Los suscritos **ALEXANDER VEGA ROCHA**, mayor de edad, con domicilio y residencia en la ciudad de Bogotá D.C., identificado con la cédula de ciudadanía número 11.202.241 de Chía - Cundinamarca, actuando en nombre y representación de la Registraduría Nacional del Estado Civil, en su calidad de Registrador Nacional del Estado Civil, según Acuerdo Nro. 25 del 13 de octubre del 2019 "Por medio de la cual se designa Registrador Nacional del Estado Civil", emitido por los presidentes de la Corte Constitucional, Corte Suprema de Justicia y Consejo de Estado, posesionado según consta en el acta de fecha 18 de noviembre de 2019, con facultades legales para suscribir este documento y en ejercicio de las atribuciones propias del cargo, quien en adelante y para todos los efectos de este convenio se denominará la Registraduría, de una parte, y por la otra, General **WILLIAM RENÉ SALAMANCA RAMÍREZ**, identificado con cédula de ciudadanía Nro. 6.770.835 de Tunja - Boyacá, actuando en calidad de Director General de la Policía Nacional, Entidad identificada con NIT 800.141.397-5, nombrado mediante Decreto Nro. 694 del 09 de mayo de 2023 y Acta de posesión Nro. 096-23 del 10 de mayo de 2023, quien para efectos de este convenio se denominará la Policía Nacional, hemos acordado celebrar el presente convenio Interadministrativo de cooperación, previas las siguientes:

CONSIDERACIONES:

1. Que el artículo 15 de la Constitución Política de Colombia establece que "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas".
2. Que el artículo 93 de la Constitución Política de Colombia establece que: "Los tratados y convenios internacionales ratificados por el Congreso, que reconocen los derechos humanos y que prohíben su limitación en los estados de excepción, prevalecen en el orden interno. Los derechos y deberes consagrados en esta Carta se interpretarán de conformidad con los tratados internacionales sobre derechos humanos ratificados por Colombia".
3. Que el inciso tercero del artículo 113 de la Constitución Política de Colombia señala que los diferentes órganos del Estado tienen funciones separadas, pero colaboran armónicamente para la realización de sus fines.
4. Que el artículo 116 de la Constitución establece que "La Corte Constitucional, la Corte Suprema de Justicia, el Consejo de Estado, la Comisión Nacional de Disciplina Judicial, la Fiscalía General de la Nación, los Tribunales y los Jueces, administran Justicia. También lo hace la Justicia Penal Militar".
5. Que el artículo 209 de la Constitución Política de Colombia establece que la función administrativa está al servicio de los intereses generales y se desarrolla con base en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad.
6. Que el artículo 218 de la Constitución establece que: "(...) La Policía Nacional es un cuerpo armado permanente de naturaleza civil, a cargo de la Nación, cuyo fin primordial es el mantenimiento de las condiciones necesarias para el ejercicio de los derechos y libertades públicas, y para asegurar que los habitantes de Colombia convivan en paz (...)".
7. Que de acuerdo al numeral 8 del artículo 250 de la Constitución Política de Colombia, la Fiscalía General de la Nación tiene la función de "Dirigir y coordinar las funciones de Policía Judicial que en forma permanente cumple la Policía Nacional y los demás organismos que señale la ley".
8. Que el artículo 266, establece que: "El Registrador Nacional del Estado Civil (...) ejercerá las funciones que establezca la ley, incluida la dirección y organización de las elecciones, el registro civil y la identificación de las personas, así como la de celebrar contratos en nombre de la Nación, en los casos que aquella disponga".

9. Que la Ley 16 de 1972 "Por medio de la cual se aprueba la Convención Americana sobre Derechos Humanos - Pacto de San José de Costa Rica", firmado en San José, Costa Rica el 22 de noviembre de 1969", establece que Colombia se compromete a respetar los derechos y libertades reconocidos en la Convención Americana sobre Derechos Humanos, y a garantizar su libre y pleno ejercicio.
10. Que la Ley 32 de 1985 "Por medio de la cual se aprueba la "Convención de Viena sobre el Derecho de los Tratados", suscrita en Viena el 23 de mayo de 1969", aprueba la Convención de Viena sobre el Derecho de los Tratados.
11. Que la Ley 62 de 1993 "Por la cual se expiden normas sobre la Policía Nacional, se crea un establecimiento público de seguridad social y bienestar para la Policía Nacional, se crea la Superintendencia de Vigilancia y Seguridad Privada y se reviste de facultades extraordinarias al Presidente de la República", establece en su artículo 19: "La Policía Nacional está instituida para proteger a todas las personas residentes en Colombia, garantizar el ejercicio de las libertades públicas y los derechos que de éstas se deriven, prestar el auxilio que requiere la ejecución de las leyes y las providencias judiciales y administrativas y ejercer, de manera permanente, las funciones de: Policía Judicial, respecto de los delitos y contravenciones: educativa, a través de orientación a la comunidad en el respecto a la ley; preventiva, de la comisión de hechos punibles; de solidaridad entre la Policía y la comunidad; de atención al menor, de vigilancia urbana, rural y cívica; de coordinación penitenciaria; y, de vigilancia y protección de los recursos naturales relacionados con la calidad del medio ambiente, la ecología y el ornato público, en los ámbitos urbano y rural".
12. Que el artículo 31 de la Ley 62 de 1993 "Por la cual se expiden normas sobre la Policía Nacional, se crea un establecimiento público de seguridad social y bienestar para la Policía Nacional, se crea la Superintendencia de Vigilancia y Seguridad Privada y se reviste de facultades extraordinarias al Presidente de la República", establece "(...) Las autoridades departamentales y municipales podrán contribuir para la adquisición de equipos, dotaciones, mejoramiento de instalaciones vivienda fiscal, apoyo logístico y bienestar de la Policía Nacional. También podrá celebrar convenios con la Nación para mejorar la seguridad pública sin perjuicio de las obligaciones que correspondan aquella".
13. Que la Ley 38 de 1993 "Por la cual se unifica el sistema de dactiloscopia y se adopta la Carta Dental para fines de identificación", establece el sistema de dactiloscopia.
14. Que de acuerdo con artículo 4 de la Ley 489 de 1998 "Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio", que establece las "Finalidades de la función administrativa. La función administrativa del Estado busca la satisfacción de las necesidades generales de todos los habitantes, de conformidad con los principios, finalidades y cometidos consagrados en la Constitución Política. Los organismos, entidades y personas encargadas, de manera permanente o transitoria, del ejercicio de funciones administrativas deben ejercerlas consultando el interés general", y el artículo 6 (Principio de coordinación) de la Ley 489 de 1998 "(...) las autoridades administrativas deben garantizar la armonía en el ejercicio de sus respectivas funciones con el fin de lograr los fines cometidos estatales". En consecuencia, prestarán su colaboración a las demás entidades para facilitar el ejercicio de sus funciones y se abstendrán de impedir o estorbar su cumplimiento por los órganos, dependencias, organismos y entidades titulares.
15. Que el artículo 95 de la Ley 489 de 1998 prevé la posibilidad de que las entidades públicas se asocien con el fin de "... cooperar en el cumplimiento de funciones administrativas o de prestar conjuntamente servicios que se hallen a su cargo, mediante la celebración de convenios interadministrativos", por ende, aplicable a la Registraduría Nacional del Estado Civil y a la Policía Nacional de Colombia, al igual que el artículo 96 "(...) Las entidades estatales, cualquiera sea su

naturaleza y orden administrativo podrán, con la observancia de los principios señalados en el artículo 209 de la Constitución, asociarse con personas jurídicas particulares, mediante la celebración de convenios de asociación o la creación de personas jurídicas, para el desarrollo conjunto de actividades en relación con los cometidos y funciones que les asigna a aquellas la ley (...)".

