, no necesariamente son utilizables.

→ Fortaleciendo la experiencia del usuario

Como líder mundial en soluciones biométricas, nuestras soluciones e innovaciones totalmente integradas se centran en la experiencia del usuario, permitiendo a nuestros clientes hacer más con menos. Este compromiso nos ha ayudado a ganar nuestro lugar como socio estratégico en el largo plazo de las más prestigiosas agencias de aplicación de la ley en el mundo, abordando los principales desafíos globales de seguridad. Y a medida que la tecnología evoluciona, nos comprometemos a avanzar nuestras soluciones también. Ahora combinamos conocimientos digitales y Cloud para aportar una eficiencia sin igual y experiencias de usuario de próxima generación a nuestros clientes.

A través de nuestras últimas innovaciones, soportamos nuestra misión de detectar amenazas en áreas públicas, otorgar de forma segura el acceso a locales y activos físicos, fortalecer la seguridad fronteriza y ayudar a la policía a mejorar drásticamente la eficiencia.

- > #1 en sistemas biométricos de la policía y el proveedor más grande del mundo de terminales biométricos
- > 150 + millones de travesías de pasajeros manejadas
- > 160 Sistemas AFIS (Automated Fingerprint Identification System) desplegados en todo el mundo

1.6.6 > NORAM Identity & Security

Nuestro objetivo: proporcionar seguridad de identidad para asegurar y hacer más sencilla la vida.

La identidad es única – es quien eres, donde vives y representa todo lo que haces. Es personal y privado y merece el más alto nivel de protección.

→ Nuestra profunda experiencia

En IDEMIA, nuestra misión es crear un futuro seguro y sencillo donde la verificación de identidad es indiscutible y sólo usted puede certificar su identidad. Como socio de confianza para las agencias del gobierno de Estados Unidos por más de 50 años, nuestra experiencia en el dominio de la identidad civil, la seguridad pública, los mercados comerciales, la identificación biométrica y la autenticación de documentos es insuperable. Estas fortalezas, combinadas con nuestras relaciones inigualables y el enfoque pionero de IDEMIA en la resolución y prueba de la identidad de las personas, nos hacen el proveedor principal de las soluciones mejores de su clase para las transacciones civiles y comerciales.

→ Afrontar los retos de hoy

La globalización, digitalización y movilidad – son fuerzas conductoras que contribuyen al escenario evolutivo de la identidad y la seguridad. Con el fraude de identidad en aumento, los consumidores necesitan – y en esto son muy exigentes – credenciales de identificación seguras que aprovechen la última tecnología biométrica. Al implementar la amplia gama de soluciones de IDEMIA aprobadas por el gobierno, usted puede estar seguro de que sus identidades están protegidas.

Ya sea que estemos agilizando la seguridad aeroportuaria a través de nuestra TSA pre ✓
® o revolucionando la tecnología de licencias de conducir móvil, nuestras mejores
soluciones y servicios garantizan que el control total de identidad está en sus manos.

- > #1 en la emisión de DL & ID en Estados Unidos
- > #1 en Estados Unidos para servicios biométricos automatizados
- > 5 + millones de ciudadanos inscritos en el programa de TSA pre ✓ ®

2 / Resumen ejecutivo

IDEMIA, líder global en identidades confiables en un mundo cada vez más digital, pone a consideración de la **Registraduría Nacional del Estado Civil – RNEC** el presente documento técnico para la ejecución del proyecto de **Fortalecimiento, mantenimiento y sostenibilidad de la plataforma PMT II**”, así como la adquisición de insumos para la expedición de documentos de identidad en los formatos establecidos por la **Registraduría Nacional del Estado Civil** y los servicios conexos.

Con el ánimo de garantizar la prestación de servicios de forma ininterrumpida, IDEMIA, por medio de la presente, pone a disposición de la **RNEC** las actividades correspondientes al proyecto aquí detallado, que comprende todas las tareas globales encaminadas a lograr la continuidad y sostenibilidad del Sistema de Identificación de los colombianos y por otro lado actividades de fortalecimiento de la infraestructura actual de la plataforma PMT II.

Los siguientes son los componentes de la solución ofertada por IDEMIA:

1. Robustecer la plataforma tecnológica

- A. Insumos para cédula física en policarbonato
Adicional ochocientos veinticinco mil (825.000) de tarjetas
- B. Ampliación de cédula digital
Ampliación de capacidad para ochocientos veinticinco mil (825.000) unidades.
- C. Ampliación del flujo de transacciones del MBSS facial, seiscientos mil (600.000) licencias adicionales.
- D. Caso de uso
 - a. Portal web de Gestión de Cédula Digital
 - b. Módulo de Interoperabilidad
 - c. App Móvil de Verificación
 - d. Evolución de los sistemas operativos de smartphone (ANDROID – iOS)

2. Suministro de EIS para el sistema de atención integrado de identificación

- A. Suministro de hardware para EIS: Estación Integrada de servicios – 254 unidades
- B. Alistamiento de las EIS

3. Mantenimiento y sostenibilidad de la plataforma tecnológica PMT II del sistema de identificación y registro civil a nivel nacional

Este servicio se ofrece por un término de ejecución hasta el 31 de diciembre de 2022, y comprenderá los siguientes grupos de actividades:

Actividad 1: Realizar mantenimientos de la plataforma PMT II.

Subactividad 1: Realizar mantenimiento correctivo de la plataforma PMT II.

Subactividad 2: Mantenimiento plataforma Cédula Digital

Subactividad 3: Mantenimiento plataforma Autenticación Facial

Actividad 2: Ofrecer la disponibilidad de la plataforma PMT II.

Actividad 3: Disponer de un soporte técnico a usuarios.

Actividad 4. Cargar la información del trámite del colombiano.

Actividad 5. Validar la información del trámite.

Actividad 6. Producir documentos de identificación.

Administrar y operar la fabrica

4. Insumos Teslin TI y CC

Suministro de insumos en Teslin para producción de Cédula de Ciudadanía y Tarjeta de Identidad.

5. Robustecimiento de la App Cédula Digital Colombia

De acuerdo con los requerimientos presentados por Registraduría Nacional del Estado Civil en su solicitud de cotización RDRC-360 del 4 de octubre de 2022 y su anexo, IDEMIA oferta lo solicitado para una solución que permitirá incorporar nuevas funcionalidades a la cédula digital diseñadas para soportar los servicios ciudadanos digitales de entidades públicas y particulares, para que la cédula de ciudadanía digital sea la llave de acceso a trámites y servicios generando posibilidad de notificación y firmado digital de documentos, gestión de documentos remitidos por autoridades y entidades autorizadas, al igual que el servicio de wallet para alojar otros documentos.

A continuación, se detallan los componentes ofrecidos por IDEMIA.

3 / Robustecer la plataforma tecnológica

IDEMIA presenta este documento técnico con el fin de atender las necesidades de RNEC mediante una solución de fortalecimiento de la plataforma tecnológica PMT II, con los siguientes componentes:

- A. Insumos para cédula física en policarbonato
Adicional ochocientos veinticinco mil (825.000) de tarjetas
- B. Ampliación de cédula digital
Ampliación de capacidad para ochocientos veinticinco mil (825.000) unidades.
- C. Ampliación del flujo de transacciones del MBSS facial
- D. Caso de uso portal web mobile / App de verificación
 - a. Portal de gestión de Cédula Digital para uso del ciudadano
 - b. Módulo de interoperabilidad para autenticación con portales
 - c. Evolución App móvil de verificación
 - d. Evolución de los sistemas operativos de smartphone (ANDROID – IOS)

A continuación, se detallan los componentes ofrecidos por IDEMIA.

3.1 > Insumos para cédula física en policarbonato

RNEC requiere la fabricación, pre personalización y entrega en la ciudad de Bogotá de ochocientos veinticinco mil (825.000) unidades de tarjetas en policarbonato tamaño ID1, de conformidad con “el documento técnico para la producción de la cédula de ciudadanía digital de la RNEC”, acogiendo la personalización con tecnología LASINK.

Esta sección, IDEMIA describe la propuesta para el suministro de Insumos para producción de tarjetas ID1 de cédula de física de seguridad personalizada en policarbonato.

3.1.1 > Tarjetas en policarbonato pre - personalizadas con tecnología LASINK para documento de Identidad

Se considera la fabricación, personalización y entrega ochocientos veinticinco mil (825.000) unidades de tarjetas en policarbonato tamaño ID1, de conformidad con las medidas de seguridad y la tecnología LASINK ya definidas por la **RNEC**.

Nota: *Esta entrega se hará en dos momentos; el primero se entregarán 200.000 tarjetas pre – personalizadas. La segunda entrega para la cantidad restante (625.000) se llevará a cabo en la fábrica de producción de documentos de IDEMIA en Europa, dado que respecto a la capacidad actual de bodegaje de la entidad no es posible almacenar dicho material conforme las disposiciones de capacidad y exigencias de temperatura, humedad y seguridad requeridas para estos elementos, según la solicitud de la entidad (Ver documento Bóveda de Seguridad Fábrica RNEC). Para esta actividad se requiere la participación de una persona debidamente autorizada por la supervisión del contrato.*

3.1.1.1 > Características físicas de la tarjeta a ser suministrada

Diseño de la Tarjeta

El diseño actual de la cédula de identidad ya definido por RNEC tiene las siguientes características que cumplen las recomendaciones ICAO las cuales recomiendan distribuir los datos en 7 zonas dentro del documento de la siguiente manera:

- Parte Frontal
 - Zona 1: Obligatorio, encabezado.
 - Zona 2: Obligatorio y opcional, datos personales y otros datos.
 - Zona 3: Obligatorio y opcional, datos del documento.
 - Zona 4: Obligatorio, firma del titular o marca habitual.
 - Zona 5: Obligatorio, característica de identificación.

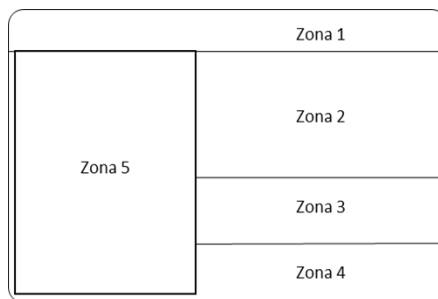
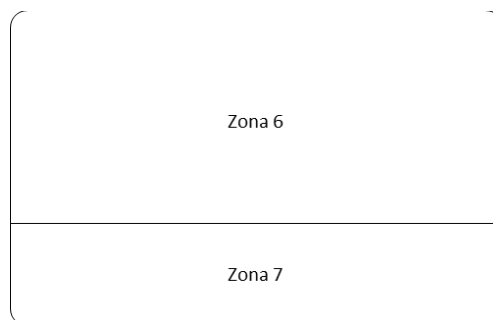


Ilustración 1. ICAO zonas para la información de un documento de identidad frente

- Parte del reverso

- Zona 6: Opcional, datos adicionales.
- Zona 7: Obligatorio, Zona de Lectura Mecánica MRZ.



El siguiente Cuadro refleja las características técnicas de la tarjeta a suministrar:

DOCUMENTO DE IDENTIFICACIÓN	
ITEM	DESCRIPCIÓN
Dimensiones	Las dimensiones y tolerancias definidas en ISO/IEC 7810 para las tarjetas ID-1 de policarbonato, bajo condiciones de 23°C $\pm$ 3°C y humedad relativa entre 40% y 60%, son: • Tamaño Nominal Mínimo: 53,92 mm x 85,47 mm Máximo: 54,03 mm x 85,72 mm • Radio de redondeo de esquinas Radio mínimo: 2,88 mm Radio máximo: 3,48 mm • Espesor El espesor es de 0,76 mm $\pm$ 0,08 mm.

DOCUMENTO DE IDENTIFICACIÓN	
ITEM	DESCRIPCIÓN
Material	100% Policarbonato (PC)
Duración del material	10 años (en condiciones normales de uso)
Cumplimiento de Estándares	• ISO 7810 Identification cards - Physical characteristics ID-1 format. • ICAO Document 9303 Part 3, for Machine Readable Travel Documents (MRTD).

Tabla 1. Características técnicas del documento en policarbonato

Material Policarbonato

Los documentos de identidad estarán fabricados completamente en policarbonato. Desde comienzos de los años 90 el policarbonato es ampliamente reconocido por la mayoría de entidades que requieren la expedición de documentos de identidad, cómo el material más seguro para la elaboración de los mismos. Esto se debe a que durante la fabricación del documento se integran varias capas de policarbonato, utilizando para hacerlo máquinas especializadas que aportan la temperatura y la presión necesaria, en este proceso las capas se fusionan en un solo bloque.

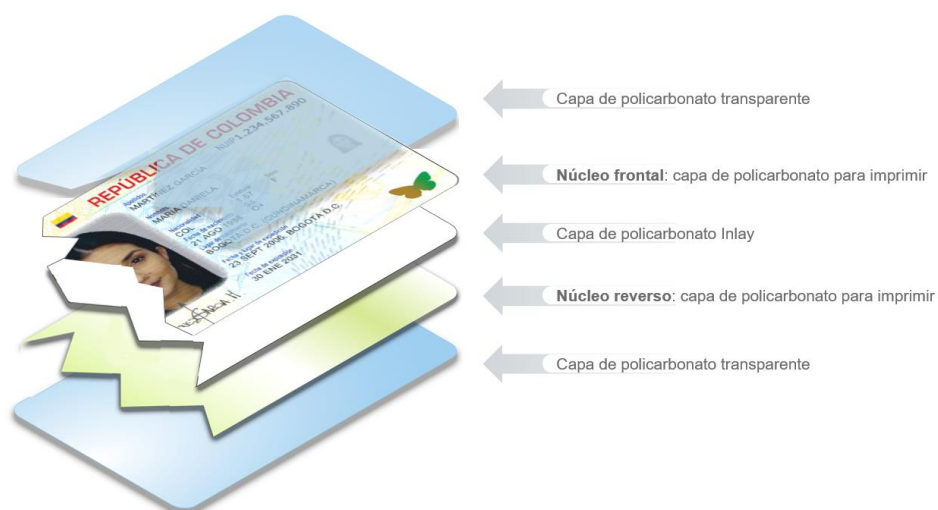


Ilustración 2. Estructura del cuerpo de la tarjeta en policarbonato

La alta seguridad del policarbonato radica en sus propiedades físicas: Es imposible separar dos capas de policarbonato que se han fusionado, lo cual deja evidente cualquier intento de separación. De este modo todas las características de seguridad, incluida la información personalizada grabada con láser, están protegidas por las capas exteriores de policarbonato del documento; a la vez que la personalización gráfica es irreversible y no puede alterarse, por cuanto la personalización de la información se realiza en las capas internas del documento.

Cuando la personalización de una tarjeta en policarbonato se hace con láser, se presenta una ventaja dentro del proceso la cual es que no se requiere ningún tipo de consumible como tintas, laminados, o cabezales de impresión, lo que en el largo plazo se traduce en un ahorro significativo para la **RNEC**.

Otra ventaja importante es que el policarbonato es el único material que soporta, además de las medidas de seguridad tradicionales, las medidas de nivel 1 más fuertes disponibles actualmente como relieves táctiles (positivo), medidas robustas que facilitan una rápida verificación de la autenticidad los documentos.

Finalmente, la utilización del policarbonato como material de producción de los documentos de identidad, brinda una mayor durabilidad al documento, que puede llegar hasta los diez (10) años, bajo condiciones normales de uso.

El uso normal excluye:

- Mantener el documento en climas extremos durante períodos prolongados de tiempo.
- La exposición del documento a la luz solar extrema, a la humedad (por ejemplo, el sudor, el agua y otros líquidos), o a agentes químicos agresivos.
- La exposición del documento a acciones mecánicas dañinas como flexión, estampado y la punción.

3.1.2 > Entregable

IDEMIA proveerá como entregable:

- Ochocientos veinticinco mil (825.000) unidades de tarjetas pre personalizadas en policarbonato para cédula de Identidad según diseño ya establecido por RNEC.

Los documentos de identidad estarán fabricados completamente en policarbonato, cumpliendo con las especificaciones técnicas establecidas por la **RNEC** para la producción de la cédula de seguridad personalizada en policarbonato.

Nota: *Esta entrega se hará en dos momentos; el primero se entregarán 200.000 tarjetas pre – personalizadas. La segunda entrega para la cantidad restante (625.000) se llevará a cabo en la fábrica de producción de documentos de IDEMIA en Europa. Dado que respecto a la capacidad actual de bodegaje de la entidad no es posible almacenar dicho material conforme las disposiciones de capacidad y exigencias de temperatura, humedad y seguridad requeridas para estos elementos, según la solicitud de la entidad (Ver documento Bóveda de Seguridad Fábrica RNEC). Para esta actividad se requiere la participación de una persona debidamente autorizada por la supervisión del contrato.*

3.2 > Ampliación de Capacidad para le Emisión de Unidades de Cédulas digitales.

En la actualidad, la **RNEC** cuenta con una infraestructura que está habilitada y personalizada para prestar servicios de gestión de identidad y emisión de documentos de identidad digital, la ampliación de la capacidad de generación de este documento digital implica ajustes en el sistema que actualmente existe para tal fin.

RNEC requiere el ajuste de la infraestructura actual de la gestión y expedición de identidad digital con el licenciamiento para aumentar su capacidad de generación y expedición de documentos digitales hasta ochocientos veinticinco mil (825.000) unidades adicionales a la capacidad actual instalada.

En particular, los ajustes más importantes son realizados al software, por cuanto se debe ampliar las capacidades del flujo de trabajo y esto tiene implicaciones en todo el sistema de gestión y de generación de documentos, sin embargo, la solución incluye, de ser necesario, la personalización, desarrollo y ajustes de software que se requieren en el sistema y la gestión para la expedición del documento de identidad digital.

La solución propuesta cuenta con las siguientes características:

- Ampliación de capacidad para emisión de hasta ochocientos veinticinco mil (825.000) unidades de Cédulas Digitales adicionales a la capacidad actual.
- Emisión de hasta ochocientos veinticinco mil (825.000) unidades de Cédulas Digitales adicionales a la capacidad actual.
- Licenciamiento para la generación de hasta ochocientos veinticinco mil (825.000) unidades de Cédulas Digitales adicionales a la capacidad actual.

3.2.1 > Generación de Cédulas Digitales adicionales

Esta parte de la presente oferta de IDEMIA incluye el ajuste del sistema actual de gestión y expedición de identidad digital con el licenciamiento para aumentar su capacidad de generación y expedición de documentos digitales en hasta ochocientos veinticinco mil (825.000) unidades adicionales a las actuales.

La siguiente ilustración muestra el flujo de trabajo de la generación y expedición de un documento digital.

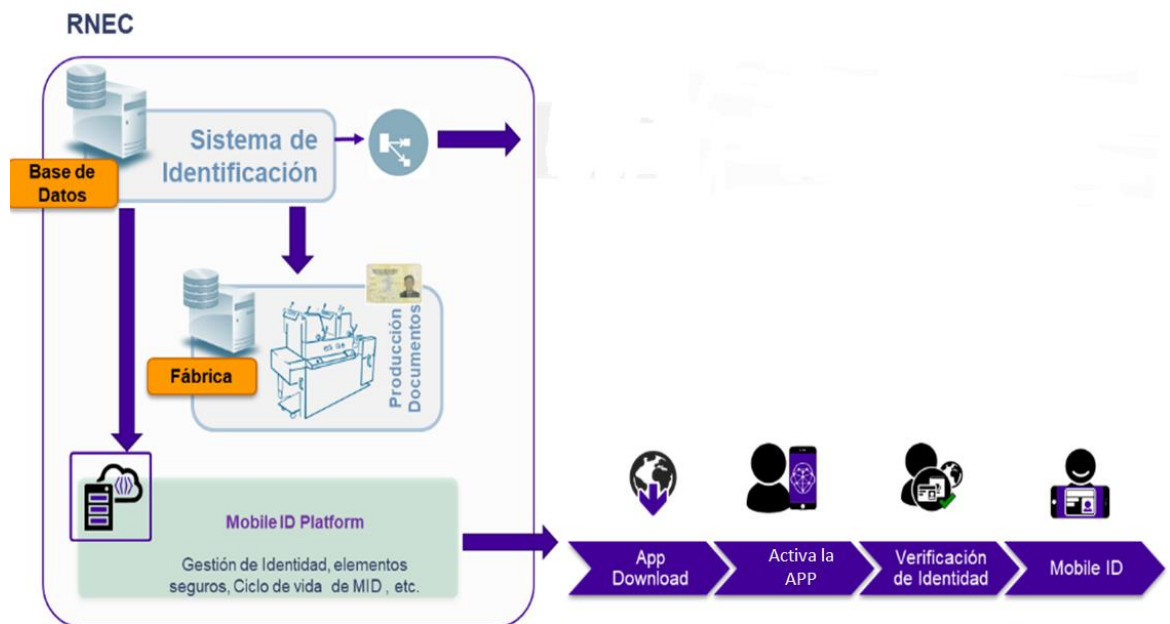


Ilustración 3. Grafica del flujo de trabajo de la identidad digital

3.2.2 > Entregable

IDEMIA proveerá los siguientes componentes:

- Licenciamiento para la generación de hasta ochocientos veinticinco mil (825.000) unidades de identidades digitales adicionales a la capacidad actual.

3.3 > Ampliación del flujo de transacciones del MBSS facial

La Registraduría Nacional del Estado Civil – RNEC, ha implementado un MBSS facial con el cual presta los servicios de autenticación para entidades públicas y privadas con las cuales tenga convenio o hayan llegado a un acuerdo de prestación de este servicio.

La RNEC ha considerado que el flujo transaccional actual del MBSS facial instalado debe ser ampliado por lo cual ha solicitado a IDEMIA realizar una oferta para implementar esta actividad.