16. Que la Ley 906 de 2004 "Por la cual se expide el Código de Procedimiento Penal", establece en el artículo 200 que "Corresponde a la Fiscalía General de la Nación realizar la indagación e investigación de los hechos que revistan características de un delito que lleguen a su conocimiento por medio de denuncia, querella, petición especial o por cualquier otro medio idóneo. En desarrollo de la función prevista en el inciso anterior a la Fiscalía General de la Nación, por conducto del fiscal director de la investigación, le corresponde la dirección, coordinación, control jurídico y verificación técnico-científica de las actividades que desarrolle la Policía Judicial, en los términos previstos en este código. Por Policía Judicial se entiende la función que cumplen las entidades del Estado para apoyar la investigación penal y, en el ejercicio de las mismas, dependen funcionalmente del Fiscal General de la Nación y sus delegados. Los organismos oficiales y particulares están obligados a prestar la colaboración que soliciten las unidades de Policía Judicial, en los términos establecidos dentro de la indagación e investigación para la elaboración de los actos urgentes y cumplimiento a las actividades contempladas en los programas metodológicos, respectivamente; so pena de las sanciones a que haya lugar".
17. Que el artículo 201 de la norma ibidem, establece que "Ejercen permanentemente las funciones de Policía Judicial los servidores investidos de esa función, pertenecientes al Cuerpo Técnico de Investigación de la Fiscalía General de la Nación y a la Policía Nacional, por intermedio de sus dependencias especializadas. Parágrafo 1 En los lugares del territorio nacional donde no hubiere miembros de Policía Judicial de la Policía Nacional, estas funciones las podrá ejercer la Policía Nacional", de igual forma, en el artículo 251 "...para la identificación de personas se podrán utilizar los diferentes métodos que el estado de la ciencia aporte, y que la criminalística establezca en sus manuales, tales como las características morfológicas de las huellas digitales, la carta dental y el perfil genético presente en el ADN, los cuales deberán cumplir con los requisitos del artículo 420 de este código respecto de la prueba pericial".
18. Que en el artículo 298 de la norma citada, expresa: "...El mandamiento escrito expedido por el juez correspondiente indicará de forma clara y sucinta los motivos de la captura, el nombre y los datos que permitan individualizar al indiciado o imputado, cuya captura se ordena, el delito que provisionalmente se señale, la fecha de los hechos y el fiscal que dirige la investigación. La orden de captura tendrá una vigencia máxima de un (1) año, pero podrá prorrogarse tantas veces como resulte necesario, a petición del fiscal correspondiente, quien estará obligado a comunicar la prórroga al organismo de Policía Judicial encargado de hacerla efectiva. La Policía Judicial puede divulgar a través de los medios de comunicación las órdenes de captura. De la misma forma el juez determinará si la orden podrá ser difundida por las autoridades de policía en los medios de comunicación, durante su vigencia".
19. Que la Ley 1098 de 2006 "Por la cual se expide el Código de la Infancia y la Adolescencia", tiene por finalidad garantizar a los niños, a las niñas y a los adolescentes su pleno y armonioso desarrollo para que crezcan en el seno de la familia y de la comunidad, en un ambiente de felicidad, amor y comprensión. Prevalecerá el reconocimiento a la igualdad y la dignidad humana, sin discriminación alguna.
20. Que los artículos 25, 47, 142, 144 y 145 de la ley 1098 de 2006, relacionado con la identificación de los menores infractores, se dispuso en la misma como responsables de los trámites en materia investigativa al Grupo de Policía de Infancia y Adolescencia de la Policía Nacional, quienes deberán proceder a su identificación y a la recolección de los datos en las bases de datos disponibles para la misma, en particular las administradas por la Registraduría Nacional

del Estado Civil, siguiendo los lineamientos de la Ley 906 de 2004 en las circunstancias que apliquen.

21. Que la Ley 1341 de 2009 "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones –TIC–, se crea la agencia nacional de espectro y se dictan otras disposiciones", establece la definición de tecnologías de la información y las comunicaciones y los principios aplicables.
22. Que la Ley 1407 de 2010 "Por la cual se expide el Código Penal Militar", establece los delitos y el procedimiento para sancionar conductas punibles realizadas por funcionarios de la Fuerza Pública.
23. Que la Ley 1437 de 2011 "Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo", establece el procedimiento para la expedición de actos administrativos y el actuar de la administración.
24. Que de conformidad con lo previsto por el artículo 266 de la Constitución Política, en concordancia con el Decreto Ley 2241 de 1986 y el Decreto 1010 de 2000, corresponde a la Registraduría Nacional del Estado Civil ejercer, entre otras, la función de organizar y dirigir el registro civil y la identificación de los colombianos.
25. Que el artículo 213 del Código Electoral establece que: "Toda persona tiene derecho a que la Registraduría le informe sobre el número, lugar y fecha de expedición de los documentos de identidad pertenecientes a terceros. Tienen carácter reservado las informaciones que reposen en los archivos de la Registraduría referentes a la identidad de las personas, como son sus datos biográficos, su filiación y fórmula dactiloscópica. De la información reservada sólo podrá hacerse uso por orden de autoridad competente; con fines investigativos, los jueces y funcionarios de policía y de seguridad tendrán acceso a los archivos de la Registraduría".
26. Que el artículo 99 de la Ley 1453 de 2011, establece que "en los eventos en que el capturado no presente documento de identidad, la Policía Judicial tomará el registro decadactilar y verificará la identidad con documentos obtenidos en la Registraduría Nacional del Estado Civil y sus delegadas, de manera directa, o a través de la consulta de los medios técnicos o tecnológicos de los que se dispongan o tengan acceso" aunado a lo anterior la Fiscalía General de la Nación, mediante resolución 3329 de 2007, determinó que la Policía Judicial debería acceder a los sistemas de información a los cuales tienen acceso por intermedio de la Registraduría, a fin de lograr la correcta identificación de las personas vinculadas a los procesos investigativos para evitar errores judiciales.
27. Que la Ley Estatutaria 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales", establece en el artículo 2 "...El régimen de protección de datos personales que se establece en la presente ley no será de aplicación (...) b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo; c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia (...) Parágrafo. Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley."
28. Que el artículo 10 de la norma ibidem, establece: "...Casos en que no es necesaria la autorización. La autorización del Titular no será necesaria cuando se trate de: a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial; b) Datos de naturaleza pública;

29. Que la Ley 1621 de 2013 "Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones", define en su artículo 42 la "Colaboración de las Entidades Públicas y Privadas. Los organismos de inteligencia podrán solicitar la cooperación de las entidades públicas y privadas para el cumplimiento de los fines enunciados en esta Ley. En caso de que la información solicitada por el organismo de inteligencia esté amparada por la reserva legal, estos organismos y las entidades públicas y privadas podrán suscribir convenios interinstitucionales de mutuo acuerdo. En cualquier caso, la entrega de tal información no constituirá una violación a la reserva legal, toda vez que la misma continuará bajo este principio, al cual se encuentran obligados los servidores públicos de inteligencia y contrainteligencia en virtud de lo dispuesto en la presente Ley".
30. Que el Congreso de la República estableció en la Ley 1753 de 2015 "Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 Todos por un nuevo país", artículo 159 señalando que: "Para el desarrollo de los planes, programas y proyectos incluidos en el Plan Nacional de Desarrollo y en general para el ejercicio de las funciones públicas, las entidades públicas y los particulares que ejerzan funciones públicas, pondrán a disposición de las entidades públicas que así lo soliciten, la información que generen, obtengan, adquieran o controlen y administren, en cumplimiento y ejercicio de su objeto misional. El uso y reutilización de esta información deberá garantizar la observancia de los principios y normas de protección de datos personales, de conformidad con lo dispuesto en las Leyes 1581 de 2012 y 1712 de 2014, así como las demás normas que regulan la materia. El suministro de la información será gratuito, deberá solicitarse y realizarse respaldado en estándares que faciliten el proceso de intercambio y no en tecnologías específicas que impidan el acceso, no estará sujeto al pago de tributo, tarifa o precio alguno y las entidades públicas solo podrán cobrar los costos asociados a su reproducción o los derivados de la aplicación de procesamientos o filtros especiales. Las entidades públicas propenderán por la integración de los sistemas de información para el ejercicio eficiente y adecuado de la función pública".
31. Que la Ley 1765 de 2015 "Por la cual se reestructura la Justicia Penal Militar y Policial, se establecen requisitos para el desempeño de sus cargos, se implementa su Fiscalía General Penal Militar y Policial, se organiza su cuerpo técnico de investigación, se señalan disposiciones sobre competencia para el tránsito al sistema penal acusatorio y para garantizar su plena operatividad en la Jurisdicción Especializada y se dictan otras disposiciones", establece los parámetros de funcionamiento de la Justicia Penal Militar y Policial.
32. Que la Ley 1801 de 2016 "Por la cual se expide el Código Nacional de Seguridad y Convivencia Ciudadana", establece procedimientos y mecanismos para regular los comportamientos contrarios a la convivencia, en su artículo 184 estipula "REGISTRO NACIONAL DE MEDIDAS CORRECTIVAS. La Policía Nacional llevará un registro nacional de medidas correctivas que incluirá la identificación de la persona, el tipo de comportamiento contrario a la convivencia, el tipo de medida correctiva y el estado de pago de la multa o cumplimiento de la medida correctiva. La Registraduría Nacional del Estado Civil facilitará a las autoridades de Policía el acceso a sus bases de datos para la identificación e individualización de las personas vinculadas a procesos de Policía por comportamientos que afecten la convivencia. PARÁGRAFO. Solo las personas que sean registradas en dicha base de datos tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido en ella, en los términos contemplados en la ley".
33. Que la Ley 1861 de 2017 "Por la cual se reglamenta el servicio de reclutamiento, control de reservas y la movilización" el cual establece, en el parágrafo 1 del artículo 41 la obligación legal de la Policía Nacional de implementar la Cédula de Identidad Policial, así "PARÁGRAFO 1. Para los Oficiales, Suboficiales, Nivel Ejecutivo, Agente y Patrullero de la Policía Nacional en servicio

activo, situación de retiro o de reserva la cédula de identidad policial reemplaza la tarjeta de reservista. Para los alumnos de las escuelas de formación de las Fuerzas Militares y la Policía Nacional, durante su permanencia en la institución, el respectivo documento de identidad militar o policial reemplaza la Tarjeta de Reservista". Por lo que se hace necesario para la Policía Nacional que a partir de la infraestructura que soporta el sistema de identificación y de registro civil de la Registraduría, asegure la plena individualización e identificación de miembros de la Policía Nacional, logrando un sistema integral de identificación policial robusto que funcione en interoperabilidad con las bases de datos que produce y administra la Registraduría Nacional del Estado Civil, previo cumplimiento de las condiciones técnicas y legales que exija la Registraduría Nacional del Estado Civil, logrando la expedición de las identificaciones policiales seguras a sus miembros, obedeciendo a su misionalidad, intereses y fines perseguidos que atienden a las esferas de defensa y seguridad nacional.

34. Que la Ley 1955 de 2019 "Por el cual se expide el Plan Nacional de Desarrollo 2018-2022 Pacto por Colombia, Pacto por la Equidad", establece en el artículo 147 "... Las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para este propósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones. En todos los escenarios la transformación digital deberá incorporar los componentes asociados a tecnologías emergentes, definidos como aquellos de la Cuarta Revolución Industrial, entre otros. Las entidades territoriales podrán definir estrategias de ciudades y territorios inteligentes, para lo cual deberán incorporar los lineamientos técnicos en el componente de transformación digital que elabore el Ministerio de Tecnologías de la Información y las Comunicaciones. Los proyectos estratégicos de transformación digital se orientarán por los siguientes principios: 1. Uso y aprovechamiento de la infraestructura de datos públicos, con un enfoque de apertura por defecto. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales. 3. Plena interoperabilidad entre los sistemas de información públicos que garantice el suministro e intercambio de la información de manera ágil y eficiente a través de una plataforma de interoperabilidad. Se habilita de forma plena, permanente y en tiempo real cuando se requiera, el intercambio de información de forma electrónica en los estándares definidos por el Ministerio TIC, entre entidades públicas. Dando cumplimiento a la protección de datos personales y salvaguarda de la información. 4. Optimización de la gestión de recursos públicos en proyectos de Tecnologías de la Información a través del uso de los instrumentos de agregación de demanda y priorización de los servicios de nube. 5. Promoción de tecnologías basadas en software libre o código abierto, lo anterior, sin perjuicio de la inversión en tecnologías cerradas. En todos los casos la necesidad tecnológica deberá justificarse teniendo en cuenta análisis de costo-beneficio. 6. Priorización de tecnologías emergentes de la Cuarta Revolución Industrial que faciliten la prestación de servicios del Estado a través de nuevos modelos incluyendo, pero no limitado a, tecnologías de desintermediación, DLT (Distributed Ledger Technology), análisis masivo de datos (Big data), inteligencia artificial (AI), Internet de las Cosas (IoT), Robótica y similares. 7. Vinculación de todas las interacciones digitales entre el Estado y sus usuarios a través del Portal Único del Estado colombiano. 8. Implementación de todos los trámites nuevos en forma digital o electrónica sin ninguna excepción, en consecuencia, la interacción del Ciudadano-Estado sólo será presencial cuando sea la única opción. 9. Implementación de la política de racionalización de trámites para todos los trámites, eliminación de los que no se requieran, así como en el aprovechamiento de las tecnologías emergentes y exponenciales. 10. Inclusión de programas de uso de tecnología para participación ciudadana y gobierno abierto en los procesos misionales de las entidades públicas. 11. Inclusión y actualización permanente de políticas de seguridad y confianza digital". (...)

35. Que la Ley 2272 de 2022 "Por medio de la cual se modifica, adiciona y prorroga la Ley 418 de 1997, prorrogada, modificada y adicionada por las Leyes 548 de 1999, 782 de 2002, 1106 de 2006, 1421 de 2010, 1738 de 2014 y 1941 de 2018, se define la política de paz de estado, se crea el servicio social para la paz, y se dictan otras disposiciones", define la política de paz del estado colombiano.
36. Que el Decreto 2241 del 1986 "Por el cual se adopta el Código Electoral", define las directrices del Código Electoral y establece en su artículo 213 que "Toda persona tiene derecho a que la Registraduría le informe sobre el número, lugar y fecha de expedición de los documentos de identidad pertenecientes a terceros. Tienen carácter reservado las informaciones que reposen en los archivos de la Registraduría referentes a la identidad de las personas, como son sus datos biográficos, su filiación y fórmula dactiloscópica. De la información reservada sólo podrá hacerse uso por orden de autoridad competente; con fines investigativos, los jueces y funcionarios de policía y de seguridad tendrán acceso a los archivos de la Registraduría".
37. Que el Decreto 1010 del 2000 "Por el cual se establece la organización interna de la Registraduría Nacional del Estado Civil y se fijan las funciones de sus dependencias; se define la naturaleza jurídica del Fondo Social de Vivienda de la Registraduría Nacional del Estado Civil; y se dictan otras disposiciones", establece la organización de la Registraduría Nacional del Estado Civil.
38. Que el Decreto 235 de 2010 "Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas", dispone que: "Los requerimientos de información que se hagan por entidades estatales en cumplimiento de una función administrativa o en ejercicio de una facultad legal, o por los particulares encargados de una función administrativa, a otras entidades del Estado, no constituyen solicitud de un servicio y, por ende, no generan costo alguno para la entidad solicitante".
39. Que el artículo 2° del mismo Decreto dispone que para efectos del "...intercambio de información, las entidades deberán establecer mecanismos magnéticos, electrónicos o telemáticos para integrar, compartir y/o suministrar la información que por mandato legal se requiere, o permitir el acceso total dentro del marco de la Constitución y el derecho fundamental a la intimidad, a las bases de datos completas que requieran otras entidades para el ejercicio de sus funciones".
40. Que el Decreto 019 del 2012 "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública", establece en el artículo 17 "Suprímase el requisito de imponer la huella dactilar en todo documento, trámite, procedimiento o actuación que se deba surtir ante las entidades públicas y los particulares que cumplan funciones administrativas. Excepcionalmente se podrá exigir huella dactilar en los siguientes casos (...)11. Comercio de armas, municiones y explosivos (...)13. Registros delictivos, 14. Trámites para el registro de víctimas y ayuda humanitaria", y en su artículo 18 "En los trámites y actuaciones que se cumplan ante las entidades públicas y los particulares que ejerzan funciones administrativas en los que se exija la obtención de la huella dactilar como medio de identificación inmediato de la persona, ésta se hará por medios electrónicos. Las referidas entidades y particulares contarán con los medios tecnológicos de interoperabilidad necesarios para cotejar la identidad del titular de la huella con la base de datos de la Registraduría Nacional del Estado Civil".
41. Que conforme a los artículos 17 y 18 del mencionado Decreto, las entidades públicas y particulares en ejercicio de funciones públicas, pueden realizar el procedimiento de verificación de identidad personal a través de la huella por medios electrónicos y en interoperabilidad con las bases de datos de la Registraduría, permitiendo incorporar mecanismos de validación como forma de mitigación del fraude y suplantación de identidad.
42. Que el Decreto 857 del 2014 "Por el cual se reglamenta la Ley Estatutaria 1621 del 17 de abril de 2013, por medio de la cual se expiden normas para fortalecer el marco legal que permite a

los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones", donde señala las dependencias que fungen funciones de inteligencia y contrainteligencia de la Policía Nacional, y la coordinación en el intercambio de información con entidades públicas.