Dadas las condiciones propias del MBSS, de ser escalable, se presenta esta oferta de ampliación de la transaccionalidad del MBSS facial con el siguiente contenido:

- Realización del proceso de escalabilidad tecnológica para ampliar el flujo de comparación 1:1 diaria (24 horas) del MBSS facial en seiscientos mil (600.000) transacciones, para lograr hasta un millón (1.000.000) de cotejos 1:1 diarios (24 horas) realizados por el MBSS facial.
- Licenciamiento para la escalabilidad tecnológica para ampliar el flujo transaccional en seiscientos mil (600.000) transacciones diarias (24 horas) del MBSS Facial (comparación 1:1), para lograr hasta un millón (1.000.000) de cotejos 1:1 diarios (24 horas) realizados por el MBSS facial.

Nota: La plataforma actual para el servicio de consultas 1:1 al MBSS facial cuenta con alta disponibilidad, entendiendo que ésta configuración está dispuesta en un solo sólo sitio en las condiciones actuales operativas del centro de cómputo de RNEC que administra IDEMIA.

Nota: La ampliación del flujo de transacciones del MBSS facial ofertada por IDEMIA será realizada en el sitio y con la infraestructura existente, sin incluir lugares alternos.

3.3.1 > Descripción de la solución

Actualmente la RNEC usa un Motor Biométrico MBSS (Multi Biometric Search Services) facial, el cual se encarga de realizar procesos de autenticación de personas usando para ello la biometría facial del individuo.

Este motor biométrico está instalado en las instalaciones de la RNEC con una infraestructura independiente del motor Biométrico de producción, con el objeto de no afectar el desempeño del sistema de gestión.

Con la implementación del MBSS facial se amplió la prestación de servicios de comparación facial para nuevos usos de entidades gubernamentales, así como de entidades privadas.

El Motor biométrico tiene diferentes funcionalidades, que pueden ser parametrizables acorde a las necesidades del cliente, el MBSS facial que se instaló tiene la función de:

- Comparación 1:1, conocido como proceso de autenticación de una persona, éste compara los rostros o huellas de un ciudadano, antes identificado, contra las biometrías que tiene dicha persona en el repositorio de datos biométricos para el mismo número de identificación.

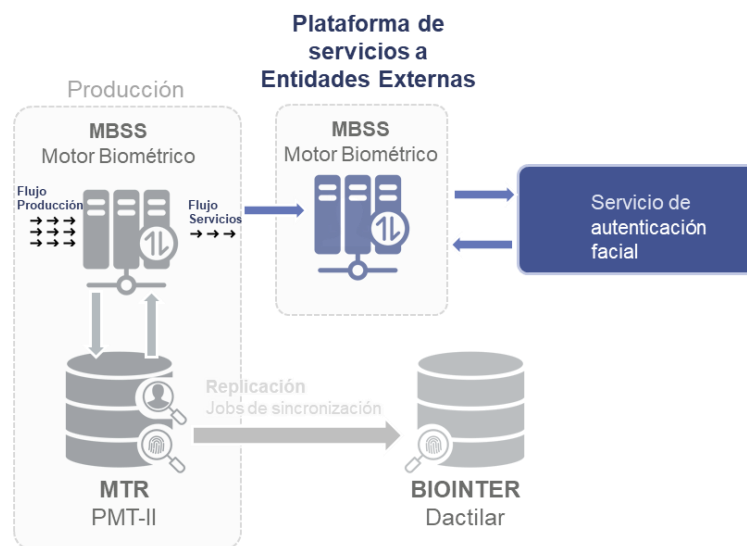


Ilustración 2. MBSS esquema de la funcionalidad. Imagen de referencia

3.3.2 > Funciones del MBSS facial

El motor biométrico MBSS facial de la RNEC cuenta con los siguientes servicios:

3.3.2.1 > Codificación

El proceso de codificación se realiza sobre las imágenes recibidas dentro de la consulta, se toma la imagen para extraer sus rasgos característicos, éstos son codificados y dicha codificación se refleja en una plantilla biométrica (este segundo paso se llama codificación o procesamiento de imagen). La plantilla biométrica junto con el NUIP es utilizada para

realizar dentro del MBSS facial una comparación, entre la información recibida y procesada y la información que se encuentra almacenada en el MBSS.

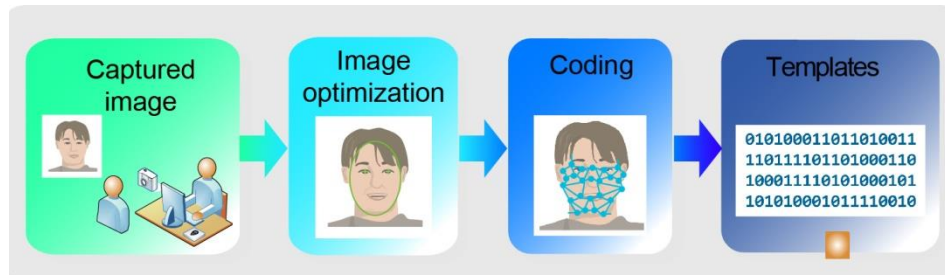


Ilustración 3. Ejemplo de proceso de codificación de rostros

Nota: La calidad de las fotos recibidas en el proceso de codificación es fundamental para obtener una plantilla con la mayor cantidad de minucias posibles, esto hace que, en procesos de autenticación posteriores, los resultados sean más efectivos.

3.3.2.2 > Proceso de Autenticación

Con la plantilla se realiza un proceso de comparación más conocido como autenticación, (comparación 1:1), la cual con la llave NUIP y Plantilla biométrica, realiza la búsqueda del registro que coincida con el NUIP y compara las plantillas biométricas (la de entrada y la almacenada).

Una vez realizada la comparación, el MBSS a través de sus servicios envía una respuesta al servicio solicitante, la cual puede ser HIT o NO HIT, con esta información los sistemas de terceros podrán realizar sus propios controles y con la información recibida realizar las acciones que haya programado para cada tipo de respuesta.

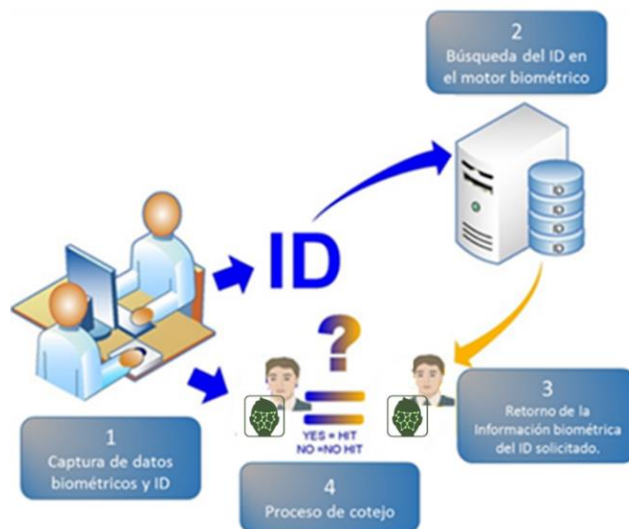


Ilustración 4. Proceso de autenticación del MBSS

3.3.2.3 > Almacenamiento

El producto MBSS facial, permite el almacenamiento de las plantillas biométricas (1 rostro) y un número de identificación único. Dentro de la solución del MBSS facial se implementó un proceso de sincronización de datos con el MBSS de producción del MTR, la información nueva que sea recibida por el proceso de gestión de identidad será transmitida al MBSS facial instalado, con esto se asegura que siempre se mantiene actualizada, estos procesos de sincronización son completamente automáticos.

3.3.3 > Dimensionamiento transaccional Diario

- La presente oferta incluye los ajustes necesarios en el sistema para la ampliación del flujo transaccional actual del MBSS facial en hasta seiscientos mil (600.000) comparaciones faciales 1:1 diarias (24 horas) adicionales, para lograr un flujo diario (24 horas) de hasta un millón (1.000.000) de cotejos 1:1 realizados por el MBSS facial.
- Se incluye el licenciamiento para ampliar el flujo transaccional en seiscientos mil (600.000) transacciones diarias (24 horas) del MBSS Facial (comparación 1:1), para lograr un flujo diario (24 horas) de hasta un millón (1.000.000) de cotejos 1:1 realizados por el MBSS facial.

3.3.4 > Entregable

- Licenciamiento para flujo transaccional de seiscientos mil (600.000) transacciones diarias (24 horas) del MBSS Facial (comparación 1:1) adicionales a las actualmente suministradas a la RNEC.

3.4 > Caso de Uso

Para fortalecer el uso de la identidad digital y el ecosistema de servicios digitales de la Entidad se propone la implementación y evolución de las siguientes funcionalidades:

- Portal web mobile de gestión de Cédula Digital en Smartphone para uso del ciudadano (portal web para uso en dispositivos móviles a través de un navegador web).
- Implementar el módulo de interoperabilidad permitirá a la RNEC proporcionar mecanismos de autenticación online mediante la cédula digital usando el protocolo OIDC.
- Evolución de la App móvil de verificación.

El detalle del alcance ofertado para las anteriores funcionalidades se explica en las subsecciones de este numeral.

La solución tecnológica incluye un módulo middleware de control y gestión de servicios, que permitirá incorporar funcionalidades desde la App de verificación y/o el portal web mobile para realizar funciones de verificación de identidad o autenticación.

El módulo middleware podrá ser invocado a través de un webview por parte de las soluciones que disponga la RNEC.

Nota: *La presente oferta no incluye API de servicios que exponga funcionalidades para integración desde interfaces externas/App para realizar gestión del ciclo de vida de la identidad digital de los colombianos. Las funcionalidades de ciclo de vida estarán disponibles en un módulo web que se puede embeber a través de WebView.*

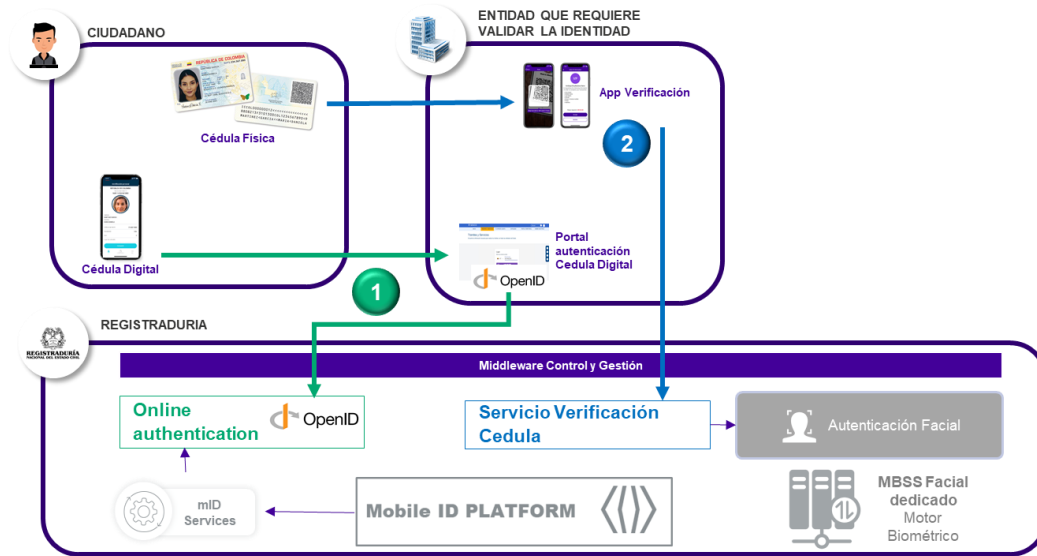


Ilustración 5. Ejemplo de arquitectura funcional propuesta

3.4.1 > Portal web de Gestión de Cédula Digital

Este módulo contempla el portal web mobile de gestión de cédula digital (portal web para uso en dispositivos móviles a través de un navegador web) para gestión de la identidad digital del ciudadano a través del cual se permitirá de manera segura y validando la identidad del ciudadano las siguientes funciones:

- Revocación de su identidad digital en smartphone (pérdida o robo)
- Cambio de dispositivo smartphone (la identidad digital solo estará activa en un dispositivo)
- Generación de nuevo token para registro. Con el fin de mejorar el servicio de registro, esto se realizará a través de un portal web mobile mediante el cual el usuario pueda solicitar un nuevo enlace (token) con validación de seguridad para asegurar la identidad del solicitante.
- La RNEC tendrá la posibilidad de llamar este portal web desde una aplicación móvil (portal web embebido WebView).

Nota: Actualmente el proceso de validación y registro (onboarding) para la identidad digital se realiza de manera presencial cuando el documento en policarbonato es entregado en la oficina de la RNEC por el solicitante del documento, en este proceso se envía un enlace (token) con una validez determinada de 48 horas.

Estas funcionalidades contarán con mecanismos y reglas de negocio que permitirán la validación de la identidad asegurando el uso de las mismas y garantizando la identidad autosoberana (self-sovereign identity) fortaleciendo los canales de atención de la solución de Identidad Digital de la Entidad alineado con la masificación del uso de la Cédula Digital.

3.4.1.1 > Entregable

- Documentación de especificaciones de Portal Web mobile de gestión de Cédula Digital en Smartphone.
- Entrega de licencia de uso de Portal Web mobile de gestión de Cédula Digital en Smartphone para el ciudadano.
- Portal web mobile para gestión de Cédula Digital en Smartphone con las funcionalidades compatibles de acuerdo a la actualización progresiva de los usuarios existentes.

3.4.2 > Módulo de interoperabilidad

Este módulo permitirá a la Registraduría Nacional del Estado Civil proporcionar mecanismos de autenticación online mediante la cédula digital usando el protocolo OIDC (OpenID Connect) que a su vez está alineado con los mecanismos de interoperabilidad requerido por el ecosistema de servicios digitales que se encuentran actualmente reglamentados en el país. Este módulo contara con las siguientes capacidades:

- Una capacidad de atención transaccional y autenticación hasta quinientas mil (500.000) transacciones diarias (24 horas) de autenticación Online hacia terceros usando los mecanismos habilitados basado en el protocolo OIDC y que permita escalabilidad.
- Disponibilidad: El modulo se instalará en el sitio central de Registraduría contando con mecanismos de disponibilidad del sitio.
- Integración: Contará con los mecanismos basados en protocolo OIDC y la documentación necesaria para la integración por parte de terceros para el uso de la Cédula Digital.

Esta funcionalidad permitirá la integración de casos de uso donde se requiera la Cédula Digital como mecanismo de autenticación por parte de entidades externas, para lo cual las entidades externas deberán realizar la integración de las interfaces en los portales de acuerdo al documento de integración que será generado como parte de la implementación de la solución.

3.4.2.1 > Entregable

- Módulo que permitirá a la RNEC proporcionar mecanismos de autenticación online mediante la cédula digital usando el protocolo OIDC.
- Licenciamiento para flujo transaccional hasta quinientas mil (500.000) transacciones diarias (24 horas) de autenticaciones a través del mecanismo OIDC (10 paquetes de 50.000 autenticaciones).

3.4.3 > App móvil de Verificación

Como parte de la solución de identidad digital implementada en el año 2020, se desarrolló una aplicación App Verificación para validar la autenticidad de la identidad digital presentado en un teléfono móvil. Este proceso permite establecer una comunicación segura entre dispositivos, la cual habilita a la App de verificación para recibir datos auténticos emitidos por la **RNEC**.

La App podrá ser utilizada por entidades públicas y privadas que deseen utilizar esta funcionalidad y que previamente hayan sido autorizadas por la **RNEC** para el uso del mismo.

Las evoluciones de la App de verificación permitirán ampliar las funcionalidades de verificación para:

- Permitir el uso de flujo por parte de las entidades externas (se realiza control para permitir el acceso a entidades de acuerdo a un perfil de uso definido) para transacciones de verificación.
- Permitir realizar la verificación del documento digital, escaneando el código QR dinámico generado en la App Cédula Digital del ciudadano en el smartphone.
- Funcionalidad que permitirá realizar la verificación de la persona portadora del documento físico, a través de la lectura de la zona de lectura mecánica (MRZ) y de un proceso de autenticación facial con el sistema central. La zona MRZ contiene los datos biográficos necesarios para esta función de verificación y al mismo tiempo su lectura permite mayor inclusividad social para el uso de la aplicación.

Nota: *La naturaleza del servicio de verificación requiere consultar el sistema central de RNEC como autoridad de confianza fuente de información para realizar la verificación de la biometría facial de la persona, lo que solamente se logra mediante el uso online de la App de verificación.*

Nota: *La función de verificación de la persona portadora del documento físico solo podrá ser usada en los dispositivos móviles que cumplen con las características mínimas requeridas en este documento, es decir mínimo sistemas operativos iOS 13 o*

superior y Android 10 o superior, con capacidad de una cámara posterior de mínimo 10 megapíxeles.



Ilustración 6. Ejemplo de flujo de uso de la evolución de la app de verificación biométrica

3.4.3.1 > Entregable

- Documentación de especificaciones de la funcionalidad de verificación del documento físico.
- Modulo para verificación del documento físico a través de la lectura de MRZ y autenticación facial.

3.4.4 > Evolución de los sistemas operativos de smartphone (ANDROID – iOS)

Como parte de la evolución de los sistemas operativos de smartphone (Android e iOS), se realizará la actualización de la aplicación móvil del ciudadano permitiendo su funcionalidad en la siguiente versión de sistemas operativos iOS y Android, así mismo con el objetivo de mantener los niveles de seguridad la evolución de los diferentes sistemas operativos, el

funcionamiento de las aplicaciones será para un uso de iOS 13 o superior y Android 9 o superior.

La App móvil del ciudadano incorporará control de versionamiento de la app, entendido como la solicitud de actualización de la versión de la App para permitir el uso de la misma cuando la versión en la tienda de aplicaciones móviles sea detectada como superior a la versión instalada en el dispositivo móvil.

Las versiones de OS soportadas pueden evolucionar en el tiempo según las recomendaciones de seguridad de Google y Apple. La App de cédula digital estará disponible en Google Play Store y Appstore.

4 / Suministro de EIS para el sistema de atención integrado de identificación

El presente documento técnico que describe los productos Estación Integrada de Servicios (EIS), equipos que la RNEC adquirirá para el fortalecimiento de la plataforma de identificación en la ejecución de procesos de enrolamiento.

Los productos y servicios a prestar son:

Productos:

- EIS: Estación Integrada de Servicios, compuesta por hardware (PC y dispositivos) y una aplicación web que permite la captura de información de los ciudadanos, quienes, a través de este proceso, solicitan a la Registraduría Nacional del Estado Civil documentos de identidad tipo tarjeta o cédula. Las siguientes cantidades son consideradas en la presente:
 - EIS fijas (254 unidades):

Los componentes de la EIS fija están relacionados en el numeral 4.1.2 >Componentes de Hardware.

Servicios:

Se prestarán los servicios de alistamiento y entrega en Bogotá, de las estaciones integradas de servicios EIS.



Ilustración 7. Etapas del servicio de alistamiento y entrega

- Nota:** *La entrega de los equipos adquiridos por la RNEC se realizará en su sitio central, en la ciudad de Bogotá. La presente oferta no incluye servicios de despliegue de estaciones EIS.*
- Nota:** *Las estaciones EIS que serán entregadas por IDEMIA como parte de los alcances de esta oferta serán operativas únicamente dentro del territorio nacional de Colombia.*
- Nota:** *Vale la pena aclarar que la Implementación del sistema de atención integrado de identificación, se ejecuta secuencialmente desarrollando las actividades de provisión de hardware, alistamiento y despliegue nacional. Esta oferta incluye exclusivamente la provisión de hardware para EIS y alistamiento de las mismas.*

4.1 > EIS: Estación Integrada de Servicios

La Estación Integrada de Servicios (EIS) es un sistema diseñado exclusivamente para cumplir los requerimientos de la RNEC, compuesto de un equipo de cómputo y un conjunto de periféricos conectados, que trabajan en un ambiente web, y acceso a la URL de la aplicación “EIS”; basada en el navegador de Google Chrome.

La EIS físicamente está compuesta por un equipo de cómputo que soporta la aplicación y el funcionamiento de la misma, una pantalla adicional visible al usuario que muestra la información capturada durante el proceso y, de esta manera, el ciudadano puede verificar inmediatamente la calidad de la información capturada durante el trámite, un MorphoTop que permite capturar de manera digital las diez huellas dactilares, un MSO para efectuar autenticación dactilar y biología de acceso al equipo, una cámara web para la captura de la fotografía digital del usuario y su uso posterior para la ejecución de autenticación facial, un pad de firmas donde se captura digitalmente la firma manuscrita y un kit de iluminación compuesto por un telón, una luz led y un soporte necesarios para su instalación en sitio.

Los componentes de hardware que hacen parte de la estación, permiten el uso de la aplicación web denominada EIS, con la cual se realiza el proceso de captura de la información, ejecutando funciones específicamente desarrolladas para la RNEC entre otras:

- Módulo de enrolamiento.
- Módulo de autenticación facial.
- Módulo de autenticación dactilar.
- Módulo de reportes.

Nota: *El software de las Estaciones Integradas de Servicio, EIS, estará en idioma español.*

4.1.1 > Funciones



Ilustración 8. Pantalla de las funciones de una EIS

1. Enrolamiento

Este módulo permite capturar la información del individuo, preparar la información para iniciar su proceso dentro del flujo de trabajo en las instalaciones centrales de la Registraduría y por último generar (personalizar un documento físico) el documento de identidad, que puede ser una tarjeta de identidad o una cédula de ciudadanía a un colombiano.

El proceso de enrolamiento sigue unos pasos lógicos y secuenciales especialmente diseñados para la RNEC con lo cual se consigue la captura de la información del ciudadano, el proceso de enrolamiento captura la siguiente información:



Ilustración 9. Proceso de enrolamiento

- Captura de Información Alfanumérica: Muestra información alfanumérica, preparación de documento, datos personales y datos de contacto.
- Recaudo: Muestra los campos correspondientes al comprobante de pago del trámite de identificación.
- Captura Dactilar: Fase donde se realiza la captura de las diez huellas dactilares, tiene un campo para ingresar una señal particular si es necesario.
- Captura Facial: Fase donde se realiza la captura de la fotografía, tiene un campo para ingresar una señal particular si es necesario.
- Firma: Fase donde se realiza la captura en formato digital de la firma manuscrita o, en caso de ser necesario, omitirla.
- Resumen de Datos: Fase donde se exponen todos los datos alfanuméricos y biográficos para ser revisados por el usuario al cual se le realiza la preparación por el operador.
- Contraseña, se muestra la contraseña en pantalla que es la parte final del proceso.

Cada uno de los pasos del proceso anteriormente descrito se realiza en pantallas independientes con el objeto de mantener enfocado al operador en cada uno de los pasos, pero consecutivas y enlazadas por cada registro; al finalizar el proceso de enrolamiento se despliega una pantalla como la siguiente:

Oficina: DEJ - BOGOTÁ D.C.-INFORMACION CIUDADANA
Usuario: 3087328
Fecha y hora: 07-JUL-2020 14:37:58
Perfil OPERADOR
Versión: 1.3.8

ESTACIÓN INTEGRADA DE SERVICIOS - EIS

100% INICIAR TOTAL

INFORMACION ALFANUMERICA RECAUDO CAPTURA DACTILAR CAPTURA FACIAL FIRMA RESUMEN DE DATOS

PREPARACIÓN DE DOCUMENTO
TIPO DE SOLICITUD: **DUPLICADO CC**
FECHA DE PREPARACIÓN: **07-JUL-2020**
OFICINA DE PREPARACIÓN: **DEJ - BOGOTÁ D.C.-INFORMACION CIUDADANA**

DATOS PERSONALES
NÚMERO DE DOCUMENTO: **DD-MM-AAAA**
PRIMER APELLIDO: **PRIMER APELLIDO**
PRIMER NOMBRE: **PRIMER NOMBRE**
SEGUNDO NOMBRE: **SEGUNDO NOMBRE**
FECHA DE NACIMIENTO: **02-ABR-1983**
PAÍS DE NACIMIENTO: **COLOMBIA**
DEPARTAMENTO DE NACIMIENTO: **ATLANTICO**
MUNICIPIO DE NACIMIENTO: **BARRANQUILLA**
CORREGIMIENTO DE NACIMIENTO: **BARRANQUILLA**
NOMBRE DE LA MADRE: **NOMBRE**
NOMBRE DE LA MADRE: **NOMBRE**
SEXO: **FEMENINO**
ESTATURA (CM): **153**
GRUPO SANGUÍNEO: **O+**
SEÑAL PARTICULAR: **NINGUNA**

DATOS DE CONTACTO
DIRECCIÓN DE RESIDENCIA: **AU 45 5 654 4 45 SJHSJSJS -/ ACHI, BOLIVAR, COLOMBIA**
TELÉFONO: **3216549873**
CORREO ELECTRÓNICO: **correo@gmail.com**
OFICINA DE ENTREGA DEL DOCUMENTO: **DEJ-BOGOTÁ D.C.-INFORMACION CIUDADANA**

DATOS BIOMÉTRICOS
CAPTURA DACTILAR
PULGAR DERECHO, INDICE DERECHO, MEDIO DERECHO, ANULAR DERECHO, MEÑIQUE DERECHO
PULGAR IZQUIERDO, INDICE IZQUIERDO, MEDIO IZQUIERDO, ANULAR IZQUIERDO, MEÑIQUE IZQUIERDO
FOTO CAPTURADA
FIRMA CAPTURADA

ANTERIOR CONFIRMAR CANCELAR

Ilustración 10. Pantalla del proceso de enrolamiento

Nota: Para enrolamiento de colombianos nacidos en el exterior, dado el caso en el que el lugar de nacimiento no exista en el sistema, la RNEC realizará su creación e IDEMIA realizará la actualización en los sistemas a que haya lugar.

2. Autenticación Facial

Este módulo permite realizar una autenticación 1:1 de manera independiente a un usuario; requiriendo conocer el número de identificación y la presencia física de quien se pretende autenticar para capturar la fotografía de su rostro.

El proceso de autenticación facial es un proceso muy rápido que se realiza mediante el ingreso del NUIP y la captura fotográfica del rostro del usuario con la cámara web, la estación EIS envía al motor multibiométrico MBSS esta información (NUIP y fotografía) encriptada, el cual realizará una búsqueda cerrada (1:1) y en pocos segundos devuelve un resultado a la estación, el cual puede ser “Autenticación Exitosa” o “Autenticación NO Exitosa”; por tanto, el sistema determina si la persona que se presenta y que aduce ser titular de dicho NUIP lo es o NO.

Oficina: DEJ - BOGOTÁ D.C. - INFORMACIÓN CIUDADANA
Perfil: OPERADOR
Versión: 1.3.8

REGISTRADURÍA

ESTACIÓN INTEGRADA DE SERVICIOS - EIS

AUTENTICACIÓN FACIAL

Número de Documento (NUIP/NIP):

FOTO EN VIVO

Estado del Servicio: CONECTADO
Estado del Dispositivo: TRABAJANDO
Estado de la Captura: TERMINADO

Foto con calidad óptima de acuerdo a validación de normas ICAO.

FOTO CAPTURADA

INFORMACIÓN ICAO:					
EXPOSICIÓN:	OK	ILUMINACIÓN:	OK	ENFOQUE:	OK
OJOS ABIERTOS:	OK	LONG. FRONTAL COMPLETA:	OK	ANCHO FRONTAL COMPLETO:	OK
POS. HORIZ. COMPLETA:	OK	IMG. FRONTAL COMPLETA:	OK	RESOL. MÍN. FRONTAL:	OK
CARA FRONTAL COMPLETA:	OK	POS. VERT. COMPLETA:	OK	REFLEJO DE GAFAS:	OK
PUNTOS FACIALES:	OK	DINÁMICA BAJA:	OK	BOCA CERRADA:	OK
NO FRONTAL:	OK	FONDO UNIFORME:	OK	COLOR NATURAL:	OK

REINICIAR CAPTURA

UNIRSE CANCELAR

AUTENTICAR

Ilustración 11. Autenticación Facial Exitosa.



Filio W. PÉZ - BOGOTÁ D.C. - INFORMACIÓN CIUDADANA
 Unidad: 3057228

Fecha y hora: 05-JUL-2020 13:43:53
 Perfil: OPERADOR
 Versión: 1.3.8

ESTACIÓN INTEGRADA DE SERVICIOS - EIS




AUTENTICACIÓN FACIAL

AUTENTICACIÓN NO EXITOSA

[Visualizar resultado de la autenticación](#)


La foto no coincide con la almacenada para el número de documento consultado. A continuación, los datos pertenecientes al número de documento:

DATOS ALFANUMÉRICOS
 TIPO DE DOCUMENTO
 CEDULA DE CIUDADANIA
 PRIMER APELLIDO
 Primer Apellido
 PRIMER NOMBRE
 Primer Nombre
 FECHA DE NACIMIENTO
 10-MAY-1980

NÚMERO DE DOCUMENTO
 Número de documento
 PARTICULA
 SEGUNDO NOMBRE
 Segundo Nombre
 LUGAR DE NACIMIENTO
 CUNDINAMARCA - BOGOTÁ D.C.

FECHA DE EXPEDICIÓN
 DD-MM-AAAA
 SEGUNDO APELLIDO
 Segundo Apellido
 SEXO
 MASCULINO
 SEÑAL PARTICULAR

DATOS BIOMÉTRICOS

 Foto Documento

 Foto Capturada

FINALIZAR

Ilustración 12. Autenticación facial no exitosa.

3. Autenticación Dactilar

Este módulo permite realizar una autenticación 1:1 de manera independiente a un usuario; para esto se requiere conocer el número de identificación y la presencia física de quien se pretende autenticar para capturarlo la o las huellas dactilares, máximo dos huellas.

El proceso de autenticación dactilar es un proceso muy rápido que se realiza mediante el ingreso del NUIP y la captura de la o las huellas dactilares del usuario con el MSO, la estación EIS envía al motor multibiométrico MBSS esta información (NUIP y huella(s)) encriptada, el cual realiza una búsqueda cerrada (1:1) y que en pocos segundos devuelve un resultado a la estación “Autenticación Exitosa” o “Autenticación NO Exitosa”, es decir, es el titular del NUIP o NO es el titular del NUIP.

Ilustración 13. Pantalla de autenticación dactilar

Si el resultado del proceso de autenticación dactilar es “Autenticación Exitosa”, aparecerá un mensaje de color verde en la parte superior; esto quiere decir que el usuario al cual se le capturó la o las huellas es el titular del NUIP.

Al final de un proceso exitoso mostrará la última foto utilizada para expedir un documento para que el operador haga una validación adicional con dicha imagen.

Ilustración 14. Autenticación dactilar exitosa

4. Reportes

Este módulo permite generar de manera consolidada o detallada, en formato digital (Excel o PDF), un reporte de las actividades realizadas por los diferentes usuarios en las estaciones EIS, es decir, reportes de Autenticación, Enrolamiento y Auditoría (Login – Logout).

Si se generan de manera detallada, se obtiene la información de un periodo de tiempo hasta de un mes, con el objetivo de entregar información que pueda ser manejada fácilmente; si se genera un reporte consolidado, éste permite obtener la información de un periodo de tiempo hasta de seis meses, estos reportes pueden ser descargados al equipo para ser revisados y analizados; en caso de ser necesario pueden ser impresos.

Existen tres tipos de reportes:

- **De autenticación:** El reporte de autenticación obtiene la información de las autenticaciones realizadas en las estaciones EIS, bien sea Autenticación Dactilar, Autenticación Facial o ambas autenticaciones en el mismo reporte; conforme a los filtros o parámetros indicados y el perfil del usuario que genere el reporte.
- **De enrolamiento:** El reporte de enrolamiento obtiene la información de los trámites de identificación realizados en las estaciones EIS, bien sea de tarjeta de identidad o cédula de ciudadanía, en todos los tipos de expedición (primera vez, duplicado, renovación y rectificación); todo en el mismo reporte, y conforme a los filtros o parámetros indicados y al perfil del usuario que lo genere.
- **De login / Logout:** El reporte de login logout, indica en el mismo la cantidad de sesiones iniciadas por los diferentes usuarios de las estaciones EIS, la hora de conexión y detalles adicionales que permiten la identificación del usuario y el lugar de conexión de la sesión.



Ilustración 15. Tipos de Reportes

4.1.2 > Componentes de Hardware

La estación integrada de servicios cuenta con los siguientes elementos:



Ilustración 16. Imagen referencial de EIS en ambiente operativo

- PC: equipo de escritorio con sus dispositivos mouse, teclado y pantalla.
- Webcam: cámara Web para la captura de la foto
- Captor biométrico multidactilar MorphoTop: con el cual se realiza la captura de la información biométrica dactilar de los ciudadanos en formato 4-4-2.
- Captor biométrico unidactilar MSO: el cual es utilizado para el proceso de ingreso y autenticación a la aplicación EIS.
- Pad de firmas: para la captura de la imagen de la firma de los ciudadanos.
- Monitor (adicional): conectado al pc donde se realiza el proceso de enrolamiento y sobre el cual se despliega la información capturada al ciudadano, para que, en tiempo real, el usuario valide la calidad de la misma.
- Kit de Iluminación: elementos como soporte de cámara, luz led para fotografía y fondo, para asegurar una captura óptima de la foto.

Componentes de la EIS fija	
	Computador de escritorio Homologado para compatibilidad de operación con el software de la EIS Procesador Intel® Core™ i7 de 10a generación, RAM 16GB, disco de estado sólido SSD de 512 GB, SO Windows 11 Pro 64bit. Pantalla Full HD 21.5 pulgadas
	Segundo monitor de 21,5 pulgadas Resolución 1920 x 1080 (Full HD) Puertos USB para conexión de pantalla
	Webcam Cámara Logitech C920S
	Captore biométricos MorphoTop™ IDEMIA, MTOP 2020
	Captore biométricos MSO™ IDEMIA, MSO 1300
	Pad de firmas Wacom STU430, Tableta LCD de firma
	Kit de Iluminación Luz con control de iluminación, con control de apagado/encendido. Paral para luz y cámara, ajustable en altura, con accesorio para fijación a mesa. Fondo blanco para garantizar la calidad y uniformidad del fondo de la fotografía.

Tabla 2. Componentes de la EIS fija

Nota: Las características del computador de escritorio de la EIS, han sido dimensionadas por diseño para trabajar con el software de la EIS. Se recomienda que no se realice el uso de aplicaciones adicionales en el mismo computador con el fin de garantizar su operación correcta.

Nota: Es importante aclarar que las referencias y marcas descritas podrán ser de distintas referencias iguales o de mejores características.

4.1.3 > Entregables

La siguiente tabla contiene el detalle de los entregables de este componente

ITEM	Detalle	Cant.
EIS fijas	Entrega en la ciudad de Bogotá de estaciones EIS, cada una compuesta de: PC de escritorio, segundo monitor, webcam, MorphoTop, MSO 1300, pad de firmas y kit de iluminación.	254
Alistamiento de EIS fija	Servicio de alistamiento de estación EIS fija	254

Tabla 3. Entregables de EIS fijas en sitio central

Nota: Se recomienda que los canales de comunicación para las estaciones integradas de servicios EIS sean cada uno de 2 Mbps (Mega bits por segundo), con un mínimo de 1.8 Mbps.

4.2 > Servicios para EIS

La presente incluye los siguientes servicios para EIS fijas.

4.2.1.1 > Alistamiento

El objetivo del proceso de alistamiento es entregar las estaciones EIS fijas completamente operativas y funcionales, para lo cual se ejecutarán actividades tales como:

- Desembalaje del hardware y verificación de estado.
- Instalación de las aplicaciones.
- Pruebas de funcionalidad.
- Embalaje del equipo.
- Entrega en sitio central Bogotá.

La EIS permiten ajustar de manera centralizada los niveles de validación de parámetros ICAO para la toma de fotografía por oficina de la RNEC. Aprovechando esta funcionalidad, IDEMIA realizara procesos de ajuste de los parámetros por oficinas, basada en las directrices definidas por la entidad.

Nota: *La presente oferta no incluye servicios asociados con el despliegue de las EIS que serán entregadas en Bogotá ni servicios de soporte remoto o en sitio relacionados con despliegue de estaciones EIS.*

4.3 > Entregable

IDEMIA hará entrega de los siguientes productos y servicios.

- 254 unidades de EIS fijas.
- Servicios de alistamiento para las 254 EIS fijas.
- Servicio de entrega en las instalaciones de RNEC en la ciudad de Bogotá de las 254 EIS fijas.

5 / Mantenimiento y sostenibilidad de la plataforma tecnológica PMT II del sistema de identificación y registro civil a nivel nacional

El proyecto de inversión “Mantenimiento y sostenibilidad de la plataforma que soporta los sistemas de Identificación y Registro Civil PMT II” tiene como objetivo general prestar de manera oportuna y eficiente el servicio de registro civil e identificación a los colombianos.

5.1 > Alcance del proyecto

El mantenimiento y sostenibilidad propuesto por IDEMIA para la infraestructura que soporta los sistemas de Identificación y Registro Civil PMT II de la RNEC cumple con los siguientes dos objetivos específicos:

- Soportar la infraestructura de Registro Civil y de Identificación.
- Soportar la generación de los documentos de identificación.

Para el cumplimiento de cada uno de estos objetivos, IDEMIA ejecutará las siguientes actividades:

Objetivo 1: Soportar la infraestructura de Registro Civil y de Identificación.

Actividades

1. Realizar mantenimiento de la plataforma PMT II.
2. Ofrecer la disponibilidad de la plataforma PMT II.
3. Disponer de un soporte técnico a usuarios.

Objetivo 2: Soportar la generación de los documentos de identificación.

Actividades

4. Cargar información del trámite del colombiano.
5. Validar información del trámite.
6. Producir documentos de identificación.

Las siguientes secciones explican los alcances de los servicios de mantenimiento y sostenimiento que serán ejecutados hasta el 31 de diciembre de 2.022.

Nota: *Los tiempos referenciados para las actividades 1, 2, 3, 4 ,5 y 6 de este servicio son los máximos, los que podrán modificarse de común acuerdo entre IDEMIA y la supervisión del contrato dentro del primer mes de ejecución del mismo.*

5.2 > Actividades de Mantenimiento y Sostenimiento

Desde la implementación del Proyecto de Modernización Tecnológica PMT II, se ha dado mantenimiento correctivo, sostenibilidad y soporte del sistema, permitiendo la continuidad operacional en la prestación de los servicios misionales de la RNEC a los colombianos. Así mismo, atendiendo las necesidades de actualización de la plataforma, se han emprendido acciones de sostenimiento asociadas con la renovación de hardware, software y aplicativos que componen la solución.

En el presente se incluyen actividades de mantenimiento y sostenibilidad de la plataforma PMT II, hasta el 31 de diciembre de 2.022. Para la ejecución de las actividades a contratar se considera a la Registraduría Nacional del Estado Civil (RNEC), como responsable del Registro Civil y la Identificación de los colombianos.

El alcance incluido en el presente documento de IDEMIA para la plataforma tecnológica del Sistema de Identificación y Registro Civil de RNEC, incluye la siguiente infraestructura y funcionalidades:

- Sistema de Registro Civil para el procesamiento de RCN, RCM y RCD a nivel nacional que incluye:
 - Módulo DCU para la solicitud de documentos de identificación
 - Sistema de Gestión Electrónica de Documentos GED de Registro Civil
 - Línea de digitalización
 - Base de datos central de registro BDR

- Réplica total de la BDR
- Servicios Web
- Interfaces internas y externas
- Un sistema de identificación compuesto por:
 - Almacenamiento con capacidad de hasta 60 millones de personas
 - Sistema central para la validación automática de datos biográficos y biométricos (flujos de trabajo establecidos de 48.000 1:N por día en huellas y fotografías y 100.000 1:1 por día en huellas y/o fotografías.)
 - Sistema de Réplica I, BIOINTER de Identificación
 - Fábrica de documentos (cédulas de ciudadanía en Teslin y policarbonato y tarjetas de identidad en Teslin)
 - Sistema de gestión electrónica de documentos GED de Identificación
 - Sistema HLED Web MorphoTablet™
 - Sistema de Seguimiento y Control SSC
 - Sistema de Web Service
 - Estación Integrada de Servicios – EIS (fijas y móviles adquiridas en los años 2019, 2020, 2021 y 2022)
 - Aplicación móvil para reimpresión de documentos en Teslin
 - Analítica estratégica de datos
 - Interfaces internas y externas.
 - Plataforma de cédula de seguridad personalizada en policarbonato, (IDPS) para producción de cédula de ciudadanía de seguridad personalizada en policarbonato.
 - Plataforma para la cédula de ciudadanía digital, Aplicación móvil para la cédula de ciudadanía digital y Aplicación móvil para verificación de cédula de ciudadanía digital.
 - Plataforma de servicios de autenticación facial para entidades externas - MBSS facial. Se garantiza la disponibilidad actual con que cuenta la RNEC adicional a la cantidad transaccional a ser adquirida y que hacen parte de la presente oferta.
- Infraestructura y funcionalidades suministrados por IDEMIA para el Sistema de Identificación y Registro Civil de RNEC que inicien su operación productiva durante el año 2022, limitadas a las siguientes:
 - Estación Integrada de Servicios – EIS (fijas y móviles entregadas en operación)

En las siguientes secciones se describe los servicios de IDEMIA para cada una de las actividades que se han propuesto anteriormente.

5.2.1 > Actividad 1: Realizar mantenimiento de la plataforma PMT II

5.2.1.1 > Subactividad 1: Realizar mantenimiento correctivo de la plataforma PMT II

Para la prestación del servicio de mantenimiento correctivo IDEMIA cubre todos los equipos, proporcionados por IDEMIA, que hacen parte de la solución integral que soporta los sistemas de Identificación y Registro Civil, los cuales serán relacionados y entregados por la Entidad en el inventario de equipos y sus correspondientes hojas de vida al iniciar el contrato. Los equipos que requieran mantenimiento correctivo serán objeto de los procesos previamente definidos en conjunto con la entidad, para encontrar una solución dentro de los tiempos definidos en el documento técnico de IDEMIA.

IDEMIA realizará el mantenimiento correctivo así como el soporte técnico del software y hardware con cobertura nacional, dando sostenibilidad a la plataforma de la solución PMT II instalada en el marco de los contratos 057 de 2005, 074 de 2010, 091 de 2011, 068 de 2012, 151 de 2012, 255 de 2013, 003 de 2016 y 006 de 2017, 012 de 2018, 018 del 2019, 002 de 2020, 014, 052, 065, 104 del 2021, 006 y 033 del 2022, para lo cual se dispondrá de un lugar y una infraestructura debidamente adecuada en la ciudad de Bogotá, que garantizará una correcta ejecución de los mantenimientos correctivos de hardware y software y apropiará un stock de repuestos, directamente o a través de sus proveedores, a fin de garantizar la actualización permanente de los eventos que requieren tratamiento correctivo desde la generación de la solicitud en la Registraduría y la trazabilidad de las actividades de recepción y despacho del ciclo que surte el equipo hasta su entrega definitiva, se contará con una herramienta adecuada para tal fin.

La actividad de mantenimiento correctivo proporcionará la sostenibilidad a las bases de datos y aplicaciones web actuales e incluirá dentro de sus actividades aquellas implementadas en la ejecución de contratos realizados con la RNEC nombrados anteriormente.