43. Que el Decreto 620 de 2020 "Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales", establece que la identificación por medios digitales se regirá por las disposiciones de la Registraduría.
44. Que la Ley 2052 de 2020, "Por medio de la cual se establecen disposiciones transversales a la rama ejecutiva del nivel nacional y territorial y a los particulares que cumplen funciones públicas y/o administrativas, en relación con la racionalización de trámites y se dictan otras disposiciones", establece que es un deber de las entidades que integran la Rama Ejecutiva del nivel nacional y territorial y particulares que cumplan funciones públicas y/o administrativas, la automatización y digitalización de los trámites conforme a los lineamientos establecidos por el Departamento Administrativo de la Función Pública y el Ministerio de Tecnologías de la Información y las Comunicaciones, además, proveer trámites en línea, e implementar los servicios ciudadanos digitales.
45. Que el Decreto 113 del 2022 "Por el cual se modifica la estructura del Ministerio de Defensa Nacional", establece las funciones de la Policía Nacional.
46. Que el Registrador Nacional, con el fin de dar cumplimiento a lo dispuesto en la ley, expidió la Resolución 5633 del 29 de junio de 2016, mediante la cual se reglamentan las condiciones y el procedimiento para el acceso a las bases de datos de la información que produce y administra la entidad; normativa aplicable al presente convenio, así como las demás normas que la modifiquen, adicionen o complementen. Que en el mencionado acto administrativo se establecieron varios procedimientos para la consulta de la información contenida en las bases de La Registraduría, entre los cuáles se encuentra la consulta del Archivo Nacional de Identificación – ANI -, la consulta del sistema de información de Registro Civil – SIRC -, la base de datos dispuesta para el proceso de autenticación biométrica dactilar.
47. Que la Policía Nacional de Colombia, dentro de su mapa de procesos establece las actividades y responsabilidades que deben liderar diferentes Direcciones, Oficinas Asesoras, Metropolitanas de Policía, Departamentos de Policía, Escuelas de Formación y demás unidades que la conforman, las cuales realizarán consultas a las bases que produce y administra la Registraduría Nacional del Estado Civil, para el cumplimiento de sus actividades administrativas, de control, asesoría, docente y operativas que permitan garantizar los principios filosóficos de convivencia ciudadana, las decisiones gerenciales y de soporte que la Policía Nacional requiere, obligándose a utilizar la información suministrada por la Registraduría, única y exclusivamente para el cumplimiento de sus obligaciones constitucionales y legales. Para ello, la Policía Nacional de Colombia, suscribirá el compromiso de confidencialidad y no divulgación que le será entregado por la Registraduría Nacional.
48. Que para la Policía Nacional de Colombia, el acceso a la información que administra la Registraduría, se constituye en una herramienta útil con la cual se soportarán actividades de las unidades de los niveles administrativos, de control, asesor, docente y operativas de la Institución Policial, a fin de tener calidad del dato y la identificación de los ciudadanos existente en los diferentes sistemas de información que administra la Registraduría, en procura de validar la información de forma veraz e integra que permita optimizar los procesos y procedimientos que

requieren la identificación, para trámites administrativos internos y comprobar la información suministrada por los ciudadanos.

49. Que el acceso, consulta, uso y aprovechamiento de la infraestructura en la cual se desarrolla el Sistema Nacional de Identificación de propiedad de la Registraduría, estará sujeta a lo señalado en el presente Convenio y los correspondientes ANEXOS TÉCNICOS que se elaborarán teniendo en cuenta las necesidades y funciones tanto constitucionales como legales de la Policía Nacional.
50. Que la Policía Nacional cuenta con las capacidades tecnológicas y logísticas para dar cabal cumplimento al sistema unificado de dactiloscopia utilizado por la Registraduría Nacional del Estado Civil, según lo ordenado por la Ley 38 de 1993.
51. Que la Policía Nacional de Colombia requiere implementar sistemas de reconocimiento biométrico y facial para garantizar la seguridad humana de los habitantes de Colombia, y que, en virtud del marco normativo, promueve el uso responsable y transparente de esta tecnología a través de una estructura de gobernanza que salvaguarda los derechos humanos y los datos personales. Los datos biométricos faciales de las bases de datos de la Policía Nacional serán cotejados, confrontados y comparados con los datos biométricos que reposan en el Sistema Nacional de Identificación de la Registraduría como criterio orientador y no como identificación plena de un colombiano, para lo cual la Policía Nacional de Colombia se obliga a cumplir con las condiciones, requisitos y especificaciones que se establecen en la Resolución 5633 de 2016 y demás que la modifiquen, adicionen o derogue.
52. Que mediante comunicación oficial GS-2023-002618-OFITE de fecha 04/04/2023, la Policía Nacional de Colombia solicitó la suscripción de un convenio interadministrativo de cooperación con la Registraduría Nacional del Estado Civil.
53. Que mediante comunicación oficial RDRCI de fecha 22/06/2023, la Registraduría Nacional del Estado Civil, expresó "...que conforme al principio de colaboración armónica entre las entidades públicas, y en aras de cooperar y coadyuvar en el cumplimiento de las obligaciones constitucionales, legales y de los fines estatales, es de interés de esta Entidad celebrar el convenio interadministrativo marco con la Policía Nacional".

Vistas las anteriores consideraciones, las partes acuerdan celebrar el presente convenio interadministrativo de Cooperación, y aceptan cumplir los compromisos contenidos en las siguientes,

CLÁUSULAS:

CLÁUSULA PRIMERA: OBJETO. Aunar esfuerzos, recursos tecnológicos, administrativos y humanos con el fin de apoyar las funciones constitucionales y legales de la Policía Nacional de Colombia, de su Policía Judicial, de sus procesos internos administrativos (Afiliaciones a sanidad, bienestar, procesos de incorporación, liquidaciones, pensionados, carnetización, juntas médico laborales, y demás actividades propias de la institución), las relacionadas con inteligencia y contrainteligencia, permitiendo el acceso y consulta de la información contenida en las bases de datos que produce y administra la Registraduría Nacional del Estado Civil.

CLÁUSULA SEGUNDA: ALCANCE DEL OBJETO. La información que la Policía Nacional de Colombia, accederá y consultará en las bases de datos de la Registraduría se enmarca dentro de sus funciones constitucionales y legales que permiten la verificación de la identidad de los clientes internos (policías y sus beneficiarios) y externos (ciudadanos colombianos) de la Policía Nacional de Colombia; por lo tanto, la Policía Nacional de Colombia se compromete a preservar el buen nombre, la dignidad y el respeto a la intimidad de las personas, de conformidad con lo dispuesto por la Constitución Política y las Leyes.

El acceso, consulta, uso y aprovechamiento de la infraestructura en la cual se desarrolla el Sistema Nacional de Identificación de propiedad de la Registraduría, estará sujeta a lo señalado en el presente Convenio y en los correspondientes ANEXOS TÉCNICOS que se elaborará teniendo en cuenta las necesidades y funciones tanto constitucionales como legales de la Policía Nacional, representada por cada una de sus unidades, los cuales estarán sujetos a la previa revisión y aprobación por parte del Grupo de Acceso a la Información y Protección de Datos Personales de la Registraduría Nacional del Estado Civil o quien haga sus veces.

PARÁGRAFO PRIMERO. La información a la que accederá la Policía Nacional de Colombia deberá ser justificada por cada una de las dependencias o entidades adscritas a la Policía Nacional, conforme a sus funciones legales y constitucionales

PARÁGRAFO SEGUNDO. La consulta y acceso a las bases de datos, se hará de conformidad a lo establecido en la Resolución 5633 de 2016 o en el acto administrativo que la modifiquen, adicionen, complementen o deroguen que expida la Registraduría Nacional para la interoperabilidad, y/o a través de los medios tecnológicos dispuestos por la Registraduría para interoperar con la Policía Nacional de Colombia.

CLÁUSULA TERCERA: OBLIGACIONES COMUNES A LAS PARTES. 1) Cumplir íntegramente con el objeto del convenio, así como con las obligaciones inherentes a la naturaleza del mismo. 2) Proporcionar las máximas condiciones de seguridad para consultar la información, verificando los procesos, procedimientos informáticos y las buenas prácticas del manejo de la información, con el fin de evitar los riesgos por pérdida, destrucción, alteración, uso no autorizado y/o fraudulento de la información consultada en el marco del presente convenio. 3) Expedir y suscribir los anexos técnicos para la expedición de documentos de identificación, el acceso, consulta, validación y verificación de los datos contenidos en las bases de datos que produce y administra la Registraduría Nacional para las diferentes unidades policiales que lo requieran. 4) cumplir con las obligaciones, especificaciones, requerimientos y condiciones descritas en cada uno de los anexos técnicos 5) Designar por escrito un supervisor del convenio. 6). Para la expedición de los documentos de identificación policial, se tendrán en cuenta la necesidad de identificación del personal en servicio activo, integrantes de la reserva policial, pensionados y sus beneficiarios, y funcionarios de inteligencia y contrainteligencia en ejercicio de sus funciones de la Policía Nacional de Colombia, así como las condiciones y especificaciones que se exijan y requieran por parte de la Registraduría Nacional del Estado Civil las cuales se materializarán en los respectivos ANEXOS TÉCNICOS. 7) Atender con diligencia los requerimientos realizados por las partes.