NOTA: Para las actividades de soporte y disponibilidad consideradas en la presente, nos permitimos precisar que la impresora XEROX DC 5000 que representa una de las dos líneas de producción de documentos de identidad en Teslin y que se encuentra ubicada en la fábrica de documentos de la Entidad, ésta llegó al fin del periodo de soporte desde el pasado 31 de diciembre de 2019. Esto significa que el soporte técnico directo brindado por el fabricante a través de su representante en Colombia, tiene fuertes e impactantes limitaciones. En este sentido, destacamos que ni el fabricante ni su representante en Colombia garantizan el abastecimiento de partes, repuestos y suministro para la impresora referida; por lo tanto, se cuenta con la disponibilidad sólo de aquellas partes que se consigan en el mercado; en consecuencia, las acciones de IDEMIA frente a un eventual incidente que afecte la operación y disponibilidad de esta máquina estará

limitado por dichas condiciones y limitaciones, ajenas a la actividad y control de IDEMIA. Los consumibles utilizados en la impresión de la mencionada impresora están a cargo de la Registraduría Nacional del Estado Civil y en caso de faltar estos la disponibilidad de esta máquina en la línea de producción estará limitada por dichas condiciones y limitaciones, ajenas a la actividad y control de IDEMIA.

IDEMIA hará uso de una plataforma de TESTBED, la cual estará ubicada en las oficinas centrales de IDEMIA con el objetivo de llevar a cabo las pruebas técnicas para los casos en que se requiera realizar diagnóstico de funcionamiento de alguno de los módulos de los sistemas de identificación y registro civil y/o de la plataforma tecnológica que los soporta a nivel de hardware y software.

5.2.1.2 > Subactividad 2: Mantenimiento plataforma Cédula Digital

El sistema de Identidad Digital, consiste en la infraestructura de hardware y software que permite la generación y expedición de una cédula de identidad digital con capacidad inicial de 50.000 unidades, la que fue ampliada bajo el contrato 065 de 2021 para la generación de hasta ciento diez y ocho mil ochenta (118.080) identidades digitales adicionales, y posteriormente ampliada bajo el contrato 033 de 2022 para la generación de hasta novecientos doce mil doscientos ochenta y cuatro (912.284) identidades digitales adicionales.

La plataforma de identidad digital incluye los siguientes componentes principales:

- Plataforma de identidad digital: a la cual se tiene acceso a través de una solución móvil tipo App. Esta plataforma se encarga de todo el proceso de identificación del ciudadano, validación biométrica y finalmente la expedición del documento digital.
- Gestión de Identidad: con lo cual se realiza la identificación del ciudadano que está solicitando el documento de identidad digital, este proceso se realiza en sitio central.
- Interoperabilidad: permite interactuar con otros sistemas internos de la Registraduría en primer lugar para lograr la combinación de información de diferentes bases de datos para identificar y asegurar la entrega del documento a la persona que es propietaria de esa identidad y en segundo, permite a terceros recibir información segura de los atributos del documento.

La prestación del servicio de mantenimiento correctivo IDEMIA para la plataforma de identidad digital (cédula digital) cubre todos los equipos, proporcionados por IDEMIA, que hacen parte de esta plataforma y sus componentes.

IDEMIA realizará el mantenimiento correctivo así como el soporte técnico del software y hardware dando sostenibilidad a la plataforma de identidad digital instalada en el marco de los contratos 002 de 2020, 065 de 2021, 033 de 2022 y las adicionales incluidas en esta oferta, para lo cual se dispondrá de un lugar y una infraestructura debidamente adecuada en la ciudad de Bogotá, que facilitará y garantizará una correcta ejecución de los

mantenimientos correctivos de hardware y software y apropiará un stock de repuestos, directamente o a través de sus proveedores, a fin de garantizar la atención de los eventos que requieren tratamiento correctivo desde la generación de la solicitud en la Registraduría y la trazabilidad de las actividades de recepción y despacho del ciclo que surte el equipo hasta su entrega definitiva, contando con una herramienta adecuada para tal fin.

5.2.1.3 > Subactividad 3: Mantenimiento plataforma Autenticación Facial

La plataforma de autenticación facial para terceros usa un motor biométrico MBSS (Multi Biometric Search Services) que ha sido instalado en una infraestructura independiente pero sincronizada a la base de datos biométrica de la plataforma operativa de identificación de la RNEC con el objeto de no afectar el desempeño del sistema central. Esta plataforma permite la prestación de servicios de comparación facial para usos, tanto de entidades gubernamentales como de entidades privadas.

El motor biométrico MBSS de la plataforma de autenticación facial para terceros tiene las siguientes funciones:

- Comparación facial 1:1, conocido como proceso de autenticación de una persona, éste compara los rostros de un ciudadano, antes identificado, contra las biometrías que tiene dicha persona en el repositorio de datos biométricos para el mismo número de identificación.

La plataforma de autenticación facial para terceros se implementó dentro de los alcances del contrato 002 de 2020 con una capacidad de flujo transaccional para procesar 100.000 solicitudes de identificación facial al día.

El contrato 072 de 2021 amplió permanentemente la capacidad de esta plataforma en 300.000 transacciones diarias adicionales y temporalmente en 100.000 transacciones adicionales al día durante el periodo electoral del año 2022.

La prestación del servicio de mantenimiento correctivo IDEMIA para la plataforma de autenticación facial para terceros cubre todos los equipos, proporcionados por IDEMIA, que hacen parte de esta plataforma y sus componentes. Los equipos que requieran mantenimiento correctivo serán objeto de los procesos definidos en conjunto con la entidad, para encontrar una solución dentro de los términos definidos en el presente documento técnico de IDEMIA.

IDEMIA realizará el mantenimiento correctivo así como el soporte técnico del software y hardware dando sostenibilidad a la plataforma de autenticación facial para terceros instalada en el marco de los contratos 002 de 2020 y 072 de 2021, para lo cual se dispondrá de un lugar y una infraestructura debidamente adecuada en la ciudad de Bogotá, que facilitará y garantizará una correcta ejecución de los mantenimientos correctivos de hardware y software y apropiará un stock de repuestos, directamente o a través de sus proveedores, a fin de garantizar la atención de los eventos que requieren tratamiento

correctivo desde la generación de la solicitud en la Registraduría y la trazabilidad de las actividades de recepción y despacho del ciclo que surte el equipo hasta su entrega definitiva, contando con una herramienta adecuada para tal fin.

Es de anotar que los servicios del presente documento no incluyen las siguientes acciones en cualquiera de las tres subactividades de la actividad “Realizar mantenimiento de la plataforma PMT II”:

- Cualquier actividad relacionada con administración, configuración, mantenimiento correctivo sobre componentes de comunicaciones y seguridad, tales como: switches, enrutadores y firewalls o redes LAN, MAN o WAN.
- Instalación y mantenimiento de las redes locales y de la red de telecomunicaciones requeridas para la operación de las estaciones.
- Servicios de conexión remota para dispositivos usados para entrega de documentos tales como conexión 3G/4G y la conexión Wifi. Estos servicios estarán bajo la responsabilidad de la RNEC.

5.2.2 > Actividad 2: Ofrecer la disponibilidad de la plataforma PMT II.

→Subactividades

✓ Administrar la base de datos replicada y servicios WEB de autenticación

La Registraduría Nacional del Estado Civil, durante los años 2020, 2021 y 2022 ha implementado y ampliado sus servicios con el propósito de expandir las actividades misionales de la entidad a la ciudadanía y de esta manera facilitar procesos de solicitud de documentos y servicios de autenticación biométrica en línea a entidades públicas y privadas.

En la implementación de estos proyectos, se ha hecho necesaria la consolidación de bases de datos replicadas y el desarrollo de nuevas aplicaciones tipo web, tales como:

- Bases de datos replicadas para prestación de servicios a terceros:
 - MBSS facial.
- Servicios WEB
 - Para autenticación facial para clientes externos.

Adicionalmente, se incluyen la prestación del servicio a las bases de datos que fueron replicadas en proyectos anteriores ejecutados hasta el año 2021, esto con el objetivo de garantizar la integridad, la disponibilidad y confiabilidad de los datos que serán usados por

todos los procesos misionales de la entidad que estén relacionados con la identificación y el registro civil.

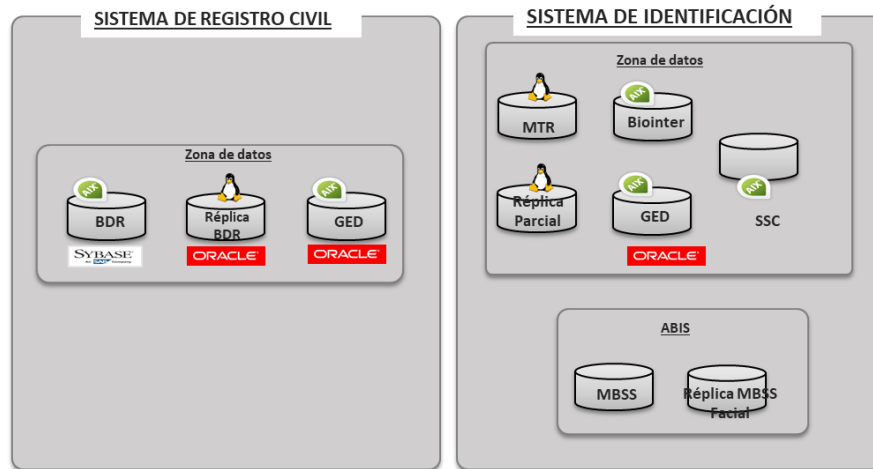


Ilustración 17: esquema de referencia de las bases de datos del sistema de identificación y registro civil

IDEMIA garantizará la actualización a diario del código de novedad (Vigencia) del documento de Identidad, generado por el Archivo Nacional de Identificación (ANI) y que debe ser reflejado en la base de datos intermedia (BIOINTER) a través del MTR en sitio central.

- ✓ Administrar la base de datos de Identificación y Registro Civil de la RNEC, garantizando su operatividad y la integridad de la información

Implica gestionar y dar respuesta a requerimientos de LA REGISTRADURIA tales como cruces o extracción de información, actualización de información y generación de estadísticas, siempre que éstos no obstaculicen el sistema de producción de documentos o el desempeño de las aplicaciones.

IDEMIA monitoreará la solución informática del sistema integral implementado por el Proyecto de Modernización Tecnológica en su segunda fase PMT II y contratos posteriores para mantenerlo habilitado y disponible 24 horas al día, 7 días a la semana (7x24), exceptuando ventanas de mantenimiento que se realicen de forma acordada con la RNEC, así mismo se actualizarán las bases de datos del Sistema de Identificación y Registro Civil con la información proveniente de entes con función registral y de identificación que permita mantener actualizados todos los subsistemas incluyendo los remotos. Verificará y monitoreará que las actualizaciones e integridad de las bases de datos y de tablas de referencia se estén ejecutando de acuerdo con los procedimientos establecidos en el Proyecto de Modernización Tecnológica y finalmente realizará las copias de seguridad

definidas (totales e incrementales) para el sistema con la periodicidad requerida por la Entidad.

Como parte complementaria, IDEMIA administrará el tablero de transferencia automática que conmuta la energía externa para el centro de cómputo ABIS.

IDEMIA administrará los recursos tecnológicos complementarios y aplicativos de:

- Identificación:
 - Aplicaciones: ABIS, MTR, CMS, ICPS, Web Services, GED ID, SSC, IDPS – implementado para personalización de documentos en policarbonato (componente adquirido en 2020)
 - Interfaz MTR-SIRC-ANI, INTERAFIS
 - Réplica I de la Base del MTR para el Web Service del Sitio Central y Aplicativos asociados a la operación del Workflow,
 - Web Service para autenticación biométrica, BIOINTER, MBSS facial (componente adquirido en 2020), Sistema HLED Web para MorphoTablet™ y Estación Integrada de Servicios – EIS (fijas y móviles)
 - Aplicaciones y componentes implementados para la gestión de Identidad Digital.
 - Plataforma de servicios de autenticación facial para entidades externas - MBSS facial.
- Registro Civil:
 - SIRC, GED RC, SSC – Parte Registro Civil, Línea de digitalización y Réplica total de la base de datos de Registro Civil y Web service de Registro Civil.

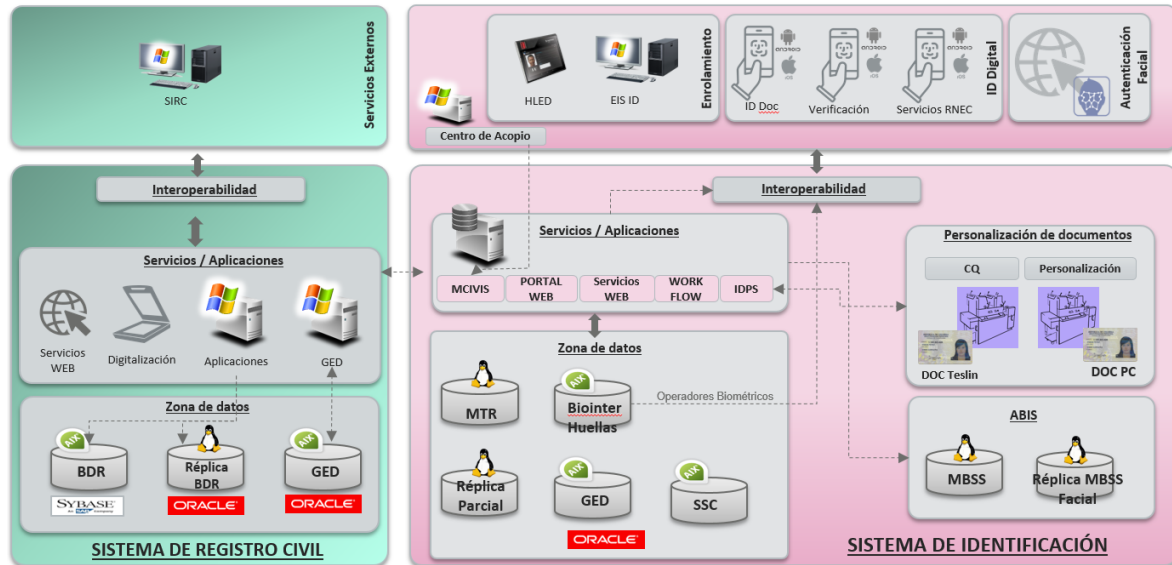


Ilustración 18. esquema de referencia de la solución PMT

Considerando la necesidad de la Entidad de incluir una biometría complementaria para lograr una mayor precisión en la identificación de los colombianos, durante la vigencia 2018 se incorporó el motor multibiométrico ABIS, lo que requirió la gestión, control de calidad y disponibilidad de las plantillas (templates) derivadas de la incorporación de dicha biometría a nivel de operación, mantenimiento correctivo y sostenibilidad.

Una vez incorporada la biometría complementaria, la Entidad, en 2018 realizó el diseño y desarrollo de la herramienta HLED Web, en el 2019 implementó la herramienta EIS, ambas con la inclusión de servicios que permiten la verificación del titular mediante el uso de la biometría facial en la preparación y entrega del documento de identidad. Igualmente, en el 2020 con la plataforma de autenticación facial para terceros / MBSSF, el servicio se encuentra en aumento para ser consumido por las entidades externas públicas y privadas, quienes pueden realizar la verificación de la titularidad del documento o autenticarse al momento de hacer uso de su cédula digital; este dinamismo en la capacidad transaccional ha incrementado el uso de las autenticaciones faciales, por lo tanto, es necesario monitorear 7x24 la solución implementada, con el fin de garantizar la prestación de los servicios misionales de la Entidad en materia de identificación a nivel nacional con personal calificado y capacitado para dar soporte, operar y administrar estas tecnologías.

Por otro lado, la inclusión del sistema de enrolamiento de la Estación integrada de servicios – EIS, implementado en sedes de la Registraduría, se deberá mantener disponible la aplicación; lo que requiere fortalecer las actividades relacionadas con el monitoreo, operación y administración que garantizará la interoperabilidad y sincronización con las bases de datos en sitio central y demás subsistemas de la Entidad.

5.2.3 > Actividad 3: Disponer de un soporte técnico a usuarios

→Subactividades

✓ Servicio de Mesa de Ayuda

Para asegurar la operación y el funcionamiento de la mesa ayuda, IDEMIA administra y pone a disposición una infraestructura de hardware y software a través de la cual realiza la gestión de los casos reportados por los usuarios, los cuales son registrados y documentados en el sistema de gestión de mantenimiento correctivo y soporte técnico, lo que permite hacer seguimiento a través de la generación de informes de casos atendidos y dar respuesta a los mismos.

Las acciones desde la creación del caso en la mesa de ayuda hasta el inicio de su gestión se espera que sean realizadas un tiempo máximo de 1 día hábil. El tiempo de respuesta no será superior a 3 días hábiles.

Esta plataforma incluye:

1. Acceso a un software para el registro de todos los eventos concernientes a la totalidad de equipos instalados¹, donde se resuelvan problemas de funcionamiento de hardware y software.
2. Una cuenta de correo electrónico con el fin de recibir y dar respuesta a las solicitudes de soporte con respecto a los aplicativos de Identificación, Registro Civil.
3. Una troncal de voz para la planta telefónica y un sistema de "encolamiento" para gestionar las llamadas en espera.

¹ Corresponden a los equipos que están dentro del Inventario proporcionado por la Entidad al inicio del contrato.

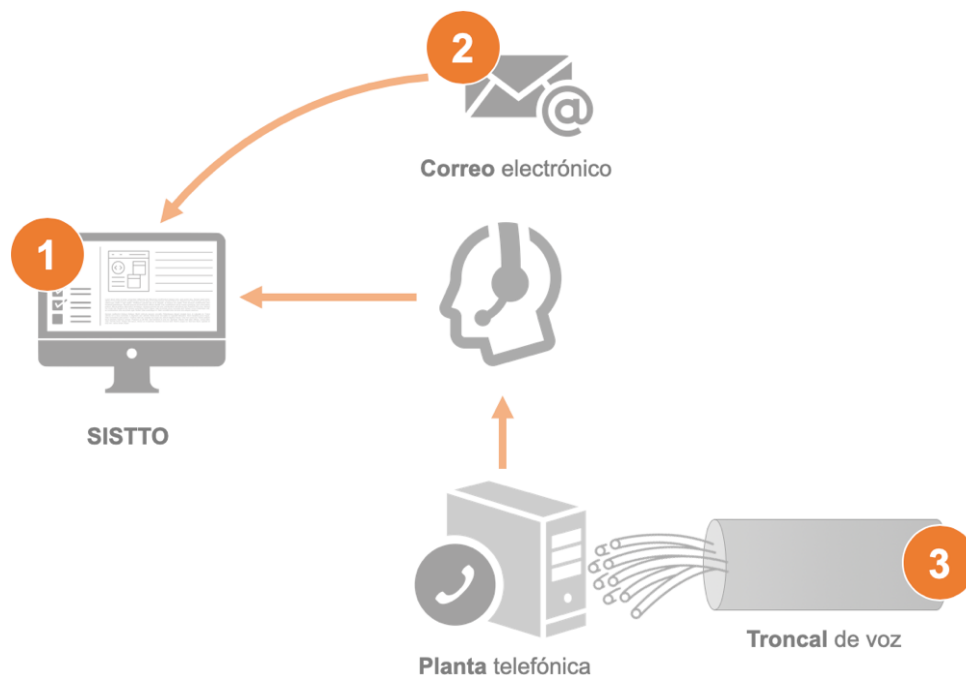


Ilustración 19: esquema de la mesa de ayuda

5.2.4 > Actividad 4. Cargar la información del trámite del colombiano

→ Subactividades

Las tareas contempladas para esta actividad incluyen:

1. Sostener la operación de la fábrica y subsistema en el sitio central
2. Realizar el cargue de la información proveniente de los centros de acopio y trámites WEB
3. Operar el cliente control calidad de los datos
4. Operar el cliente IQC (Image Quality)
5. Operar el cliente SQC (Signature Quatily Control)
6. Asegurar que las transacciones provenientes de la estación integrada de servicios EIS sean cargadas de manera automática en el sistema central de identificación.
7. Garantizar que los trámites provenientes de la aplicación móvil para trámite de reimpresión de documentos de identidad en Teslin con autenticación facial, y los tramites de reimpresión realizados desde el portal institucional sean cargados al

sistema de forma oportuna y segura, procesando y reportando las excepciones en caso de presentarse.

5.2.5 > Actividad 5. Validar la información del trámite

→Subactividades

Validar la información del trámite incluye actividades que serán realizadas para garantizar la calidad de la información contenida en la personalización de los documentos producidos en Teslin y en Policarbonato en el entendido que ambos hacen parte de la solución integral.

Entre las actividades que se realizarán se encuentran las siguientes que serán aplicables según sea el caso de producción en Teslin o en Policarbonato.

Para Teslin:

1. Labores de control de calidad y retratamiento de foto y firma
2. Depuración a través de un rechazo definitivo de las solicitudes de CQC con imposibilidad de retratamiento en el módulo CARD-RET de foto y firma. Para el caso de los estados “Rechazado Definitivamente” IDEMIA informará a la Entidad para su respectivo tratamiento.

Para Policarbonato:

1. Labores de control de calidad y retratamiento de firma
2. Para casos de rechazo IDEMIA informará a la Entidad para su respectivo tratamiento.

5.2.6 > Actividad 6. Producir documentos de identificación

→Subactividades

- ✓ Garantizar la disponibilidad de la línea de producción de los documentos de identidad

Los servicios de IDEMIA ofrecidos incluyen las líneas de producción de documentos personalizados en Teslin y policarbonato, los que conjuntamente representan los volúmenes estimados de producción indicados en esta sección.

IDEMIA realizará un flujo de producción promedio de hasta diez y ocho mil (18.000) documentos al día distribuidos así: hasta catorce mil (14.000) documentos en promedio expedidos en formato Teslin y hasta cuatro mil (4.000) documentos en promedio de seguridad personalizados en policarbonato, es decir, un aproximado semanal de noventa (90.000) documentos de identidad sumada la producción en Teslin y la producción en policarbonato, teniendo en cuenta los planes de producción, la disponibilidad de insumos y la demanda de trámites.

Así mismo, se presentará un informe mensual de los insumos utilizados para la producción de los documentos de identidad.

Nota: *Si bien es cierto el equipo INNOVATIME INNO 6000 con que cuenta actualmente RNEC es modular, por lo que se podría aumentar su capacidad de producción, actualmente tiene 2 módulos láser instalados, lo que limita su capacidad de producción. Cada tarjeta en policarbonato es grabada por un láser en el anverso y luego por el otro láser en el reverso, el contar con dos módulos láser permite que el equipo esté optimizado para trabajar sobre 2 cédulas a la vez (una por cada láser). La cédula colombiana requiere la personalización de una gran cantidad de datos variables (fotografía, datos biográficos, código QR, MRZ, ...) por lo que se requiere un tiempo mínimo de trabajo de cada láser para personalizar correctamente cada documento (no se puede aumentar la velocidad de personalización sin afectar la calidad del documento personalizado). Adicionalmente se debe tener en cuenta que el proceso de emisión de documentos seguros de identificación cubre diferentes pasos que están articulados para tener la eficiencia en el mismo desde el momento en el cual son recibidas las solicitudes en la planta de producción, luego se procede a agrupar los diferentes lotes a personalizar por los lugares de entrega, cargar la máquina de personalización con suficientes tarjetas de policarbonato en blanco, y se procede a enviar los lotes previamente preparados a la máquina de personalización INNO 6000 o INNO Kiosk; una vez son personalizados se sigue con el flujo de control de calidad y se realizan las diferentes validaciones de los datos personalizados en el documento contra los datos de la solicitud, se valida la lectura del MRZ, se valida lectura del código QR Cifrado a través de un proceso de descifrado por el HSM centralizado y verificación de minucias de las huellas entre otros, posteriormente y gracias al agrupar los lotes por lugar de despacho se logra que sea eficiente el empaque y posterior entrega a la entidad de forma expedita. Este proceso es basado en las mejores prácticas de producción a nivel mundial y ha sido ajustado a las necesidades de la RNEC, logrando así la eficiencia en el proceso de emisión de documentos seguros. Parte de un proceso estable de producción es el mantenimiento periódico que se realiza a ambas impresoras de Policarbonato que pueden ser desde limpieza de los laser hasta procedimientos de configuración solicitados por el fabricante, estos de mantenimientos serán acordados con el cliente para no impactar la operación. La preparación de lotes de producción y las ventanas de mantenimiento preventivo y correctivo son tiempos donde el equipo no está*

personalizando tarjetas. Es por esto que el equipo actual tiene una capacidad máxima de personalización de 4000 documentos por día. Si la entidad requiere una capacidad superior de personalización de documentos es necesario considerar ampliación de la plataforma actual, la que sería objeto de una oferta de bienes y servicios separada de la presente oferta.

Nota: *Resaltamos del mismo modo que la RNEC actualmente no cuenta con un respaldo del equipo INNO6000 que permita garantizar la continuidad de la producción en caso de cualquier actividad que requiera una pausa en la producción de documentos personalizados.*

IDEMIA gestionará el flujo de producción de documentos en policarbonato en las máquinas de personalización de documentos homologada para la tecnología Lasink INNO6000.

✓ Administrar y operar la fábrica de documentos de identidad, con personal calificado

Administrar la fábrica de producción de documentos de identidad mediante un esquema de operación en oficinas centrales, supervisor de CCD y (IQC, SQC y RDC), supervisor de fábrica (troquelado y laminado, empaque), supervisor en CQC y envíos (control casilleros, CQC, certificación LMU, LEX, LEN y distribución).²

Administrar y gestionar los insumos de producción y envíos de documentos de identidad recibidos de la Registraduría y generar un informe mensual de los insumos utilizados para la producción de documentos de identidad.

²CCD: Control de Calidad de Datos, IQC: Image Quality Control, SQC: Signature Quality Control, RDC: Cargue de CD, CQC: Card Quality Control, LUM: Lote De Municipio, LEX: Lote De Expedición, LEN: Lote De Entrega. Cuando a estas siglas se les antepone P o PC, quiere indicar que es para policarbonato. IQC no se realiza para policarbonato.

6 / Insumos TESLIN® para TI y CC

Esta sección describe la propuesta de IDEMIA para el suministro de Insumos para producción de Cédula de Ciudadanía y Tarjeta de Identidad fabricadas actualmente en TESLIN®.

Nota: El contratista asegurará la adaptabilidad de los insumos a la línea de producción y personalización actualmente implementada por la Registraduría Nacional del Estado Civil.

6.1 > TESLIN® SP1000 TS Preimpreso

El sustrato de impresión sintético TESLIN® ofertado por IDEMIA tendrá las siguientes especificaciones técnicas y cumplirá con los elementos de seguridad documental establecidos en la siguiente tabla:

Sustrato de impresión sintético TESLIN®	
Especificación técnica: Sustrato de impresión sintético TESLIN®	
Referencia	TESLIN® – Ref. SP1000TS
Dimensiones y Formato	
Espesor – Calibre	254 µm (10 milésimas de pulgada)
Presentación	Cajas de 500 Hojas tamaño A3 (420 mm x 297 mm) ± 1 mm
Formato	Distribución diseño (3 x 7 documentos) por hoja A3
Rendimiento	Veintiuno (21) documentos por hoja tamaño A3
Características de seguridad	Preimpresión fondo de seguridad Offset seco y húmedo. Aspectos técnicos y de seguridad como: utilización tintas fluorescentes, tintas anticopia, metálicas, tintas variablemente

Sustrato de impresión sintético TESLIN®	
	ópticas (OVI) para formato de tarjeta de identidad, guiloches, irisados, microtextos y elementos de seguridad.
Elementos de Seguridad: Sustrato de impresión TESLIN® SP1000TS	
Tintas fluorescentes	Tintas con agregados sólidos luminiscentes expuestos con colores fluorescentes ante incidencia de radiación ultravioleta.
Tintas anticopia	Tintas de seguridad que evitan su copiado a través de medios físicos.
Tintas metálicas oro y plata	Incorporan partículas metálicas oro y plata que otorgan brillo a la figura o filigrana además de poseer propiedades fluorescentes en la tinta plata.
Tintas variablemente ópticas (OVI) para formato de tarjeta de identidad	Tintas que otorgan efecto óptico de variabilidad del color al modificar el ángulo de incidencia de la luz y/o de observación.
Guiloches	Orlas o tramas de líneas finas, traslapadas intrincadamente, con repetición de patrones formados por curvas en filigrana en red continua.
Irisados	Degradación de colores, elaborado en batería con separadores cromáticos los cuales se mezclan entre sí.
Microtextos de seguridad	Títulos o leyendas de dimensiones reducidas, resultando necesario emplear lentes con aumento para su visualización.
Fondos con orlas, tramas finas con diseños Antifotográficos	Diseño de micro líneas formaciones y alineaciones para imposibilitar reproducción mediante fotocopadoras o equipos de digitalización.
Colores de tintas suaves y apastelados – Tabla Pantone	Entre otros.

Tabla 4. Especificación técnica del sustrato de impresión sintético TESLIN®

Nota: El sustrato es la superficie de impresión en la base del papel sintético TESLIN®, que eleva el estándar de las tarjetas de seguridad, la durabilidad, la resistencia al agua, sustancias químicas, rasgado y la abrasión, térmicamente estable y disipador de la estática.

6.2 > Laminados holográficos y claros

La estampación HOLOGRÁFICA en el laminado anverso para cédula de ciudadanía tendrá las siguientes especificaciones técnicas y cumplirá con los elementos de seguridad documental establecidos en la siguiente tabla:

Plástico de Laminación Anverso Holográfico / Reverso Claro	
Especificación técnica: Plástico de Laminación Anverso Holográfico / Reverso Claro	
Referencia	Composición Poliéster/ Polietileno Tereftalato (PET/PE)
Dimensiones y Formato	
Espesor – Calibre	7 milésimas de pulgada estructura (5/2)
Presentación	Rollos emparejados (asociados o certificados) anverso-reverso alineados por los ángulos para garantizar adherencia, tamaño (0.9678 pies ancho x 1000 pies largo +/- 0.5% y diámetro de cono interno 3 pulgadas).
Formato	Distribución diseño (3 columnas) por rollo
Rendimiento	Aprox. 14.830 documentos por pareja de rollo anverso-reverso
Características de seguridad	Laminado anverso con estampación holográfica de seguridad uniforme, transparente desmetalizada. La imagen holográfica 3D del laminado holográfico debe observarse a una distancia de 18" o 45 cm en condiciones de iluminación con luz fluorescente, con movimiento de izquierda hacia derecha y efecto arco iris en los textos del holograma. Adicionalmente la parte del laminado PET/PE holográfico, debe ser uniforme sobre toda la superficie de la película (metalización en aluminio).
Elementos de Seguridad: Plástico de Laminación Anverso (Cédula de Ciudadanía)	
El holograma tridimensional (3D) a partir de escultura	Imagen generada por Láser de alta resolución y características de alta seguridad (paralelaje o apariencia de movimiento controlado ante visualización desde ángulos específicos, animación y apariencia de profundidad),
Imágenes mercuriales	Imágenes o textos con exposición aguda y brillante que entregan la impresión de movimiento de color, variación cromática según el ángulo de incidencia de la luz,
Fondos de color verdadero	Imágenes con apariencia de colores brillantes y vibrantes cuando son visualizados desde ángulos visuales específicos.
Micro imágenes, micro textos	Texto o logotipos visibles únicamente mediante equipos de magnificación comunes.

Plástico de Laminación Anverso Holográfico / Reverso Claro	
Superficie holográfica	La parte del laminado PET/PE holográfico, debe ser transparente y uniforme en la superficie de la película (desmetalización en aluminio).

Tabla 5. Especificación técnica de laminados holográficos y claros

6.3 > Entregable

La siguiente es la cantidad de insumos para la producción de documentos de identidad para cédula de ciudadanía y tarjeta de identidad, que serán entregados por IDEMIA.

Ítem	Descripción de los insumos	Total
1	Hojas de TESLIN® PREIMPRESO para Cédula de Ciudadanía	56.495
2	Rollos de laminado HOLOGRAFICO Anverso para Cédula de Ciudadanía	80
3	Rollos de laminado CLARO Reverso para Cédula de Ciudadanía	80
4	Hojas de TESLIN® PREIMPRESO para Tarjeta de Identidad	14.124
5	Rollos de laminado CLARO Anverso para Tarjeta de Identidad	20
6	Rollos de laminado CLARO Reverso para Tarjeta de Identidad	20

Tabla 6. Insumos para producción de documentos de identidad

7 / Robustecimiento de la App Cédula Digital Colombia

De acuerdo con los requerimientos presentados por Registraduría Nacional del Estado Civil en su solicitud de cotización RDRC-360 del 4 de octubre de 2022 y su anexo, IDEMIA oferta lo solicitado para la solución de Robustecimiento de la App Cédula Digital Colombia que permite incorporar nuevas funcionalidades que tendrán acceso a través de la cédula digital diseñadas para soportar los servicios ciudadanos digitales de entidades públicas y particulares, logrando así que la cédula de ciudadanía digital se convierta en la llave de acceso a trámites y servicios generando posibilidad de notificación y firmado digital de documentos, gestión de documentos remitidos por autoridades y entidades autorizadas, al igual que el servicio para alojar documentos.

Para la solución de Robustecimiento de la App Cédula Digital Colombia contenida en la presente oferta, en razón a que es un servicio que IDEMIA no provee de manera directa, realizamos una evaluación técnica con varias entidades de certificación digital (ECDs), todas con acreditación del organismo Nacional de Acreditación de Colombia (ONAC), siguiendo los requerimientos puntuales de la RNEC, lo cual dio como resultado que la empresa que cumplió con todos estos requerimientos fue la compañía Gestión de Seguridad Electrónica S.A. con siglas GSE, la cual presentó la documentación correspondiente como soporte de garantía del cumplimiento de todas las especificaciones técnicas solicitadas.

En este capítulo se explican todos los componentes técnicos que incorpora la solución de Robustecimiento de la App Cédula Digital Colombia.

7.1 > Características de la Arquitectura

La solución propuesta tiene una arquitectura tipo empresarial resiliente para el esquema de validación y autenticación digital para trámites y operaciones del App Cédula Digital Colombia, que incluyen los servicios de notificaciones certificadas, firmado de documentos con algoritmo de firma ECDSA y estampado cronológico de certificaciones, con el fin de que pueda ser adaptable a los posibles escenarios emergentes y cubra las estrategias básicas de anticipación, prevención, detención y tolerancia.

7.1.1 > Características Mínimas Ofrecidas para los Centros de Datos en Cloud

DISPONIBILIDAD EN DIFERENTES ZONAS

Se oferta una arquitectura que contempla un esquema en nube de alta disponibilidad con Centros de Datos ubicados en diferentes zonas, en el continente americano; se tendrá mínimo dos zonas de disponibilidad en una única región, con lo que se pretende que, en caso de siniestros, ataques de denegación, fallos a nivel de zona no se presente indisponibilidad de servicio.

Las características mínimas ofertadas de Centros de Datos por Zona son:

- a. Los Centros de Datos ubicados fuera de la República de Colombia únicamente procesarán peticiones, en ellos no será almacenada la data (datos de los usuarios, notificaciones, documentos firmados).
- b. Los Centros de Datos cumplirán las disposiciones legales de protección de datos vigentes en Colombia.
- c. Los Centros de Datos ofrecerán un servicio de caché en Colombia con propósito de disminuir los tiempos de respuesta al usuario final.
- d. Los Centros de Datos implementarán varias capas de seguridad y/o servicios.
- e. Los Centros de Datos cumplirán con políticas de control y la auditoría de datos y seguridad debidamente acreditados y homologados para lo cual demostrarán como mínimo el cumplimiento de los siguientes estándares: Controles de la alianza de seguridad en la nube, CSA; Administración de riesgos de terceros, CyberGRX; Estándar de calidad internacional, ISO 9001; Controles de administración de seguridad, ISO 27001; ISO 27017; Administración de Información sobre la privacidad ISO 27701; Protección de Datos Personales, ISO 27018; Informe de Controles de Auditoría, SOC 1; Informe de seguridad disponibilidad y confidencialidad, SOC 2; Informe de controles generales, SOC 3; Departamento de Defensa Procesamiento de datos DoD SRG; Normas de datos gubernamentales, FedRAMP; Instituto Nacional de Normalización y Tecnología, NIST 2.

7.1.2 > Características Mínimas de la Capa de Seguridad

La solución que incorpora un esquema de validación y autenticación digital para trámites y operaciones dentro del App de Cédula Digital Colombia se requiere una infraestructura segura, resistente, eficaz y de alto desempeño que cumplirá con estándares internacionales de seguridad y contará con las siguientes características que permitirán:

- a. Definir los permisos e identificaciones del usuario, las medidas de protección de infraestructura y de protección de datos para lograr una estrategia de adopción uniforme y planificada.
- b. Permitir el monitoreo de los servicios implementados para la aplicación de manera escalable, de las interacciones de los administradores y de las modificaciones realizadas y facilitar la auditoría de eventos.
- c. Dar respuesta a la recuperación automatizada de incidentes que ayuden a cambiar responder y analizar la causa raíz de posibles ataques.
- d. Implementar la automatización y detección por eventos, con el fin de construir soluciones en tiempo real.
- e. Incorporar un firewall de aplicaciones web tipo SAAS para que los servicios de validación y autenticación digital para trámites y operaciones a incorporar dentro del App de Cedula Digital Colombia proteja contra exploits y bots web comunes que puedan afectar la disponibilidad, comprometer la seguridad o consumir recursos excesivos.
- f. Contar con un WAF tipo SAAS que brinda control sobre la forma en que el tráfico llega a la aplicación y permitir crear reglas de seguridad que controlen el tráfico de bot y bloqueen patrones de ataque comunes, como la inyección de SQL o las secuencias de comandos entre sitios.
- g. Poseer un servicio de protección contra ataques de denegación de servicio distribuidos (DDoS) que permita proteger las aplicaciones ejecutadas y mitigar posibles ataques en línea o de manera programada y realizar una detección siempre activa con el fin de reducir el tiempo de inactividad y la latencia de la aplicación.
- h. Contar con un servicio de red de entrega de contenido (CDN) que de forma segura de cualquier tipo de datos a clientes en Colombia con baja latencia, baja red y altas velocidades de transferencia.

7.1.3 > Características Mínimas de la Capa de Monitoreo

La infraestructura deberá tener servicios que permitan el constante monitoreo de los servicios a implementar para asegurar el esquema de validación y autenticación digital en los trámites y operaciones dentro del app de Cédula Digital Colombia y dichas herramientas contemplarán como mínimo:

- a. Un servicio que permitirá a la entidad habilitar auditorías operativas y de riesgo de los servicios implementados y que facilitarán a los usuarios ver, buscar, descargar, archivar, analizar y responder a todos los incidentes asociados a la aplicación y a la actividad de toda la infraestructura.
- b. Un servicio transversal que facilitará el monitoreo y administración mediante el suministro de datos e información útil para las aplicaciones y la infraestructura a través de las siguientes actividades:
 - Recopilar datos de monitoreo en forma de registros, métricas y eventos.
 - Determinar los recursos, aplicaciones y servicios que se ejecuten en cloud y servidores locales.
 - Permitir visualizar métricas se muestren en la página de inicio de la consola de administración y seguimiento.
 - Facilitar la creación de paneles de control personalizados adicionales para mostrar métricas y alarmas, así como enviar notificaciones o realizar cambios automáticos en los recursos en función de las acciones siempre que se sobrepase un umbral previamente definido.

7.1.4 > Características Mínimas de la Capa de Red y Balanceo de Aplicativos

Los servicios por incluir dentro del App Cédula Digital Colombia se desarrollan a través de microservicios donde la capa de red y balanceo contará como mínimo con las siguientes características:

- a. Un servicio que permitirá la implementación y creación de redes privadas y grupos de seguridad que facilite independizar los recursos.

- b. Un servicio que permitirá distribuir el tráfico entrante a varios destinos, como instancias, contenedores, funciones serverless, direcciones IP; por zonas de disponibilidades únicas o múltiples a fin de proporcionar alta disponibilidad, escalabilidad y seguridad para la aplicación.

7.1.5 > Características Mínimas de la Capa Interconexión

La data (datos de los usuarios, notificaciones, documentos firmados y demás) estará alojada en centros de datos ubicados única y exclusivamente en el territorio de Colombia, la interconexión entre dichos centros de datos y los ubicados en cloud poseerá un servicio que facilite establecer una conexión desde una red local y una o más redes privadas de conexión en la misma zona.

Igualmente, se asegurará la interconexión entre redes privadas de los centros de datos ubicados en Colombia mediante interfaces virtuales privadas que conectarán directamente a los centros de datos del proveedor cloud.

La capa de interconexión tendrá como mínimo las siguientes herramientas:

- Consola de administración para configuración de las interfaces virtuales privadas.
- Sistema de selección de conexiones de red sobre Internet.
- Interconexión con todos los servicios del operador cloud a los que se pueda acceder a través de Internet.
- VPNS para conexión nube / tierra con canales privados o a través de internet protegido mediante VPNS.

7.1.6 > Características Mínimas Requeridas de los Centros de Datos en Colombia

Toda vez que la data (datos de los usuarios, notificaciones, documentos firmados) estará alojada única y exclusivamente en centros de datos con ubicación en el territorio de Colombia, por razones de seguridad nacional, las locaciones cumplirán con las siguientes características técnicas y de conectividad:

1. Se proveerá un Data Center con esquema de alta disponibilidad

2. El Data Center contará con certificado mínimo Tier III en diseño y/o construcción e ICREA IV y certificado en SOC 2 Tipo 2.
3. El Data Center estará ubicado en Colombia.
4. Los racks serán provistos por el datacenter como servicio y contarán con suministros de UPS
5. El suministro de switches VLANs con tarjetas de mínimo 1 Gbps, serán provistos por el datacenter como servicio.
6. El Data Center garantizará que cuenta con certificación en donde demuestre que la fuente principal eléctrica es propia.
7. El Data Center estará ubicado en un sitio de fácil acceso.
8. El Data Center contará con puestos de trabajo con punto de red, estos puntos de red tendrán la posibilidad de hacer conexión hasta el rack.
9. El Data Center estará en configuración 2N en todos sus componentes.
10. Garantizará que los equipos del Data Center están ubicados en pasillos con contención de aire frío – aire caliente.
11. La Interconexión entre Racks se realizará por medio de fibra óptica y/o UTP preferiblemente categoría 7 según los requerimientos o la estandarización del Data Center.
12. Red de cableado estructurado en fibra óptica y/o UTP categoría 6 o superior un manejo de velocidad Ethernet de mínimo 1 Gbps provisto por el datacenter como servicio.
13. Racks con cerraduras independientes.
14. Se realizarán las actividades necesarias para dar cierre oportuno a las vulnerabilidades identificadas a nivel de sistema operativo. Las vulnerabilidades consideradas críticas y/o severas serán cerradas en el menor tiempo posible.
15. Se garantizará mantener los sistemas operativos actualizados respecto a las actualizaciones de seguridad liberadas por los fabricantes.
16. Se implementarán mecanismos de seguridad necesarios sobre la información, de tal forma que la información del proyecto no sufra ningún daño y/o pérdida teniendo en cuenta que se garantizará confidencialidad, integridad y disponibilidad de la misma, durante los procesos de transmisión, restauración y almacenamiento.
17. Se garantizará que toda la información del proyecto que se encuentre en tránsito o reposo se mantenga cifrada usando estándares y algoritmos reconocidos internacionalmente que brinden la seguridad, la criptografía será de curva elíptica.
18. Se garantizará segregación de funciones para los procesos de administración y gestión del servicio.
19. Se contará con técnicas de múltiple factor de autenticación para el acceso a las consolas de administración.
20. Se garantizará integración segura con las capas de presentación, aplicación y bases de datos.
21. Se contará con mecanismos que permitan evitar pérdida, divulgación no autorizada, fuga, copia no autorizada de información del proyecto, de ser posible contará con una herramienta de prevención de fuga de información.
22. Se asegurará que los tiempos de autorización de ingreso a los Data Center no supere las 4 horas para un ingreso normal y 2 horas para un ingreso urgente.
23. Se suministrará el servicio de anti-malware para protección de los archivos alojados en la infraestructura.