CLÁUSULA CUARTA: OBLIGACIONES DE LA POLICÍA NACIONAL. 1). Implementar y disponer de los mecanismos necesarios para adecuarse a los adelantos tecnológicos que en materia de acceso a la información o seguridad informática realice la Registraduría. 2) Facilitar, Implementar y disponer de los medios que permitan la interoperabilidad segura de los sistemas de la Policía Nacional y la Registraduría. 3) Contar con los equipos necesarios, las respectivas licencias del motor de bases de datos, sistemas operativos y antivirus actualizados, en lo posible con la última versión estable, para el acceso y consulta a la información dispuesta por la Registraduría. 4) No utilizar la información obtenida para uso distinto del señalado en el presente convenio y en el anexo técnico correspondiente. 5) Suministrar el canal de comunicaciones dedicado y cumplir los requerimientos de seguridad de la Registraduría para el acceso de los sistemas informáticos. 6) Presentar a la Registraduría Delegada para el Registro Civil y la Identificación y la Gerencia de Informática de la Registraduría Nacional del Estado Civil, el protocolo de seguridad establecido para garantizar la confidencialidad de la información suministrada. La Policía Nacional permitirá a la Registraduría realizar la verificación, control y seguimiento del uso a los sistemas de información, cuando lo considere necesario, para la corroboración del funcionamiento del protocolo

de seguridad, políticas de seguridad de la información y los compromisos adquiridos en el presente convenio y anexos técnicos. En los casos que se detecte un posible evento o incidente de seguridad, la Registraduría informará a la Policía Nacional a través del supervisor por un mecanismo expedito, para que sin dilación disponga de lo necesario para permitir el ingreso a los puntos que se requieran. 7) Suscribir los compromisos de confidencialidad que disponga la Registraduría en los casos que haya a lugar. 8) Designar por escrito los funcionarios de cada Unidad de la Policía Nacional, desde su misionalidad para tramitar los requerimientos de acceso a la información contenida en las bases de datos de la Registraduría. 9) Garantizar la infraestructura necesaria que determine la Registraduría para la consulta de los aplicativos, tales como conectividad, seguridad de la información, bases de datos, licenciamiento, entre otros. 10) Garantizar que la información a la que se haya accedido o consultado de la base de datos de la Registraduría Nacional del Estado Civil sea única y exclusivamente para los fines definidos en el objeto del presente convenio y los anexos técnicos. Se prohíbe cualquier otro tipo de tratamiento sobre la información suministrada, así como la entrega de dicha información a terceros no autorizados, o hacer tratamiento de datos a entidades nacionales ni extranjeras. 11) Informar a la Registraduría de las situaciones que pongan en riesgo los sistemas de información, tratamiento y uso indebido de los datos una vez se tenga conocimiento de las mismas. 12) Las demás inherentes al cumplimiento del presente convenio.

CLÁUSULA QUINTA: OBLIGACIONES DE LA REGISTRADURÍA. 1) Permitir a la Policía Nacional de Colombia el acceso y consulta a los datos de acuerdo con la justificación jurídica y el anexo técnico, a través de los mecanismos tecnológicos dispuestos por la Registraduría, conforme a su disponibilidad tecnológica. 2) Facilitar a través de los supervisores, dentro de los recursos de la plataforma tecnológica disponible, los medios necesarios para la ejecución del presente convenio. 3) Facilitar los parámetros para el intercambio de información. 4.) Las demás inherentes al cumplimiento del presente convenio.

CLÁUSULA SEXTA: ANEXOS TÉCNICOS. Teniendo en cuenta las diferentes funciones constitucionales y legales atribuidas a la Policía Nacional, así como las normas en materia de protección de datos personales, habeas data, reserva legal y las herramientas tecnológicas disponibles por la Registraduría, las partes acuerdan elaborar a través de los supervisores, los anexos técnicos para el acceso y consulta a las bases de datos, los cuales tendrán como mínimo lo siguiente: justificación para el acceso conforme a la función que desempeña la Unidad de la Policía Nacional, las basés de datos que accederá, el modelo de operación, el procedimiento y modos de accesos (los cuales estarán conforme a la Resolución 5633 de 2016 o la que modifique, derogue o sustituya), los datos que se consultarán, las políticas de seguridad relacionadas con el tratamiento de datos personales y dado el caso el señalamiento de las herramientas tecnológicas para el acceso y consulta. Los anexos técnicos podrán modificarse de acuerdo con los requerimientos de las partes a través de los supervisores.

Asimismo, los anexos técnicos contendrán las obligaciones, requisitos, condiciones y especificaciones necesarias para el acceso a la base de datos. Igualmente, en los casos que haya a lugar, se indicará el personal que conformará el Comité Técnico.

Para la expedición de los documentos de identificación policial, se tendrán en cuenta los parámetros y necesidades de la Policía Nacional, los cuales se materializarán en el respectivo anexo técnico.

PARÁGRAFO PRIMERO. La Registraduría Nacional del Estado Civil permitirá el acceso a sus instalaciones a los funcionarios designados por la Policía Nacional para el ejercicio de las actuaciones de Policía Judicial, con el fin de garantizar el servicio de consulta y búsquedas técnicas.

Respecto a las consultas técnicas por medio de las impresiones dactilares y faciales, mediante la base de datos Motor Multibiométrico que produce y administra la Registraduría Nacional del Estado Civil, solo se permitirán en ejercicio de las funciones de Policía Judicial de la Policía Nacional, para lo cual se suscribirá el anexo técnico correspondiente.

De igual manera, se permitirá la creación de usuarios por el sistema o aplicativo para la consulta e impresión, previa indicación de los nombres y cédulas de las personas a las que les serán asignados, quienes deberán ceñirse a las políticas de seguridad informática institucional.

PARÁGRAFO SEGUNDO. Para los procesos de autenticación biométrica que trata la Resolución 5633 de 2016 y sus anexos técnicos, la Policía Nacional deberá informar los aliados tecnológicos, los cuales deberán cumplir con los requisitos establecidos en dicha resolución o aquellas que la modifique, sustituya o derogue.

CLÁUSULA SÉPTIMA: CONTROL DE LA EJECUCIÓN. La ejecución del convenio y el cumplimiento de las obligaciones dispuestas en su clausulado, como en los anexos técnicos a suscribir, serán verificadas conjuntamente así: por la Registraduría, a través de la Registraduría Delegada para el Registro Civil y la Identificación o a quien se designe por escrito; por la Policía Nacional de Colombia la supervisión será ejercida por el Jefe de la Oficina Tecnologías de la Información y las Comunicaciones o a quien éste designe por escrito.

CLÁUSULA OCTAVA: PLAZO DE EJECUCIÓN. El plazo de ejecución del convenio será a partir de la suscripción de este hasta el 31 diciembre de 2026. Sin perjuicio de lo anterior, las partes podrán prorrogar por periodos de cuatro años el presente convenio.

CLÁUSULA NOVENA: PÓLIZA. La Policía Nacional constituirá una póliza de seguro de ciberseguridad o la que haga sus veces con una compañía de seguros legalmente constituida en Colombia, a favor de la Registraduría y que proteja riesgos, y será remitida a la Oficina Jurídica para su aprobación. Para la adquisición de la póliza, el supervisor del convenio por parte de la Policía Nacional, realizará las coordinaciones necesarias.

CLÁUSULA DÉCIMA: SUSPENSIÓN TEMPORAL. Las partes podrán suspender el presente convenio, como una medida excepcional y temporal, por eventos de fuerza mayor, de caso fortuito o en procura del interés público, que de forma suficiente y justificada tiene fundamento, haciendo constar dichas circunstancias y sus efectos por escrito con la finalidad de salvaguardar la continuidad de la relación contractual.

PARÁGRAFO: En época pre-electoral (tres meses antes de elecciones) los días de elecciones y durante los quince (15) días siguientes a las fechas en que se realizan los eventos electorales la Registraduría por medio de la Registraduría Delegada para el Registro Civil y la Identificación y/o la Gerencia de Informática, podrá suspender la ejecución del convenio cuando las necesidades del procesamiento de datos de la entidad lo exijan, sin que para ello sea necesaria la notificación verbal, telefónica o escrita, de conformidad con el artículo 6° de la Resolución 5633 del 29 junio de 2016 y las demás que la modifiquen, adicionen o complementen.