24. Los recursos, ingenieros ofrecidos como soporte y administración, contarán con las habilidades y conocimientos necesarios para soportar la plataforma tecnológica para el proyecto en lo referente a sistemas operativos e infraestructura física.
25. Atender con la disponibilidad necesaria las visitas de auditorías internas y externas del proyecto y suministrar las evidencias solicitadas por dichas auditorías.
26. Los perfiles poseerán conocimientos y experiencia en el uso, configuración y administración de plataformas iguales o similares.
27. Garantizar estricta reserva sobre cualquier información interna de los involucrados en el proyecto, obtenida durante la prestación de los servicios, esto mediante firma de cláusulas de confidencialidad de la información.
28. Suministrar Software de virtualización con su respectivo licenciamiento.
29. Proveer todos los sistemas operativos con su respectivo licenciamiento.
30. Realizar la administración de los sistemas operativos.
31. Suministrar los servicios necesarios para la toma de copias de respaldo.
32. Realizar monitoreo de los servidores 7X24X365.
33. Realizar y enviar informes mensuales de capacidad y disponibilidad de la infraestructura.
34. Monitorear los requerimientos de crecimiento anual en máquinas con sistema operativo, licenciamiento de software para copias de respaldo y monitoreo y virtualización, para crecimiento, es decir, crear nuevas máquinas virtuales sin generar ningún costo a la Entidad siempre y cuando no se sobrepase lo aprovisionado.
35. Realizar en conjunto mínimo una prueba anual del plan de contingencia.
36. Garantizar que los equipos utilizados para la implementación de la arquitectura del proyecto sean alto rendimiento, exclusivos para el proyecto.
37. Contar con una solución de seguridad perimetral firewall en Alta disponibilidad (HA) que cumplirá mínimo con una capacidad de Throughput superior a 9 Gbps en capacidad total con mínimo 2.5 Gbps en modo NGFW , con interfaces de mínimo 1 Gb a nivel LAN y a Nivel WAN, soportará una capacidad de hasta 1.000.000 de sesiones concurrentes, protección IPSec y SSL VPN, control de aplicaciones, prevención de intrusos, antivirus, antimalware y capacidades de New generation firewall cuyo fabricante estará calificado dentro del cuadrante de líderes de Gartner.
38. Garantizar que los equipos para la generación de los procesos de confianza digital cumplan con los siguientes estándares: FIPS 140-2 Nivel 3: contraseña, Certificado #3205; QSCD para el cumplimiento de eIDAS; Certificación Common Criteria (PP 419 221-5) – y cumplan con las certificaciones UL, CSA, CE, FCC, CE, VCCI, C-TICK, KC Mark, RoHS2, WEEE, TAA, con capacidad de almacenamiento superior 130.000 llaves privadas y con capacidad de procesamiento superior a 20.000 transacciones por segundo.
39. Garantizar que los servicios de almacenamiento sean escalables de manera modular, de conformidad con la proyección de crecimiento que será comunicada según plan de trabajo acordado entre las partes.
40. Se suministrará en el centro de datos como mínimo (2) servidores de procesamiento que cumplirán con memoria RAM 512GB, dos procesadores de última generación Intel Xeon 2.4 GHz 32 Cores, 16 core cada procesador con almacenamiento de Arreglo Raid 1+0, discos SSD, espacio efectivo 5 TB efectivo, doble fuente redundante, 2 tarjeta de

red dual port con de 1 a 10 GB, 1 tarjeta de red con 1GB, consola de administración, soporte y garantía del fabricante 7x24x365.

41. Se suministrará en el centro de datos dos (2) licencias para virtualizar base de datos con soporte y garantía del fabricante 7x24x365, la virtualización y poseerá un software que centralice la administración de los nodos físicos y virtuales en una única consola, la que será administrada por un cliente y/o web.
42. En el centro de datos se proveerá como servicio dos (2) switch de mínimo 1 GB, con soporte y garantía del fabricante 7x24x365.
43. El suministro y administración de los equipos y software, que soportan la solución técnica y permiten el uso de los componentes de firmado, cifrado, almacenamiento, estampado cronológico, conservación y consulta de las notificaciones electrónicas certificadas y almacenamiento seguro de los documentos electrónicos una vez firmados, estará cargo de la Entidad de Certificación Digital acreditada ante la ONAC que provee el *Automated Meta Identity System (AMIS)* Mobile SDK, toda vez que ésta deberá garantizar su adecuado funcionamiento.
44. Se presentarán las hojas de los profesionales que harán labor de instalación administración y soporte de los equipos que ejecutan los servicios de seguridad y confianza, éstos estarán certificados por el fabricante y además contarán con certificaciones de administración de nube. De igual manera se presentarán las hojas de vida de las empresas que realizarán la instalación de cada parte de la infraestructura que contará con la certificación emitida los fabricantes.

7.1.7 > Características Mínimas Requeridas para la Capa de Red a los Centro de Datos en Colombia

En caso de requerir conectividad con otros datacenter en Colombia se cumplirán las siguientes características:

1. Los canales serán sin reuso, incluyendo elementos y configuraciones que permitan su operación las 24 horas del día.
2. Se proveerá un esquema de alta disponibilidad en canales de comunicación, mediante última milla redundante, en caso de falla.
3. El ancho de banda requerido para administración y monitoreo será diferente al suministrado.
4. Se garantizará disponibilidad de los canales: 99.96% para canales con alta disponibilidad o redundancia, y 99.7% para canales sin redundancia, los cuales se utilizarán únicamente para la conexión entre la infraestructura ubicada en Colombia y la infraestructura en nube.
5. La medición de la disponibilidad será independiente por cada uno de los canales.
6. Se certificará que se cuenta con mecanismos que garantizan un 99.982% de disponibilidad en su red troncal.
7. Tendrá capacidad de manejar multiprotocolo TCP/IP.

8. Los anchos de banda serán efectivos.
9. Habrá la posibilidad de aumentar el ancho de banda de acuerdo a la necesidad, ya sea temporal o definitiva hasta en un 10%, en un tiempo no mayor a veinte (20) días hábiles.
10. Un canal se considerará indisponible o caído cuando no permita el tráfico de datos.
11. Se considerará que un canal presenta intermitencias en condiciones donde se puede demostrar degradación de tráfico de datos parcialmente, en más de tres ocasiones en una hora.
12. Se garantizará la instalación, el soporte y la atención de fallas para el último kilómetro en todos los enlaces.
13. Se realizará el aprovisionamiento, administración, seguimiento y gestión de la infraestructura ofrecida incluyendo todos los equipos activos para garantizar la calidad y continuidad de la solución
14. Se tendrá acceso a través de internet con la seguridad necesaria para la autenticación solamente de personal autorizado.
15. Se asegurarán que todos los datos personales en reposo sean gestionados en territorio colombiano y se garantizará su cifrado mediante un esquema híbrido que utilizará algoritmo de curva elíptica, además su tratamiento estará alineado con la Ley 1581 de 2012 de protección de datos personales y su Decreto Reglamentario 1377 de 2013 o demás normas que las modifiquen o sustituyan.

7.2 > Características de los Servicios

El esquema de validación y autenticación digital para trámites y operaciones mediante el uso de mecanismos de confianza digital contemplará el siguiente alcance:

7.2.1 > Incluir notificaciones electrónicas certificadas para la activación de la Cédula de Ciudadanía Digital y los mensajes que reciba el usuario en la aplicación.

El *Automated Meta Identity System (AMIS)* Mobile SDK debe permitir la recepción de notificaciones electrónicas certificadas las cuales debe ser cifradas de extremo a extremo hacia el dispositivo móvil registrado en el momento de la solicitud de la cédula de Ciudadanía Digital o cuando se haga reposición de este, con el fin de brindar confidencialidad en la comunicación.

Dichas notificaciones serán recibidas desde entidades públicas o privadas habilitadas por la RNEC, sin superar el límite de cinco (5) documentos adjuntos a cada notificación.

Este servicio se proveerá como una bolsa global para RNEC de acuerdo con el número global de cédulas proyectadas a emitir, que más adelante se indica, en una proporción de hasta cuarenta (40) notificaciones electrónicas por cada titular de Cédula digital.

7.2.2 > Incluir la firma digital con Certificado ECDSA

Los certificados de firma digital serán emitidos por una Entidad de Certificación Digital acreditada ante el Organismo Nacional de Acreditación de Colombia (ONAC) con el alcance para la emisión de certificados de persona natural los cuales serán gestionados utilizando el algoritmo de firma digital de curva elíptica (ECDSA).

Los módulos de seguridad (HSM) que gestionen dichos certificados cumplirán con el estándar FIPS 140-2 Nivel 3 y estarán ubicados en el territorio de Colombia, y la información criptográfica de los titulares de las cédulas digitales no será dispuesta en jurisdicciones distintas a la colombiana; el soporte a esos servidores será brindado por profesionales capacitados y certificados por el fabricante, para lo cual se aportará dicha certificación vigente.

Se cumplirá con los siguientes estándares de comunicación segura de información para los servicios de notificación y firma digital a saber: JSON Web Tokens (RFC 7518 y RFC 7519), ya que son de uso común en el mundo de OAuth 2.0 y OpenID Connect, que corresponden a los estándares compatibles tanto con la app Cédula Digital Colombia como con lo descrito en las guías del MinTIC de servicios ciudadanos digitales; así como también con JSON Web Tokens (JWT) para usarse como tokens de identificación o tokens de acceso, el RFC o request for comments por su sigla en inglés, los definidos por Grupo de Trabajo de Ingeniería de Internet -IETF-.

7.2.3 > Incluir servicio de firmado de documentos notificados.

El *Automated Meta Identity System (AMIS)* Mobile SDK permitirá la firma de los documentos que sean adjuntados a través del servicio de notificaciones electrónicas certificadas, empleando el certificado de firma digital emitido y utilizando el algoritmo de firma digital de curva elíptica (ECDSA) acreditado por la Entidad de Certificación Digital; dichos documentos serán almacenados como se indica en el numeral 7.2.9 >.

Este servicio se oferta como una bolsa global para RNEC de acuerdo con el número total de Cédulas proyectadas a emitir, que se indica en el numeral 7.2.12 >, en una cantidad máxima de veinte (20) solicitudes firmadas para cada titular de Cédula Digital.

7.2.4 > Incluir servicio de estampado cronológico en transacciones de firma de documentos.

Las transacciones que se generen dentro del APP y que requieran validez jurídico probatoria llevarán estampado cronológico, cumpliendo lo definido en la Ley 527 de 1999 y Decretos Reglamentarios y lo establecido en el Decreto 620 de 2020, o las normas que las modifiquen o sustituyan, respecto del servicio de autenticación digital, incorporando el algoritmo de firma digital de curva elíptica (ECDSA) con atributo LTV (Long Term Validation).

7.2.5 > Incluir el requisito de reconocimiento por parte de Adobe en la lista (AATL, Adobe Approved Trust List).

Los documentos generados y firmados en formato .PDF, al momento de su apertura y lectura mostrarán en el panel de firma la información que garantizará la confianza de la firma y el estampado cronológico que como atributo posee el documento proveniente del servicio de Adobe; para lo cual la ECD acreditada ante el Organismo Nacional de Acreditación de Colombia (ONAC) que provea dichos servicios tendrá registrados los certificados raíz (root) en la lista de confianza aprobada por Adobe (AATL, Adobe Approved Trust List).

7.2.6 > Incluir la implementación del estándar definido por el Consorcio de Firmado en Nube para la API de Interoperabilidad de servicios de firmado y estampado.

Los nuevos esquemas de digitalización de procesos exigen que los documentos que sean firmados digital o electrónicamente puedan ser albergados en nubes públicas o privadas y que además puedan ser consultados desde dispositivos móviles, por lo que la presente oferta incluye que los certificados digitales emitidos contarán con el reconocimiento de

confianza para dichas nubes y servicios móviles, lo que se logrará mediante el cumplimiento de la norma estándar como la eIDAS en la Unión Europea y 21CFR Parte 11 y del consumo de un API de interoperabilidad desarrollado por el Cloud Signature Consortium; por lo mismo la Entidad de Certificación Digital que emita el servicio contará con la certificación emitida por la Cloud Signature Consortium e indicará que sus certificados digitales cumplen con el reconocimiento de confianza en servicios en nubes públicas, privadas y servicios móviles, para lo cual se presentará dicha certificación o evidencia de registro.

7.2.7 > Incluir el aseguramiento del cumplimiento de estándar ISO para proceso de calidad y seguridad.

La generación de los certificados digitales y servicios de certificación digital cumplirán con lo dispuesto en la Ley 527 de 1999, sus Decretos reglamentarios y lo establecido en el Decreto 620 de 2020 o norma que lo modifique o sustituya, respecto del servicio de autenticación digital cumpliendo con el estándar calidad ISO: 9001 con mínimo alcance para la generación de certificados digitales, servicios de certificación digital (archivo confiable de datos, correo electrónico certificado y estampado cronológico), soluciones para firmar digitalmente; igualmente cumplirá con estándar de seguridad ISO: 27001 con un alcance mínimo de operaciones para la gestión de servicios digitales para productos y servicios de certificados digitales, archivos de datos confiables (archivo, registro, conservación, custodia y anotación de documentos electrónicos transferibles y mensajes de datos), soluciones de firma digital y estampado cronológico.

7.2.8 > Incluir aseguramiento del cumplimiento de estándares para el manejo de datos a través de canales de Internet

El proveedor de los servicios de emisión de certificados digitales y custodia de documentos para la solución propuesta garantizará que cuenta y aplica las buenas prácticas en el manejo seguro de datos a través de servicios expuestos y de acceso a Internet, para lo cual acreditará que cuenta con el sello de auditoría de WebTrust.

7.2.9 > Incluir la implementación del servicio de guarda y custodia de los documentos firmados en el APP.

Las modificaciones al APP incluirán la construcción de un servicio de guarda, custodia y consulta de la totalidad de documentos firmados en el tiempo de uso de la aplicación y su histórico, dicho servicio será asegurado con el *Automated Meta Identity System (AMIS)* Mobile SDK mediante componentes de cifrado que están acreditados ante el Organismo Nacional de Acreditación de Colombia (ONAC) bajo el servicio de Archivo Confiable de Datos.

Este servicio se oferta como una bolsa global para RNEC de acuerdo con el número global de Cédulas proyectadas a emitir, se indica en numeral 7.2.12 >, en una proporción hasta de almacenamiento de 100MB por titular de Cédula digital y las condiciones de su consumo por parte del usuario final serán definidas y parametrizadas por la RNEC.

7.2.10 > Incluir los componentes de aplicación compatibles con IOS y ANDROID

El consumo de los servicios que se amplían dentro del APP de Cédula Digital debe ser compatible con las tecnologías será compatible con las tecnologías y desarrollos realizados por los fabricantes de la aplicación para los sistemas operativos iOS y ANDROID en las versiones vigentes soportadas.

7.2.11 > Incluir los servicios bajo el modelo Infraestructure as a Service.

Los servicios suministrados para mecanismos de firma digital serán provistos bajo el esquema infraestructura como servicio (IaaS) con el fin de garantizar la disponibilidad 7x24x365 y escalabilidad de los mismos.

7.2.12 > Incluir esquemas de capacidad de emisión de acuerdo con la demanda de la RNEC

Los servicios suministrados para los mecanismos de confianza digital estarán en capacidad de emitir con todas las funcionalidades, hasta un millón ciento cuarenta mil (1.140.000) licencias AMIS Mobile SDK perpetua para los usuarios de la App de Cédula Digital Colombia.

Nota: *Nota: Cada licencia AMIS Mobile SDK incluye un Certificado de Firma Digital Centralizado de Persona Natural emitido en algoritmo de curva elíptica con vigencia de dos (2) años por ciudadano, 40 notificaciones electrónicas certificadas, 20 solicitudes de firma de documentos y/o mensaje de datos, 100 MB de almacenamiento, para el consumo que establezca la RNEC.*

7.2.13 > Incluir esquemas de seguridad en la capa de transporte de información

Las comunicaciones de los servicios y el APP estarán protegidos por certificados de tipo TLS (Transport Layer Security) configurado, en versión 1.3 o superior, que protegerán de ataques y garantizarán confiabilidad de los datos; se incluye el escaneo de malware (diario) y vulnerabilidades (semanal) de los servicios publicados.

7.2.14 > Incluir mecanismos para manejo de alta concurrencia.

Los componentes para garantizar la validación y autenticación digital para trámites y operaciones a través de mecanismos de confianza digital a nivel de hardware y software tendrán la capacidad de atender transaccionalidad en esquemas de alta disponibilidad y balanceo de cargas de acuerdo al licenciamiento provisto para las funcionalidades.

7.2.15 > Incluir la seguridad jurídica de la protección tecnológica sobre los desarrollos realizados.

Los componentes de firmado, cifrado, almacenamiento, estampado cronológico, conservación y consulta de las notificaciones electrónicas certificadas y almacenamiento seguro de los documentos electrónicos firmados deben encontrarse dentro de una solución técnica y cada uno de estos componentes deben corresponder a servicios acreditados por

una Entidad de Certificación Digital ante el Organismo Nacional de Acreditación de Colombia – ONAC. El contratista entregará a favor de la RNEC licencia a perpetuidad sobre el ejecutable (*Automated Meta Identity System (AMIS)* Mobile SDK) que se incorpora al App Cedula Digital Colombia, la cual deberá ser suministrada por Entidad de Certificación Digital, protegida legalmente para su explotación y comercialización.

La solución debe garantizar una estabilidad y compatibilidad tecnológica por un periodo de tres (3) años.

7.3 > Entregables

7.3.1 > Primer Entregable

- a. Entrega de documento que contenga Arquitectura de la Solución asociada al *Automated Meta Identity System (AMIS)* Mobile SDK que especifique: representación arquitectónica, visión de la arquitectura, vista de escenarios, vista lógica, vista de implementación, validación de escenarios y vista de datos.

7.3.2 > Segundo Entregable

- a. Entrega del documento que permita identificar en un ambiente de pruebas la integración entre el *Automated Meta Identity System (AMIS)* Mobile SDK y el APP Cédula Digital Colombia, en el cual sea posible evidenciar el uso de los servicios requeridos.
- b. Entrega de los elementos activos de hardware y software necesarios para la implementación de la solución que no correspondan a infraestructura, plataformas o software como servicio (IaaS, PaaS, SaaS) nube, el contratista suministrará la matriz de bienes con el inventario respectivo, igualmente, entregará la carta de cesión de dichos activos, así como el documento donde la ECD se compromete a realizar la administración de los mismos durante la vigencia de los Certificados Digitales Centralizados suministrados a la RNEC.

El Hardware y software a entregar a la RNEC tiene las siguientes características mínimas:

1. Un (1) servidor para alojamiento de bases de datos con las siguientes características mínimas:
 - Procesador con velocidad de procesador de 2.2 GHZ y núcleos de procesador lógicos para mayor rendimiento

- Memoria de última generación DDR4 92 GB con capacidad futura de crecimiento
 - Almacenamiento interno de 600 GB en discos de alta capacidad de lectura y escritura
 - Tarjeta de red de 3 Puertos para conectividad de 1GB
 - 1 puerto de conectividad para la administración inteligente del equipo
 - Fuente de poder redundante y rieles para disposición en rack
 - Sistema de Cifrado Seguro ECDSA (Elliptic Curve Digital Signature Algorithm) provisto por una ECD acreditada ante el ONAC.
2. Un (1) Sistema de Almacenamiento con las siguientes características mínimas:
- Hardware tipo SAN que cuenta con el protocolo de conectividad ISCSI sobre redes TCP/IP
 - Capacidad de Almacenamiento Efectivo de 300TB raid 6
 - 2 Controladoras
 - 1 Puerto SFP
 - 2 Fuentes de poder
 - Software de administración inteligente de almacenamiento, recuperación y custodia de los archivos recopilados, bajo esquemas de cifrado seguro
 - Sistema de Cifrado Seguro (Elliptic Curve Digital Signature Algorithm) provisto por una ECD acreditada ante el ONAC.

El hardware a entregar a la RNEC, será de tecnología reciente y sus características técnicas serán socializadas a la Entidad.

- c. Licencia a perpetuidad sobre la solución técnica, suministrada por Entidad de Certificación Digital a la RNEC, debidamente registrada ante autoridades nacionales, la cual recaerá sobre el ejecutable (*Automated Meta Identity System (AMIS) Mobile SDK*) que se incorpora al App Cedula Digital Colombia, el SDK estará compuesto por: firmado, cifrado, almacenamiento, estampado cronológico, conservación y consulta de las notificaciones electrónicas certificadas y almacenamiento seguro de los documentos electrónicos firmados, cada uno de estos componentes corresponderán a servicios acreditados ante el Organismo Nacional de Acreditación de Colombia – ONAC.
- d. 1.140.000 licencias Automated Meta Identity System (AMIS) Mobile SDK perpetua para los usuarios de la App de Cédula Digital Colombia. Cada licencia *Automated Meta Identity System (AMIS) Mobile SDK* incluye un Certificado de Firma Digital Centralizado de Persona Natural emitido en algoritmo de curva elíptica con vigencia de dos (2) años por ciudadano, 40 notificaciones electrónicas certificadas, 20 solicitudes de firma de documentos y/o mensaje de datos, 100 MB de almacenamiento, para el consumo que establezca la RNEC.

8 / Obligaciones generales de IDEMIA

Con la suscripción del futuro contrato, IDEMIA se compromete a:

8.1 > Obligaciones generales

- a. Realizar a cabalidad todas las obligaciones pactadas en el contrato.
- b. Cumplir con todas las normas que regulan la industria de software y tecnologías en Colombia, tales como el Decreto 1151 de 2008, la Ley 1341 de 2009, la Ley 527 de 1999 y la Directiva 2 de 2019 de la Presidencia de la República, así como también con todas las normas ambientales e internacionales aplicables, y demás normativa concordante con la materia.
- c. Proveer el sistema de comunicaciones para el recurso humano de IDEMIA dispuesto para el proyecto y los elementos tecnológicos como equipos de cómputo, portátiles y periféricos que se requieran para éstos.
- d. Suscribir el acta de inicio de la ejecución de las actividades objeto del contrato de Fortalecimiento, mantenimiento y sostenibilidad de la plataforma PMT II”, así como la adquisición de insumos para la expedición de documentos de identidad en los formatos establecidos por la Registraduría Nacional del Estado Civil.
- e. Suscribir el compromiso de confidencialidad y no divulgación de la información.
- f. Atender los requerimientos, observaciones y demás solicitudes realizadas por la supervisión dentro del alcance del objeto contractual.
- g. Garantizar la contratación de un (1) Gerente de Proyecto y un (1) Responsable de Proyecto de Mantenimiento, ambos con dedicación exclusiva al proyecto, quienes desarrollarán la interlocución para el seguimiento de las actividades del contrato, cuyos perfiles se detallan en las obligaciones específicas asociadas con “Ofrecer la disponibilidad del sistema de Identificación y Registro civil PMT II” y todos sus componentes asociados.
- h. Elaborar y presentar un cronograma de actividades detallado a desarrollar durante la ejecución del contrato, acorde con los requerimientos presentados en el presente

documento técnico, el cual deberá ser entregado y acordado entre las partes dentro de la fase de planeación inicial para la ejecución del contrato.

- i. Asistir a las reuniones programadas por la supervisión, en ejecución de las actividades del contrato a suscribir.
- j. Entregar reportes de las actividades del objeto contractual, según formato de la Registraduría, para efecto de actualizar la información el proyecto de inversión PMT.
- k. Presentar el informe mensual requerido y asistir como mínimo a una (1) mesa directiva mensual convocada por la Entidad, en la cual se analizarán las incidencias críticas detectadas y se determinarán las acciones correctivas necesarias, así mismo, debe reflejar la ejecución del contrato de conformidad con el cronograma aprobado por la Entidad.
- l. Realizar todas las actividades necesarias para el mantenimiento y sostenibilidad de la plataforma del sistema PMTII asociadas con el mantenimiento correctivo, servicio de mesa de ayuda, administración de los sistemas de registro civil e identificación, producción de documentos y todos los componentes asociados.
- m. Atender todas las actividades de carácter logístico (almacenamiento, guardia, custodia, debido uso) y documental (actas de entrada y salida de los insumos), así como las demás actividades asociadas a la operación y producción de los documentos de identidad.
- n. Entregar reporte mensual de las actividades del objeto contractual dentro de los cinco primeros días calendario según formato de la Registraduría, para efecto de actualizar la información el proyecto de inversión PMT
- o. Realizar la entrega de los bienes y/o servicios establecidos en la presente, los cuales deberán cumplir con las especificaciones técnicas exigidas.
- p. Entregar informes de estadísticas de documentos con los datos correspondientes a personalización y entrega de documentos en policarbonato.
- q. Entregar la información que requiera la Registraduría en cuanto al personal vinculado por parte de IDEMIA en desarrollo y ejecución del objeto contractual.
- r. Por solicitud de la Entidad y de común acuerdo con IDEMIA, se analizarán las solicitudes de ajustes o evoluciones al sistema verificando su viabilidad técnica y financiera.

- s. Informar por escrito a la Supervisión de la ocurrencia de fuerza mayor o caso fortuito que pueda afectar la ejecución del objeto contractual.
- t. Cumplir todas las demás obligaciones que correspondan a la naturaleza del contrato.
- u. Capacitar y hacer la transferencia del conocimiento a aquellos funcionarios que la Registraduría designe, para desempeñar algunos roles específicos en la operación de los sistemas de registro civil e identificación en oficina central.
- v. Proporcionar un constante refuerzo de conocimiento y asistencia presencial en sitio central a los funcionarios designados hasta que los mismos adquieran los conocimientos y la experiencia que permita asumir el rol en el sistema.
- w. Acreditar el cabal cumplimiento de las obligaciones relativas al sistema de seguridad social integral, atendiendo lo establecido en el Artículo 23 de la Ley 1150 de 2007 y el Artículo 50 de la Ley 789 de 2002.
- x. Entregar el archivo físico o digital del proyecto (documentos técnicos, jurídicos, administrativos y financieros) generados durante la ejecución del contrato.
- y. Realizar la entrega de los insumos señalados en las especificaciones técnicas con la debida calidad, oportunidad y diligencia de conformidad con los plazos establecidos.
- z. En el evento que los insumos deban ser importados, deberá garantizar la importación y nacionalización mismos allegando los documentos que acrediten el cumplimiento de esta actividad.

8.2 > Obligaciones específicas de IDEMIA

8.2.1 > Realizar el mantenimiento de la plataforma PMT II.

- a. Dar sostenibilidad y realizar el mantenimiento correctivo, así como el soporte técnico del software y hardware a nivel nacional a la plataforma PMT II de la RNEC.

Nota: El mantenimiento correctivo incluye los equipos que integran el parque tecnológico del Sistema de Identificación y Registro Civil de la Plataforma PMT II de acuerdo con lo indicado en este documento técnico.

b. Aspectos específicos Mantenimiento correctivo de equipos y software

- i. Cuando se presente un inconveniente técnico sobre equipos y/o software del sistema registrado a través de la apertura de un caso en la mesa de ayuda, IDEMIA deberá atender en sitio (oficinas centrales) o vía telefónica (a nivel nacional) en un término no superior a dos (2) horas.
- ii. Realizar el diagnóstico o pasos de prueba sugeridos por el fabricante del equipo y/o software ante problemas de funcionamiento irrecuperables, con personal especializado para determinar las inconsistencias en las partes o componentes.
- iii. Cuando un equipo presente fallas sin que se logren superar desde la mesa de ayuda, la Entidad deberá enviar el mismo al centro de diagnóstico central y una vez determinados los daños IDEMIA deberá activarlo en un tiempo no superior a tres (3) días hábiles, de lo contrario, IDEMIA deberá proporcionar, en un término no superior a cuarenta y ocho (48) horas en la sede central de Bogotá, un equipo de las mismas características y configuración en cuanto a hardware y software, en calidad de préstamo mientras se hacen las reparaciones respectivas o sustituirlo de acuerdo al concepto técnico que IDEMIA, con el visto bueno que la Gerencia de Informática emita. Lo anterior, sin que se generen costos adicionales para la RNEC. En los casos que aplique, posterior a la entrega del equipo reparado en la sede central en Bogotá, la Entidad se compromete a regresar el equipo que se entregó en calidad de préstamo en un plazo no mayor a cinco (5) días hábiles.
- iv. Cuando un software o un aplicativo de las oficinas de la Registraduría Nacional del Estado Civil presente fallas, estas deberán solucionarse de conformidad con los tiempos expuestos en esta oferta de servicios.
- v. Reinstalar, en caso de ser necesario, aplicativos y sistemas operativos, bases de datos, entre otros, a todos los equipos que sean reparados o sustituidos y consignarlo en el reporte de mantenimiento, indicando las acciones realizadas y el estado en que queda operando el equipo.
- vi. Realizar el mantenimiento correctivo y preparación del ambiente operativo que conforman el sistema de cotejo y demás subsistemas instalados en el sitio central; así como los demás recursos técnicos instalados a nivel nacional. Garantizar dispositivos para la revisión y arreglo de los equipos entregados producto de la ejecución del Proyecto de Modernización Tecnológica PMT II y aquellos que se encuentren en operación.

- vii. Cuando se requiera la movilización o desplazamiento tanto de los equipos como de los repuestos para cada uno de los bienes (en el marco de este documento técnico), se realizarán por cuenta de la Registraduría salvo para aquellos equipos que superan 30 KG para los cuales IDEMIA asumirá los costos asociados al transporte.
- viii. Gestionar el mantenimiento correctivo de los equipos de la Estación Integrada de Servicios EIS, dispositivos de entrega de documentos (Morphotablet), dispositivos Morphotop y Morpho Smart (MSO), webcam, Captore biométricos MSO, PAD de firmas. En caso de presentarse un daño, los siguientes servicios garantizarán la operación continua de los equipos:
 - o Recepción del equipo en el sitio central: La RNEC enviará el equipo desde la oficina municipal hasta el centro de reparaciones ubicado en las instalaciones del CAN en Bogotá.
 - o Sustitución del equipo recibido: En caso de presentarse daños irremediables o reiterados (máximo 3 veces) que afecten totalmente la funcionalidad del equipo o periférico, reflejada en la hoja de vida del bien tecnológico, se sustituirá el bien, previo concepto técnico y de común acuerdo, con el fin de garantizar la correcta prestación del servicio misional.
 - o Envío hasta el sitio de origen de los dispositivos biométricos (Morphotop, MSO, tablet): Los costos de envío al sitio de origen (Oficinas a nivel nacional) serán asumidos por IDEMIA desde las oficinas del nivel central.
 - o Un equipo se catalogará como dañado y será recibido en el centro de reparaciones del sitio central teniendo en cuenta las directrices definidas en el documento “Procedimiento de Soporte y Mantenimiento PMT II” con referencia 080325SCOL460 “Procedimiento de Soporte y mantenimiento” y sus actualizaciones o en aquel que lo modifique o sustituya.
- c. Elaborar y suscribir las actas de mantenimiento correctivo y las que resulten de casos de soporte de aplicativos PMT y de servicios descritos en la presente, las cuales estarán sujetas al cronograma de actividades.
- d. Aplicar para el servicio de mantenimiento correctivo, los lineamientos y buenas practicas establecidos en estándares internacionales tales como ITIL y COBIT, entre otros.
- e. Realizar actualización del documento “Procedimiento de Soporte y Mantenimiento PMT II” con referencia 080325SCOL460, incluyendo los nuevos componentes agregados en la plataforma PMT II.
- f. Disponer de un lugar e infraestructura debidamente adecuados en la ciudad de Bogotá, que garantice una correcta ejecución de los mantenimientos correctivos de

hardware y software, entendido este último como la corrección de errores de funcionamiento de los aplicativos frente a lo definido en los documentos de especificación de los Sistemas de Identificación y Registro Civil.

- g. Disponer de una plataforma de TESTBED en las instalaciones de IDEMIA para aquellos casos en que se requieran pruebas técnicas de funcionalidad de hardware y software, realizar diagnósticos de mal funcionamiento de los módulos de los sistemas de identificación y registro civil.
- h. Apropiar un stock de repuestos que permita actuar de manera ágil ante daños e imprevistos que afecten la operación normal de los equipos de la solución integral que soporta los Sistemas de Identificación y Registro Civil instalada en todo el territorio nacional, y de esta manera garantizar la sostenibilidad, la operación y funcionalidad de la plataforma PMT II, con los tiempos de respuesta establecidos en este documento, ante las eventualidades consagradas en la presente. Cada equipo del stock de repuestos, una vez utilizado, deberá ser reintegrado para mantener así la disponibilidad permanente de la totalidad del stock de repuestos a lo largo del contrato.
- i. Brindar soporte técnico especializado, directamente o a través de empresas de amplia trayectoria e idoneidad, tales como IBM, DELL, ORACLE, HP, SYBASE (SAP), XEROX, EPSON, entre otras, siendo responsabilidad exclusiva de IDEMIA.
- j. Disponer y mantener operativo el software que permita registrar todos los eventos concernientes a la totalidad de equipos instalados, actualizando así la hoja de vida de los bienes tecnológicos. El software deberá ser de tipo WEB y contar con las imágenes digitalizadas de todos los procesos que se realicen sobre los equipos, así como los respectivos perfiles de consulta (Cuentas de usuario) y de generación de reportes que garanticen al personal de Registraduría, estar informado permanentemente de la trazabilidad respecto a las actividades de recepción y despacho del ciclo que surte el equipo hasta su entrega definitiva.
- k. Suministrar a la Supervisión la información sobre el avance de las actividades de mantenimiento correctivo en forma permanente.
- l. Al finalizar el contrato hacer entrega de las hojas de vida de cada uno de los bienes que conforman el parque tecnológico, actualizadas de conformidad con las actividades desarrolladas de mantenimiento correctivo y actualización de versiones de software.

Considerando que durante la ejecución del contrato puede darse que los bienes que conforman el parque tecnológico sean trasladados o retirados del lugar de operación por parte de la Registraduría sin que dicha circunstancia sea reportada oportunamente a IDEMIA, se aclara que en dichos eventos IDEMIA no asume responsabilidad alguna por dichos bienes que fueron trasladados o retirados sin mediar notificación por parte de la entidad. En este sentido, se exonerará de

cualquier responsabilidad derivada de la imposibilidad material de controlar y seguir la hoja de vida de dichos equipos (lo que impide hacer seguimiento a las acciones sobre dichos equipos).

- m. En todo proceso de mantenimiento correctivo IDEMIA deberá diligenciar los formatos SYMA de los equipos que se reparan, alistan o reciban atención en el centro de reparaciones, cuya copia deberá entregarse a la Gerencia de Informática la cuales deben indicar de forma detallada las versiones, parches o actualizaciones que se realicen al software del sistema operativo, utilitarios o aplicativos y el estado de operación, así como llevar el historial del software instalado y las modificaciones que reciba cada uno de los equipos.

Lo anterior debe garantizar la actualización de inventario de mantenimiento de conformidad con lo definido en el documento “Procedimiento de Soporte y Mantenimiento PMT II” con referencia 080325SCOL460 o en aquel que lo modifique o sustituya.

- n. Atender con diligencia y oportunidad las solicitudes de la Entidad relacionadas con cotizaciones de equipos destinados al uso del PMT, dentro de los treinta (30) días calendario con el fin de que la Entidad atienda los siniestros que se presenten por hurto o pérdida cobijados con las pólizas de la Entidad, para ser presentada ante la Aseguradora y solicitar la reposición de los equipos. Una vez se cuente con la aprobación de la empresa Aseguradora, deberá suministrar el bien dentro del término estipulado en la oferta.

El presente documento técnico, no aplica en el caso de que las causas de la falla o de la avería no sean imputables a IDEMIA o al fabricante de los Equipos. Por lo tanto, IDEMIA no está en la obligación de prestar los servicios de soporte y mantenimiento en los siguientes casos y no hacen parte del objeto de este documento técnico:

- Trabajos de instalación eléctrica relacionados con la solución instalada,
- Trabajos sobre cualquier línea de transmisión de datos conectada a los Equipos, que no estén directamente relacionados con la solución instalada,
- Distribución de equipos de poder y sistemas de aire acondicionado,
- Mantenimiento de cualquier tipo de software o hardware que podría haber sido instalado por el personal de la RNEC en las estaciones EIS suministrado por IDEMIA (por ejemplo, el sistema operativo Windows en las estaciones de trabajo PC, etc.) que sea diferente al software o hardware suministrado por IDEMIA.
- Distribución de Red de área extensa (WAN).
- Comunicación entre los sitios y las ubicaciones.
- Es responsabilidad de la RNEC la adecuación y preparación de sitios para el buen funcionamiento de los equipos instalados, así como el óptimo mantenimiento de dichos sitios, incluida la mitigación de factores ambientales.

8.2.2 > Disponer de un soporte técnico a usuarios

- a. Incorporar un soporte telefónico, online, entre otros, para resolver problemas relacionados con el funcionamiento del hardware y software.
- b. Disponer la operación y respectiva prestación de la atención telefónica de la “Mesa de ayuda” a través de una troncal provista por IDEMIA. Así mismo, poner a disposición un sistema de "encolamiento" en la planta telefónica que permita gestionar las llamadas en espera.
- c. Disponer los accesos al software específico que permite registrar y monitorear todos los eventos concernientes con la totalidad de los soportes brindados tanto en oficinas centrales como a nivel nacional, para que la RNEC tenga la capacidad de verificar y monitorear las tareas ejecutadas por IDEMIA teniendo en cuenta entre otros lo siguiente:
 - Documentar y sistematizar la solución de problemas o dudas que se presenten con los usuarios del servicio.
 - Registrar todos los casos que atiende la mesa de ayuda en el sistema de gestión de mantenimiento y soporte técnico SISTTO.
 - Hacer seguimiento y documentar los casos no solucionados y abiertos en SISTTO
- d. Disponer, mantener y asegurar el funcionamiento de los equipos necesarios para operar la mesa de ayuda de soporte PMT a los Sistemas de Identificación y Registro Civil.
- e. Disponer de una cuenta de correo electrónico y las que se establezcan con posterioridad, con el fin de recibir y dar respuesta a las solicitudes de soporte con respecto a los aplicativos de Identificación, Registro Civil y plataforma tecnológica.
- f. Garantizar la aplicación del documento Procedimiento de Soporte y Mantenimiento PMT II, con referencia 080325SCOL460 o en aquel que lo modifique o sustituya, y las directrices complementarias que sean aplicables y aquellos aspectos relevantes que surjan producto de la ejecución del contrato a suscribir, los cuales forman parte de la metodología que se debe seguir para la gestión del soporte y mantenimiento del Proyecto.
- g. Administrar la infraestructura de hardware y software que compone la plataforma tecnológica para el servicio de mesa de ayuda.

- h. Asignar una (1) persona con experiencia que coordine la gestión, administración y operación de las actividades de la mesa de ayuda, con el fin de revisar y verificar las fallas o problemas detectados en el sistema de gestión de mantenimiento y soporte SISTTO.
- i. Disponer operadores capacitados para atender las llamadas realizadas a la mesa de ayuda en el horario hábil diurno establecido por la RNEC para atención al ciudadano en las oficinas de la Entidad en Colombia.
- j. Brindar asistencia técnica y consultas según se determine conjuntamente en el manejo de las aplicaciones de Registro Civil e Identificación y demás aplicativos de la solución.
- k. Proporcionar de manera personalizada las instrucciones, recomendaciones y soluciones necesarias para que el usuario pueda hacer uso de los Sistemas de identificación y Registro Civil.
- l. Presentar informe mensual de casos atendidos por la mesa de ayuda, discriminando el tipo de caso, afectación, solución dada y sistema atendido, así como los casos abiertos y cerrados en el respectivo mes, en donde se pueda visualizar el caso referido, su tratamiento y el estado en que este se encuentra. De cualquier forma, se deberán establecer, en conjunto, mecanismos para el cierre de los casos abiertos en la vigencia del contrato.
- m. Atender de manera oportuna los casos recibidos en Mesa de Ayuda. Las acciones desde la creación del caso en la mesa de ayuda hasta el inicio de su gestión se espera que sean realizadas un tiempo máximo de 1 día hábil. El tiempo de respuesta no será superior a 3 días hábiles.
- n. Atender las recomendaciones emitidas por la Entidad, para contribuir a la mejora continua en el servicio brindado por la Mesa de Ayuda.
- o. Realizar visitas de seguimiento de común acuerdo con la supervisión, control y refuerzo de la capacitación, en caso que aplique, en oficinas centrales. El control y refuerzo de la capacitación puede ser virtual. El desplazamiento, hospedaje y viáticos de los funcionarios de la RNEC que asistan a las capacitaciones son responsabilidad de RNEC.
- p. Realizar, cuando se requiera, el escalamiento a los niveles 2 y 3 de soporte técnico de acuerdo con lo establecido en el documento "Procedimiento de Soporte y

Mantenimiento PMT II” con referencia 080325SCOL460 o en aquel que lo modifique o sustituya.

- q. Realizar el soporte técnico personalizado, telefónico, electrónico y/o por acceso remoto en el uso de todas las herramientas de procesos, informáticas y tecnológicas entregadas a la RNEC, durante el período de ejecución del contrato.

8.2.3 > Ofrecer la disponibilidad de la plataforma PMT II

- a. Administrar y realizar el soporte técnico de la solución informática del sistema de identificación y registro civil en el sitio central.
- b. Realizar las acciones de soporte a la RNEC en caso de caídas del sistema incluyendo las producidas por fuerza mayor o caso fortuito, en cuyo caso, IDEMIA deberá aportar los servicios técnicos necesarios para soportar las labores de restauración del sistema central a nivel de software, para aquellos aplicativos con licenciamiento ABIS y aplicativos sobre los cuales está estructurado la solución integral.
- c. Monitorear la solución informática del sistema integral implementado por el Proyecto de Modernización Tecnológica PMT II de la RNEC para mantenerlo habilitado y disponible las 24 horas al día, 7 días a la semana (7x24) por el tiempo de duración del contrato.
- d. Realizar las labores de administración necesarias para mantener habilitado y disponible el Sistema Integral de Producción de Documentos (Cédula de Ciudadanía, Tarjeta de Identidad, Registro Civil, Certificaciones, etc.); así como todas las aplicaciones implementadas en el Proyecto de Modernización Tecnológica y posteriores ejecutadas por IDEMIA.
- e. Actualizar las bases de datos del Sistema de Registro Civil e Identificación con la información proveniente de entes con función registral y de identificación, a través del módulo de IRG según especificaciones aprobadas por la Entidad. Si excepcionalmente se presentara una condición de no viabilidad, IDEMIA deberá presentar la argumentación informativa y explicativa que justifique la situación.
- f. Generar y ejecutar la actualización de bases de datos locales, que permitan mantener actualizados todos los subsistemas remotos. En los casos fortuitos o de fuerza mayor la actualización se realizará en coordinación con los responsables técnicos (formadores) de las Delegaciones Departamentales.