CLÁUSULA DÉCIMA PRIMERA: CONFIDENCIALIDAD DE LA INFORMACIÓN. En atención a lo definido por la Constitución Política de Colombia, la Ley 1581 de 2012, la jurisprudencia y demás normas complementarias, la Policía Nacional de Colombia, a través de su personal y/o contratistas, no podrán realizar tratamiento alguno de la información, diferente a lo establecido en el objeto del presente

convenio, debiendo garantizar el cumplimiento del compromiso de confidencialidad que disponga la Registraduría. Para ello, la Policía Nacional de Colombia se obliga a suscribir el compromiso de confidencialidad y no divulgación, suministrado por la Registraduría Nacional del Estado Civil.

La obligación de confidencialidad será continua y no desaparecerá por suspensión o terminación del Convenio, garantizando que la información suministrada será utilizada exclusivamente para el cumplimiento de las funciones constitucionales y legales indicadas en el presente Convenio y anexo técnico. Las partes, ni su personal, podrán revelar ninguna información confidencial o de propiedad de éstas relacionada con el Convenio, sin previo consentimiento por escrito de cada una de las partes.

PARÁGRAFO PRIMERO. La Policía Nacional de Colombia se obliga a garantizar lo establecido por la Corte Constitucional en Sentencia C-748 de 2011 frente a que "...la entidad administrativa receptora cumpla con las obligaciones de protección y garantía que se derivan del citado derecho fundamental, en especial la vigencia de los principios de finalidad, utilidad y circulación restringida". En virtud de lo anterior, utilizará la información suministrada por la Registraduría exclusivamente para el cumplimiento de sus obligaciones constitucionales y legales. Para ello, la Policía Nacional de Colombia suscribirá el compromiso de confidencialidad y no divulgación, necesario para la ejecución del presente convenio.

PARÁGRAFO SEGUNDO. La Policía Nacional de Colombia no entregará la información a terceros en ninguna circunstancia. Igualmente, debe evitar los riesgos de pérdida, destrucción, alteración y uso no autorizado o fraudulento de la información, para lo cual se compromete a cumplir las disposiciones legales, constitucionales y jurisprudenciales que regulen la materia o resulten aplicables a la protección de datos personales y derechos fundamentales conexos, y a lo estipulado dentro del compromiso de confidencialidad y no divulgación. El uso indebido de la información por parte de la entidad receptora, por quienes la administren, soliciten, validen, manejen, procesen o usen, dará lugar a la terminación unilateral del presente convenio por parte de la Registraduría, sin perjuicio de las acciones legales a que haya lugar.

PARÁGRAFO TERCERO. La Policía Nacional de Colombia se obliga para con la Registraduría a guardar plena confidencialidad de la información, haciendo parte integral del presente Convenio, el compromiso de confidencialidad que deberán suscribir quienes tengan a cargo la gestión y uso directo de la información suministrada. La confidencialidad será continua y no vencerá por suspensión o terminación del presente Convenio.

CLÁUSULA DÉCIMA SEGUNDA: VALOR. Las partes declaran que la firma del convenio no implica erogación presupuestal alguna, por tanto, no genera contraprestaciones económicas entre ellas. No obstante, tanto la Registraduría como la Policía Nacional deberán gestionar y aportar los recursos que se requieran para atender las obligaciones que les atañen en virtud del presente convenio.

CLÁUSULA DÉCIMA TERCERA: CESIÓN. Las partes se comprometen a no ceder total, ni parcialmente el presente convenio, ni los derechos y compromisos que se derivan del mismo, bajo ninguna consideración.

CLÁUSULA DÉCIMA CUARTA: INEXISTENCIA DE RELACIÓN LABORAL. Las partes manifiestan expresamente que ninguno de los empleados, agentes o dependientes adquiere, por la celebración del presente convenio, relación laboral alguna con la otra parte, extendiéndose esta salvedad a las personas que en desarrollo del mismo convenio llegue a contratarse por cualquier causa la Policía Nacional de Colombia y/o la Registraduría.

CLÁUSULA DÉCIMA QUINTA: SOLUCIÓN DE CONTROVERSIAS. En caso de diferencias, discrepancias o conflictos generados con ocasión de la celebración, interpretación, ejecución, modificación o terminación del presente convenio; la Policía Nacional y la Registraduría, las solucionarán en forma directa dentro los treinta (30) días siguientes, contados a partir del surgimiento del conflicto, en caso de no darse fórmula de arreglo, para todos los efectos se entenderá dar por terminado de común acuerdo el presente convenio y se elaborará el acta de terminación.

CLÁUSULA DÉCIMA SEXTA: INDEMNIDAD. Las partes se mantendrán indemnes entre sí, por cualquier daño o perjuicio originado en reclamaciones de terceros y que se deriven o tengan como causa las actuaciones, omisiones, ocasionadas por su parte o cualquiera de sus subcontratistas o dependientes durante la ejecución del presente convenio. Por lo tanto, cada una de las partes asumirá la responsabilidad por el manejo de la información suministrada en desarrollo de este convenio y responderá civil y penalmente tanto por el incumplimiento de las obligaciones derivadas del mismo como por los hechos u omisiones que le fueran imputables.

CLÁUSULA DÉCIMA SÉPTIMA: TERMINACIÓN. El convenio terminará por las siguientes causales: 1) Por mutuo acuerdo entre las partes. 2) Vencimiento del plazo pactado. 3) Por la decisión de alguna de las partes. La parte que esté interesada en la terminación del convenio debe comunicar su decisión por escrito a la otra, por lo menos con treinta (30) días de antelación. 4) Por el incumplimiento de las obligaciones pactadas en el convenio interadministrativo, en los compromisos de confidencialidad o en los anexos técnicos. 5) Por fuerza mayor o caso fortuito. 6) Por uso indebido de la información conforme al objeto del convenio.

PARÁGRAFO. Cuando se configure alguna de las causas de terminación del presente convenio, hasta tanto se materialice la misma, la Registraduría deberá garantizar la prestación del servicio para el cumplimiento de la misionalidad de la Dirección de Investigación Criminal e INTERPOL.

CLÁUSULA DÉCIMA OCTAVA: INHABILIDADES, INCOMPATIBILIDADES Y PROHIBICIONES. Las partes declaran bajo juramento que no han suministrado información falsa y que no se hallan incursos en causal alguna de inhabilidad o incompatibilidad establecida en la Constitución Política de Colombia y la Ley. Así mismo, las partes declaran que no les asiste inhabilidad o incompatibilidad alguna de las señaladas en la Ley 1474 de 2011 y demás disposiciones vigentes sobre la materia, que les impida la celebración del presente convenio. De igual manera, declaran que en caso de sobrevenir alguna inhabilidad o incompatibilidad se obligan a responder ante la otra parte y frente a terceros por los perjuicios que se ocasionen.

CLÁUSULA DÉCIMA NOVENA: RÉGIMEN LEGAL APLICABLE. Este convenio se regula por las disposiciones contenidas en la Constitución Política de Colombia, en la Ley 489 de 1998 y sus decretos reglamentarios, y por las disposiciones que conforme a su esencia y naturaleza le sean aplicables.

CLÁUSULA VIGÉSIMA: PERFECCIONAMIENTO Y EJECUCIÓN. El presente convenio requiere para su perfeccionamiento la firma de las partes de acuerdo con la normativa vigente. Con arreglo a las disposiciones legales, la Policía Nacional efectuará la publicación del convenio.

CLÁUSULA VIGÉSIMA PRIMERA: DOCUMENTOS. Forman parte del presente Convenio: los Estudios previos, los actos administrativos de nombramiento, posesión y delegación y los demás documentos que provengan del desarrollo de este.

DÉCIMA VIGÉSIMA SEGUNDA: CONVENIOS PRECEDENTES. Las partes expresan que una vez se suscriba el presente convenio y cada uno de sus respectivos anexos técnicos con la unidad policial que corresponda, se entenderá terminado cualquier otro negocio jurídico que, en relación con el objeto del presente convenio y sus anexos, exista entre la Policía Nacional y la Registraduría Nacional del Estado Civil.

CLÁUSULA VIGÉSIMA TERCERA: DOMICILIO. Las partes declaran que, para todos los efectos judiciales y extrajudiciales aceptan la ciudad de Bogotá D.C., como domicilio principal y las mismas se podrán notificar en: La Registraduría: Avenida calle 26 Nro. 51-50 CAN Piso 5°, Secretaría General de la Registraduría Nacional del Estado Civil en Bogotá D.C., Dirección General de la Policía Nacional: Carrera 59 Nro. 26-21 CAN, teléfono 5159000, Bogotá, D.C.