- g. Garantizar la operación óptima de la plataforma tecnológica y realizar las acciones a que haya lugar en casos de caídas del sistema, ejecutar las acciones contingentes y asegurar los elementos físicos, técnicos y humanos para restablecer el sistema de acuerdo con el plan de contingencia vigente y al procedimiento correctivo de bienes del proyecto.
- h. Ejecutar todas las actividades para garantizar el funcionamiento correcto y continuo del motor Multibiométrico MorphoBSS “Morpho Biometric Search Services” (MBSS) garantizando la disponibilidad del servicio.
- i. Brindar apoyo al Servicio Nacional de Inscripción – SNI - en atención al Decreto 019 de 2012 modificado por el Decreto 2106 de 2019 con el fin de mantener actualizadas las bases de datos de Registro Civil.
- j. Actualizar el plan de contingencia vigente para los servicios aquí ofertados acorde con las condiciones de operación y riesgo actuales.
- k. Garantizar la ejecución del plan de contingencia vigente para los servicios aquí ofertados, definido para cada subsistema, cuando sea necesario aplicarlo.
- l. Suministrar la información y proponer las medidas necesarias para llevar a cabo las acciones solicitadas por los grupos de validación, individualización, archivo de identificación y jurídica de identificación en un tiempo máximo de 5 días hábiles desde la solicitud, para los casos de relanzamiento y retratamiento, salvo para los casos excepcionales en los que se debe informar el motivo de la excepción y el tiempo estimado de la solución.
- m. Para el caso de los estados “Rechazado Definitivamente” IDEMIA deberá informar semanalmente a la Registraduría Nacional del Estado Civil mediante archivo magnético en Excel el motivo y código de rechazo de las solicitudes de TI y CC por Delegación Departamental, con el objeto de informarlo al ciudadano.
- n. Consignar en el informe mensual el uso del dispositivo de almacenamiento SAN, discriminado por base de datos con la respectiva proyección de uso y disponibilidad.
- o. Administrar el tablero de transferencia automática que conmuta la energía externa para el centro de cómputo ABIS.
- p. Gestionar y dar respuesta a requerimientos de la RNEC tales como cruces o extracción de información, actualización de información, generación de estadísticas, siempre que éstos no obstaculicen el sistema de producción de documentos o el desempeño de las aplicaciones. Estas actividades serán realizadas de común acuerdo con la Entidad como parte de la ejecución del contrato.

Nota: Es importante tener en cuenta que, dependiendo del volumen de información solicitado por la Entidad, éste puede tomar varios días en su procesamiento y podría tener que ejecutarse en horarios no hábiles para no interrumpir la operación del sistema.

- q. Servir de soporte técnico a la RNEC para coadyuvar en la realización de campañas en oficinas remotas.
- r. Realizar las copias de seguridad definidas (totales e incrementales) para el sistema, con la periodicidad establecida siguiendo los documentos de “Plan de seguridad PMT II” y de “Políticas de Seguridad Informática” vigentes para los servicios aquí ofertados, o aquellos que los modifiquen o sustituyan.
- s. Contar con un plan de respaldo y verificación del respaldo, según procedimiento DRL, y presentar evidencias de restauración realizadas para las bases de datos que se encuentren en operación, producto del desarrollo de la solución integral que soporta los Sistemas de Identificación y Registro Civil.
- t. Verificar y monitorear que las actualizaciones e integridad de las bases de datos y de tablas de referencia se estén ejecutando de conformidad con los manuales y procedimientos establecidos en el Proyecto de Modernización Tecnológica en su segunda fase PMT II. Brindar el apoyo técnico necesario de acuerdo con los nuevos servicios que la RNEC deberá prestar a los entes externos, de conformidad con los presentados por el Gobierno Nacional mediante Decreto 019 de 2012 modificado por el Decreto 2106 de 2019, por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública para los siguientes servicios:
 - i. Prestar apoyo técnico en la labor de ingreso de la administración del S. N. I. (Servicio Nacional de Inscripción), que conlleve a garantizar los óptimos flujos en la incorporación, procesamiento y captura de la información para los Registros Civiles de Nacimiento, Matrimonio y Defunción.
 - ii. Prestar apoyo técnico en la búsqueda de soluciones para la prestación e integración del servicio tecnológico autenticación biométrica.
 - iii. Poner a disposición la información desde la interfaz MTR SIRC que permita la realización de los procesos de actualización con ANI
- u. Brindar apoyo y soporte técnico a LA REGISTRADURIA en relación con lo establecido en el decreto 019 de 2012 modificado por el Decreto 2106 de 2019, reglamentario y otros que impacte el servicio a la ciudadanía en materias tales como biometría y acceso a las bases de datos, cuya información proviene del sistema PMT II.

v. Administrar los siguientes aplicativos:

- i. Identificación: Motor Multibiométrico MorphoBSS “Morpho Biometric Search Services” (MBSS facial y dactilar), MTR, CMS, ICPS, IDPS, Web Services, GED, SSC – Parte Identificación, Interfaz MTR-SIRC-ANI, INTERAFIS, Réplica I de la Base del MTR para el Web Service del Sitio Central, Aplicativos asociados a la operación del Workflow, Web Service para autenticación biométrica, BIOINTER, Sistema HLED Web Morpotablet, sistema de la Estación Integrada de Servicios – EIS, Aplicación móvil para la reimpresión de documentos en Teslin, aplicaciones para la identidad digital y para la prestación de servicios de autenticación facial para entidades externas – MBSS Facial.
 - ii. Registro Civil: SIRC, GED, SSC – Parte Registro Civil, Línea de digitalización, Réplica total de la base de datos de Registro Civil, Web Service.
- w. Teniendo en cuenta la complejidad de las actividades que deberá realizar IDEMIA sobre la plataforma tecnológica implementada, deberá contar como mínimo con un (1) profesional de tiempo completo vinculado al proyecto en cada uno de los siguientes roles:

No.	ROL	PERFIL
1.	Gerente de Proyecto	Profesional en áreas de ingeniería o administración con estudios de Postgrado en Gestión de Proyectos Informáticos o Gestión de Tecnología o Certificación Internacional PMI de Gestión de Proyectos (PMP). 5 años de experiencia en gerencia o implementación de proyectos informáticos, alto nivel de inglés, con disponibilidad exclusiva para el proyecto.
2.	Responsable de Mantenimiento para el Proyecto	Profesional en ingeniería de sistemas, administración o carreras afines, con estudios de Postgrado en Gestión de Proyectos Informáticos o Gestión de Tecnología o Certificación Internacional PMI de Gestión de Proyectos (PMP). 5 años en administración o implementación de proyectos informáticos, alto nivel de inglés, con disponibilidad exclusiva para el proyecto.
3.	Jefe de Administración - ID	Profesional en ingeniería de sistemas o carreras afines con 5 años de experiencia en administración de sistemas Windows y AIX, configuración, diseño y gestión de servicios, amplios conocimientos en administración de bases de datos con certificación en ORACLE 11 G o superior. Conocimientos generales en ORACLE LINUX y Sistemas de Respaldo TSM, aplicación de políticas de

No.	ROL	PERFIL
		seguridad, respaldo y recuperación de la información, monitoreo y detectar problemas en los sistemas, dirección de grupo, habilidades gerenciales, alto nivel de inglés.
4.	Jefe de Administración – RC	Profesional en ingeniería de sistemas o carreras afines con 5 años de experiencia en administración de sistemas, Windows y Oracle Linux configuración, diseño y gestión de servicios, amplios conocimientos y administración de bases de datos con certificación en SYBASE ASE 15. Con conocimientos en Oracle Linux y Sistemas de Respaldo TSM. Aplicación de políticas de seguridad, respaldo y recuperación de la información, monitorear y detectar problemas en los sistemas, dirección de grupo, habilidades gerenciales, alto nivel de inglés.
5.	DBA – ID	Profesional en Ingeniería de sistemas o carreras afines con 4 años de experiencia en administración de bases de datos con certificación en ORACLE 10 G y/o 11 G o superior, dominio de PLSQL, sistemas operativos AIX, Oracle Linux y Windows server, alto nivel de inglés.
6.	DBA – RC	Profesional en ingeniería de sistemas o electrónico con 4 años de experiencia en administración de bases de datos con certificación en SYBASE ASE 15, sistemas operativos AIX y Windows 2003 server, alto nivel de inglés.
7.	Jefe de Producción	Profesional en ingeniería de sistemas, administración o carreras afines, con experiencia en actividades de mantenimiento de máquinas de producción, laminado y troquelado en serie, así como manejo de tecnología LASINK, nivel de inglés medio.
8.	DBA - BIOINTER	Profesional en ingeniería de sistemas, electrónico o afines, con 5 años en experiencia como Oracle DBA, certificación en Oracle Enterprise 11 G o superior. 2 años de experiencia en procesos de replicación y sincronización de bases de datos Oracle.

No.	ROL	PERFIL
		2 años de experiencia específica en administración de base de datos, Oracle a partir de la certificación en Oracle 11 G o superior. 1 año de experiencia con sistemas operativos Oracle Linux o Windows Server. Nivel de inglés intermedio. Disponibilidad 5 días a la semana 8 horas al día (5x8). Experiencia en instalaciones y administración de las herramientas Oracle (Advance Security y Database Vault)

- x. Brindar soporte al software Web Service para el acceso de la base de datos biométrica y soporte de la sincronización de la base de datos (BIOINTER) directamente por la mesa de ayuda o mediante el DBA responsable de la base de datos BIOINTER.
- y. Brindar los niveles 2 y 3 de soporte para software aplicativo y la integridad de la base de datos réplica, de acuerdo con lo establecido en el documento "Procedimiento de Soporte y Mantenimiento PMT II" vigente o en aquel que lo modifique o sustituya.
- z. Prestar el servicio de soporte a la infraestructura de contingencia, (sitio, hardware y software de terceros), en caso de ser necesaria su utilización en función de las definiciones del plan de contingencia vigente.
- aa. Prestar el mantenimiento correctivo de los módulos de software aplicativo desarrollado.
- bb. Administrar la base de datos intermedia (BIOINTER) y entregar a la RNEC estadísticas mensuales a partir de los logs generados que evidencien la replicación desde la base de datos MTR a la base de datos intermedia (BIOINTER) en sitio central.
- cc. Administrar y entregar a la RNEC estadísticas mensuales a partir de los logs generados que evidencian la multi-sincronización desde la base de datos intermedia (BIOINTER) a las bases de datos replicadas para autenticación biométrica dispuestas para las entidades públicas o entidades particulares con funciones públicas.
- dd. Garantizar la actualización a diario del código de novedad (Vigencia) del documento de Identidad, generado por el Archivo Nacional de Identificación (ANI) y que debe ser reflejado en la base de datos intermedia (BIOINTER) a través del MTR en sitio central.

- ee. Garantizar la sincronización a diario mediante los Jobs que permitan actualizar los deltas entre la base de datos del MTR a la base de datos intermedia (BIOINTER) destinada para sincronizar las bases de datos para autenticación biométrica (Réplica).
- ff. Dar soporte a la RNEC en el proceso de puesta a punto e instalación de nuevos operadores biométricos en la ciudad de Bogotá, D.C, Sitio Central CAN.
- gg. Entregar a la RNEC, cuando ésta lo determine, y en caso de ser requerido, una copia de la base de datos intermedia (BIOINTER) en producción, en el formato y en el medio de almacenamiento, con las seguridades acordadas y generadas con herramientas ORACLE. Como parte del proceso de puesta en producción de los operadores biométricos IDEMIA deberá realizar la validación de las especificaciones técnicas de la plataforma del operador biométrico con el objetivo de asegurar la compatibilidad de los diferentes mecanismos de replicación y acceso a la información. Lo anterior teniendo en cuenta que los operadores biométricos deberán garantizar el uso de la base de datos replicada bajo las condiciones de seguridad establecidas en la Resolución 5633 de 2016.
- hh. Realizar, cuando la RNEC lo determine, los cambios de configuración a que haya lugar, incluyendo la intervención de Oracle Streams para permitir la propagación y el manejo de datos en la base de datos intermedia (BIOINTER) en sitio central, para garantizar la sincronización de esta con las bases de datos replicadas para autenticación biométrica dispuestas para las entidades públicas o entidades particulares con funciones públicas.
- ii. Brindar acompañamiento técnico a la Entidad para la realización de pruebas entre el sitio central y el Data Center de los operadores biométricos, que garanticen la sincronización de la base de datos intermedia (BIOINTER) a la base de datos replicada para autenticación biométrica dispuestas para las entidades públicas o entidades particulares con funciones públicas.
- jj. Restablecer la base de datos intermedia en caso de afectación alguna del hardware entregado, con el mismo nivel de servicio del contrato.
- kk. Prestar los servicios de soporte y mantenimiento correctivo para las aplicaciones y el hardware de:
 - i. Personalización de documentos en policarbonato
 - ii. Identidad digital y su gestión
 - iii. MBSS para la prestación de servicios de autenticación facial a terceros
 - iv. Nuevas funcionalidades incluidas en esta oferta.
- ll. Prestar servicios de soporte y mantenimiento correctivo a la Plataforma Tecnología para Registro Civil – PMT II
La entidad actualmente cuenta con una solución tecnológica “Cliente – Servidor” para la plataforma para Registro Civil que permite a través de diferentes estaciones

y servidores dar servicio a la actividad misional en las oficinas de la Registraduría Nacional del Estado Civil que conforman parte del Proyecto de Modernización Tecnológica Fase II (PMT II), así como un “Web Service” de consulta que presta el servicio a terceros de datos en las bases de datos de Registro Civil en la solución que administra IDEMIA.

- i. Se prestarán los servicios a la solución Cliente-Servidor que hoy en día cuenta con un licenciamiento que es distribuido a las estaciones de Registro Civil pertenecientes al PMT II de hasta 1,989 licencias para Estación. Estas son utilizadas actualmente en su totalidad por las estaciones SIRC cliente (multi-estación y mono estación).
- ii. Se prestarán los servicios de soporte y mantenimiento correctivo al Servicio Web WS RCX, el que se define en un Documento de Control de Interfaces (ICD) que permite la integración de aplicaciones de terceros (internos y externos) para consultas de la base de datos del sistema del Registro Civil con alrededor de 11 métodos de consulta que están descritos en el “Documento de Control de Interfaces (IDC) y documento de Definición de Requisitos (RDD) 2017_2000026358 – V 2.0 – 26. May.2017”. Las características de este servicio son:
 - Las consultas de los métodos RCN, RCM, RCD, VRCN, VRCM, VRCD, VNIPRCN y VTI, tienen un tiempo promedio de respuesta de 20 segundos, este tiempo transcurrido es contado desde la recepción de la solicitud al servidor y el envío de la respuesta del servidor.
 - La consulta de Núcleo Familiar es igual o menor a 90 segundos, este tiempo transcurrido es contado desde la recepción de la solicitud al servidor y el envío de la respuesta del servidor.
 - El promedio de transacciones que pueden ser atendidas por la Servicio Web WS RCX es de 5,850 por hora.

8.2.4 > Cargar información del trámite del colombiano

Las actividades de carga de información del trámite del colombiano se realizarán de acuerdo con el proceso de personalización que se esté realizando según sea su aplicación para producción de documentos en Teslin o para producción de documentos en policarbonato.

- a) Realizar y sostener la operación de la fábrica y subsistemas en el sitio central.
- b) Administrar y gestionar los insumos de producción y envíos de documentos de identidad recibidos de la Registraduría y generar reportes de la utilización de los mismos.

- c) Administrar la fábrica de producción de documentos de identidad mediante un Grupo de Supervisores para el esquema de operación en oficinas centrales, así: - jefe de producción, supervisor de CCD (IQC, SQC y RDC), supervisor de fábrica (troquelado y laminado, empaque), supervisor en CQC y envíos (control casilleros, CQC, certificación, LMU, LEX, LEN y Distribución),
- d) Realizar el cargue de la información proveniente de los centros de acopio, Estación Integrada de Servicios – EIS, o Aplicación móvil para reimpresión de documentos en Teslin, operar el cliente control calidad de los datos, Operar el cliente IQC (Image Quality Control), Operar el cliente SQC (Signature Quality Control).
- e) Procesar las excepciones (a nivel sistema).
- f) Producir los documentos de identidad en teslin impresos, laminados y troquelados, además de documentos de identidad en policarbonato personalizado con tecnología LASINK.
- g) Ejecutar la labor de control de casilleros.
- h) Realizar el control calidad de los documentos CQC.
- i) Realizar el procedimiento de certificación.
- j) Generación LMU-LEX-LEN.
- k) Realizar las labores de empaque.
- l) Preparar los documentos para distribución.
- m) Entrega de los Documentos a coordinación de envíos.
- n) Digitalizar las actas LMU LEN LEX generadas en fábrica, así como las colillas o comprobantes de entrega debidamente indexadas

8.2.5 > Validar información del tramite

- a. Realizar las labores de retratamiento de foto y firma.
- b. Realizar la depuración a través de un rechazo definitivo de las solicitudes de CQC con imposibilidad de retratamiento en el módulo CARD-RET de foto y firma.

8.2.6 > Producir documentos de identificación

- a. Realizar un flujo de producción promedio de hasta diez y ocho mil (18.000) documentos al día distribuidos así: hasta catorce mil (14.000) documentos en promedio expedidos en formato Teslin y hasta cuatro mil (4.000) documentos en promedio de seguridad personalizados en policarbonato, es decir, un aproximado semanal de noventa (90.000) documentos de identidad sumada la producción en Teslin y la producción en policarbonato, teniendo en cuenta los planes de producción, la disponibilidad de insumos y la demanda de trámites.
- b. Trabajar como mínimo cinco (5) días a la semana de lunes a viernes, garantizando el promedio semana de producción.
- c. Contratar el personal requerido para la operación de la línea de producción.
- d. Recibir de la Registraduría el inventario de insumos de producción y envío de documentos de identidad disponibles al momento de iniciar el contrato.
- e. Entregar a la Registraduría el inventario de insumos de producción y envío de documentos de identidad disponibles al momento de finalizar el contrato, con la actualización de todos los movimientos surtidos durante la ejecución del mismo.
- f. Realizar el acompañamiento al personal técnico del sitio central, indicado por la supervisión y establecer una interlocución permanente que permita a estos funcionarios tomar decisiones, solucionar o aclarar aspectos específicos y particulares relacionados con las herramientas de operación del sistema instalado.

Nota: *El contratista deberá presentar a la entidad un informe mensual de los insumos utilizados para la producción de documentos de identidad, en especial aquellos resultantes del retail, rechazo y desperdicios y conformación de lotes de producción, proponiendo estrategias y actividades encaminadas a la reducción de los porcentajes propios del proceso de producción (dichos porcentajes se definen en el documento denominado: "Control de insumos procesados de producción de documentos" referencia 2015_000006427).*

8.2.7 > Robustecimiento de la App Cédula Digital

- a. Entrega de documento que contenga Arquitectura de la Solución asociada al *Automated Meta Identity System (AMIS)* Mobile SDK que especifique: representación arquitectónica, visión de la arquitectura, vista de escenarios, vista lógica, vista de implementación, validación de escenarios y vista de datos.

- b. Entrega del documento que permita identificar en un ambiente de pruebas la integración entre el *Automated Meta Identity System (AMIS)* Mobile SDK y el APP Cédula Digital Colombia, en el cual sea posible evidenciar el uso de los servicios requeridos.
- c. Entrega de los elementos activos de hardware y software necesarios para la implementación de la solución que no correspondan a infraestructura, plataformas o software como servicio (IaaS, PaaS, SaaS) nube, el contratista suministrará la matriz de bienes con el inventario respectivo, igualmente, entregará la carta de cesión de dichos activos, así como el documento donde la ECD se compromete a realizar la administración de los mismos durante la vigencia de los Certificados Digitales Centralizados suministrados a la RNEC.
- d. Licencia a perpetuidad sobre la solución técnica, suministrada por Entidad de Certificación Digital a la RNEC, debidamente registrada ante autoridades nacionales, la cual recaerá sobre el ejecutable (*Automated Meta Identity System (AMIS)* Mobile SDK) que se incorpora al App Cedula Digital Colombia, el SDK estará compuesto por: firmado, cifrado, almacenamiento, estampado cronológico, conservación y consulta de las notificaciones electrónicas certificadas y almacenamiento seguro de los documentos electrónicos firmados, cada uno de estos componentes corresponderán a servicios acreditados ante el Organismo Nacional de Acreditación de Colombia – ONAC.
- e. 1.140.000 licencias *Automated Meta Identity System (AMIS)* Mobile SDK perpetua para los usuarios de la App de Cédula Digital Colombia. Cada licencia *Automated Meta Identity System (AMIS)* Mobile SDK incluye un Certificado de Firma Digital Centralizado de Persona Natural emitido en algoritmo de curva elíptica con vigencia de dos (2) años por ciudadano, 40 notificaciones electrónicas certificadas, 20 solicitudes de firma de documentos y/o mensaje de datos, 100 MB de almacenamiento, para el consumo que establezca la RNEC.



www.idemia.com