Para constancia se firman dos (2) ejemplares idénticos, en Bogotá, D.C., a los 20 NOV. 2023

Por la Policía Nacional de Colombia

General **WILLIAM RENÉ SALAMANCA RAMÍREZ**
Director General Policía Nacional de Colombia

Por la Registraduría Nacional del Estado Civil

Doctor **ALEXANDER VEGA ROCHA**
Registrador Nacional del Estado Civil

Revisado y aprobado Policía Nacional de Colombia

Elaborado por: CT. Ronald Alexander Franco Aguilera – OFTIC/ASJUR
Revisado por: TC. Jaime Hernán Rojas Parra – OFTIC/JEFAT
CR. Diana Constanza Torres Castellanos - OFPLA/JEFA
BG. Hernán Alonso Meneses Gelves – SEGEN/JEFAT
BG. Nicolás Alejandro Zapata Restrepo - SUDIR

Fecha de elaboración: 08/11/2023
Ubicación: Y:\ASESORIA JURÍDICA\CONVENIOS\CONVENIO REGISTRADURÍA NACIONAL DE ESTADO CIVIL

Revisado y aprobado Registraduría Nacional del Estado Civil

Ing. Didier Alberto Chilito Velasco –Registrador Delegado para el Registro Civil y la Identificación
Ing. Javier Antonio Sánchez Roldán – Coordinador Grupo de Acceso a la Información y Protección de Datos Personales
Dr. José Antonio Parra Fandiño – Jefe Oficina Jurídica

COMPROMISO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN CONVENIO INTERADMINISTRATIVO ENTRE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL Y LA POLICÍA NACIONAL DE COLOMBIA.

El suscrito General **WILLIAM RENÉ SALAMANCA RAMÍREZ,** identificado con cédula de ciudadanía Nro. 6.770.835 de Tunja - Boyacá, actuando en calidad de Director General de **LA POLICÍA NACIONAL DE COLOMBIA**, Entidad identificada con NIT 800.141.397-5, nombrado mediante Decreto Nro. 694 del 09 de mayo de 2023 y Acta de posesión Nro. 096-23 del 10 de mayo de 2023, suscribe el presente **COMPROMISO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN** relacionado con la reserva legal que tiene la consulta a la base de datos dispuesta por la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL** para el proceso de autenticación biométrica, que se regirá por las cláusulas que se determinan a continuación:

CONSIDERACIONES

1. Que en relación con la información de las personas y en general en cuanto a los temas de la identificación ciudadana, la normatividad vigente es restrictiva, dada la naturaleza de la información, según lo establecido en la Ley Estatutaria 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales, reglamentada parcialmente por el Decreto Nacional 1377 de 2013, recopilada en el capítulo 25 del Decreto Único Reglamentario 1074 de 2015.

2. Que el artículo 227 de la Ley 1450 del 2011, modificada por el "nuevo Plan de desarrollo 2014-2018" en su artículo 159 de la Ley 1753 de 2015, el suministro de información que reposa en la base de datos, señalando que: "Para el desarrollo de los planes, programas y proyectos incluidos en Plan Nacional de Desarrollo y en general para el ejercicio de las funciones públicas, las entidades públicas y los particulares que ejerzan funciones públicas, pondrán a disposición de las entidades públicas que así lo soliciten, la información que generen, obtengan, adquieran o controlen y administren, en cumplimiento y ejercicio de su objeto misional. El uso y reutilización de esta información deberá garantizar la observancia de los principios y normas de protección de datos personales, de conformidad con lo dispuesto en las Leyes 1581 de 2012 y 1712 de 2014, así como las demás las normas que regulan la materia. (...)".

3. Que el Gobierno Nacional, a través del Decreto Ley 019 de 2012 estableció normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la administración pública, estableciendo en los artículos 17° y 18°, que la obtención de la huella dactilar como medio de identificación inmediato de la persona se realice por medios electrónicos, con los métodos tecnológicos e interoperabilidad necesarios para cotejar la identidad del titular de la huella con la base de datos que genera y administra la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.**

4. Que el artículo 10 de la Ley Estatutaria 1581 de 2012 al señalar los casos en los cuales no se requiere autorización del titular, establece en su literal (a): "Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial", lo cual otorga viabilidad para la entrega de información personal que produce y administra la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.**

5. Que el Registrador Nacional, con el fin de dar cumplimiento a lo dispuesto en la ley, expidió la Resolución 5633 del 29 de junio de 2016, "Por la cual se reglamentan las condiciones y el procedimiento para el acceso a los datos y a las bases de datos de la información que produce y administra la Registraduría Nacional Del estado Civil", o la que modifique, derogue, sustituya o adicione.

6. Que mediante la Resolución 4173 del 20 de mayo de 2016 la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL** estableció las políticas informáticas.

7. Que, la **POLICÍA NACIONAL DE COLOMBIA** requiere el acceso a los datos y bases de datos que produce y administra la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL - RNEC**, en aras de poder corroborar la información de los colombianos existentes en los diferentes sistemas de información que administra la entidad, en procura de optimizar los procesos y procedimientos de validación de la identificación, trámites administrativos internos y confirmación de la información suministrada por los titulares con el fin único de cumplir sus obligaciones constitucionales y legales. Además, en el ejercicio de policía judicial requiere contar con fuentes de información que le permitan apoyar las actividades investigativas relacionadas con las distintas modalidades delictivas que afectan la seguridad y convivencia ciudadana, coadyuvando con ello a la identificación de personas en cumplimiento de los procesos misionales en materia de investigación criminal, dando cumplimiento a las funciones permanentes de Policía Judicial, otorgadas por el Artículo 250 numeral 8 de la Constitución Política de Colombia y reguladas por el Artículo 201 de la Ley 906 de 2004. Adicionalmente, realizar cotejos biométricos de los ciudadanos en diligencias de control y vigilancia, que permitan la Identificación de los colombianos en aras de preservar la seguridad ciudadana.

8. Que la **POLICÍA NACIONAL DE COLOMBIA** celebra el convenio interadministrativo con la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL** con el objeto de Aunar esfuerzos, recursos tecnológicos, administrativos y humanos con el fin de apoyar las funciones constitucionales y legales de la Policía Nacional de Colombia, de sus funciones como Policía Judicial, procesos internos administrativos, las relacionadas con inteligencia y contrainteligencia, permitiendo el acceso y consulta de la información contenida en las bases de datos que produce y administra la Registraduría.

9. Que teniendo en cuenta la reserva legal que mantiene la información incorporada en las bases de datos que produce y administra la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL**, objeto del Convenio Interadministrativo suscrito con la **POLICÍA**, y en cumplimiento de las condiciones y procedimientos establecidos por el Registrador Nacional en las Resoluciones 4137 de 2016 y 5633 de 2016, se suscribe compromiso de confidencialidad y no divulgación de la información, de conformidad con lo establecido en el numeral 7 de la **CLÁUSULA CUARTA: OBLIGACIONES DE LA POLICÍA NACIONAL.** "Suscribir los compromisos de confidencialidad que disponga la Registraduría en los casos que haya a lugar".

El presente compromiso se regirá por las siguientes cláusulas:

CLÁUSULA PRIMERA - DEFINICIONES: INFORMACIÓN CONFIDENCIAL: Información Confidencial significa cualquier información relacionada con los datos personales de la población colombiana suministrada por la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL,** bien sea que dicha información sea escrita, oral, visual o electrónica. Complementariamente, y para los efectos del presente compromiso, la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL** manifiesta expresamente desde ya, que las bases de datos y la información suministrada para el desarrollo del objeto del convenio suscrito, tiene el carácter de información confidencial.

PARTE REVELADORA: Se constituye en **PARTE REVELADORA**, la que suministra a la otra parte, información confidencial o no confidencial, que en este caso corresponde a la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.**

PARTE RECEPTORA: Se constituye en **PARTE RECEPTORA**, quienes reciben de la **PARTE REVELADORA** información confidencial o no confidencial, que en marco del convenio suscrito es la **POLICÍA NACIONAL DE COLOMBIA.**

CLÁUSULA SEGUNDA – OBJETO: El presente compromiso de confidencialidad y no divulgación de la información relacionada con "(...) Aunar esfuerzos, recursos tecnológicos, administrativos y humanos con el fin de apoyar las funciones constitucionales y legales de la Policía Nacional de Colombia, de su Policía Judicial, de sus procesos internos administrativos (Afiliaciones a sanidad, bienestar, procesos de incorporación, liquidaciones, pensionados, carnetización, juntas médico laborales, y demás actividades propias de la institución), las relacionadas con inteligencia y contrainteligencia, permitiendo el acceso y consulta de la información contenida en las bases de datos que produce y administra la Registraduría Nacional del Estado Civil", tiene por objeto el señalamiento y especificación de las políticas de confidencialidad que debe cumplir **LA PARTE RECEPTORA**.

CLÁUSULA TERCERA – DURACIÓN: Este compromiso tendrá una duración PERPETUA, a partir de su suscripción, por la connotación que tiene la información confidencial de Seguridad y defensa nacional que administra y produce la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL**, así como, la información biométrica de los colombianos son considerados de naturaleza sensible conforme a lo estipulado en el artículo 5 de la Ley Estatutaria 1581 de 2012, a partir de su suscripción, sin perjuicio de la protección de la información que haya sido revelada con anterioridad a la firma del presente compromiso.

CLÁUSULA CUARTA – OBLIGACIONES: 1.) Preservar el buen nombre, la dignidad y el respeto a la intimidad de las personas, de conformidad con lo dispuesto por la Constitución Política y las normas legales vigentes. 2.) La Información Confidencial no puede ser utilizada por la **PARTE RECEPTORA** para fines diferentes a los establecidos en el contexto de este Compromiso de Confidencialidad. 3.) **LA PARTE RECEPTORA** se obliga a no revelar, divulgar, exhibir, mostrar, hacer circular, compilar, sustraer, ofrecer, vender, intercambiar, captar, interceptar, modificar, recolectar, almacenar, replicar, complementar o crear bases de datos con la información dada a conocer por **LA PARTE REVELADORA**. 4.) Igualmente, hacer cumplir en nombre propio sobre sus contratistas, subcontratistas y respectivos empleados el no almacenar, guardar, copiar, complementar o crear bases de datos con la información que hayan accedido o consultado de la base de datos de **LA PARTE REVELADORA.** 5.) Instruir al personal que estará encargado de recibir la información confidencial, debiendo suscribir el correspondiente compromiso de confidencialidad, si fuere necesario, de su obligación de recibir, tratar y usar la información confidencial destinada únicamente al propósito del cumplimiento del objeto del convenio suscrito, en los mismos términos en que se establece en el presente compromiso. 6.) Igualmente, **LA PARTE RECEPTORA** como las personas a su cargo, se comprometen a no utilizar la **INFORMACIÓN,** de ninguna forma que pudiere causar perjuicio directo o indirecto a los titulares de la información suministrada o a la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.** 7.) Cumplir con las disposiciones sobre protección de datos personales, de acuerdo con lo dispuesto en la Ley Estatutaria 1581 de 2012, en sus decretos reglamentarios, así como aquellas que lo modifiquen, adicionen o deroguen. 8.) la **PARTE RECEPTORA** deberá informar a **LA PARTE REVELADORA** cuando ocurra un evento o incidente de seguridad con la información confidencial.

PARÁGRAFO PRIMERO: LA PARTE RECEPTORA deberá responder frente a la **PARTE REVELADORA** por la indebida utilización de la **INFORMACIÓN** recibida. De igual forma, se compromete a guardar absoluta confidencialidad sobre todos los datos a que tenga acceso en virtud del desarrollo del convenio.

PARÁGRAFO SEGUNDO: LA PARTE RECEPTORA deberá Permitir, en todo momento, al personal

designado por **PARTE REVELADORA**, la realización de visitas, revisión y evaluación de cumplimiento de las políticas de seguridad y disposiciones sobre la protección de datos personales, sobre los sistemas, puntos de atención de **LA PARTE RECEPTORA**, data center, equipo y en general todo aquel componente tecnológico, de propiedad de la Entidad y de sus Aliados Tecnológicos, que tenga relación con el acceso y uso de la información de **PARTE REVELADORA**.

PARÁGRAFO TERCERO: Informar a **LA PARTE REVELADORA** sobre las situaciones que pongan en riesgo los sistemas de interoperabilidad para el tratamiento de la información y del uso indebido de los datos consultados frente al titular de los mismos.

CLÁUSULA QUINTA – PROPIEDAD INTELECTUAL: Los archivos, software y las bases de datos de **LA PARTE REVELADORA,** que contienen la información de los colombianos, son de conformidad con lo establecido en la normatividad vigente, exclusivamente de su propiedad, por lo que **LA PARTE RECEPTORA** reconoce por medio de este Compromiso, que no goza de ningún derecho o licencia en relación con éstos y que la información allí contenida, se revela únicamente con el propósito de facilitar el cumplimiento del objeto del convenio.

CLÁUSULA SEXTA – DESTINACIÓN: La información sólo podrá ser utilizada para desarrollar los fines señalados en el Convenio Interadministrativo suscrito entre las partes.

CLÁUSULA SÉPTIMA – CUSTODIA: LA PARTE RECEPTORA garantiza la aplicación de las medidas de seguridad exigidas por **LA PARTE REVELADORA** y se obliga a garantizar la protección y debido tratamiento de las mismas, para evitar divulgación, fuga, reproducción, almacenamiento o cualquier otro uso no autorizado de información confidencial.

CLÁUSULA OCTAVA – VERIFICACIÓN DE LA CONFIDENCIALIDAD Y USO DE LA INFORMACIÓN: LA PARTE REVELADORA se reserva el derecho de verificar en cualquier momento y sin previo aviso, el cumplimiento del presente compromiso, con respecto al tratamiento de la información consultada por la **PARTE RECEPTORA.**

CLÁUSULA NOVENA – SANCIONES: La violación de la confidencialidad o el uso indebido de la información, será causal unilateral de terminación del convenio suscrito, sin perjuicio a las sanciones de ley a que haya lugar.

CLÁUSULA DÉCIMA- VALIDEZ Y PERFECCIONAMIENTO: El presente compromiso de confidencialidad y no divulgación de la información se perfecciona con la firma de la **PARTE RECEPTORA.**

Para constancia, se firma doble ejemplar del presente compromiso en la ciudad de Bogotá D.C., a los 20 NOV 202

General **WILLIAM RENE SALAMANCA RAMÍREZ**
Director General Policía Nacional de Colombia

REGISTRADURÍA
NACIONAL DEL ESTADO CIVIL

ANEXO TÉCNICO No. 2

Versión 1.0

INFRAESTRUCTURA TECNOLÓGICA PARA EL PROCESO DE AUTENTICACIÓN BIOMÉTRICA DACTILAR

AMBIENTE DE PRODUCCIÓN

RESOLUCIÓN No. 27145 de 2023

NOVIEMBRE 22 de 2023

REQUERIMIENTOS Y CONDICIONES PARA EL DISEÑO Y ESPECIFICACIÓN DEL SERVICIO DE AUTENTICACIÓN BIOMÉTRICA EN AMBIENTE DE PRODUCCIÓN

Contenido

1. MODALIDAD DE ACCESO 4
1.1 Modalidad Housing o Colocation 4
1.2 Modalidad Colocation Compartido 4
1.3 Modalidad Infraestructura Propia 5
2. HARDWARE 7
2.1. Servidores 7
2.1.1. Base de datos 7
2.1.2. Aplicaciones 8
2.1.3. Oracle Audit Vault 8
2.1.4. Oracle Firewall 9
2.2. Disponibilidad 9
2.3. Responsabilidades de Administración 9
2.4. Sistema de Backup 11
2.4.1. Modalidad Housing o Colocation 11
2.4.2. Modalidad Colocation Compartido 12
2.4.3. Modalidad Infraestructura Propia 12
2.5. Nivel de Soporte 12
3. BALANCEADORES DE CARGA 12
3.1. Servicio de balanceo de carga de servidores de acceso 13
3.2. Ancho de Banda 13
3.3. Nivel de Servicio 13
4. FIREWALL ACCESO 13
4.1. Servicio de firewall perimetral (Alta disponibilidad) 13
4.2. Ancho de banda 14
5. LICENCIAMIENTO REQUERIDO 14
5.1. Productos imprescindibles de seguridad para protección de la base de datos 16
5.1.1. Audit Vault (Alta disponibilidad CLUSTER) 16
5.1.2. Database Vault 16
5.1.3. Advanced Security 16
5.1.4. Database Firewall (Alta disponibilidad CLUSTER) 16
5.1.5. Shareplex 17
5.2. Propiedad del Licenciamiento 17
5.2.1. Modalidad Housing o Colocation 17
5.2.2. Modalidad Colocation Compartido 17
5.2.3. Modalidad Infraestructura Propia 17
6. REQUISITOS ADICIONALES 19
6.1. Modalidad Housing o Colocation 19
6.2. Modalidad Colocation Compartido 20
6.3. Modalidad de Infraestructura Propia 23
7. SERVICIO WEB–AUTENTICACIÓN BIOMETRICA – PRODUCCIÓN 26

7.1. Objetivo General 26
7.2. Objetivos Específicos 26
7.3. Antecedentes del Proyecto 27
7.4. Alcance del Proyecto 27
7.5. Acrónimos / Glosario 27
7.6. Descripción Técnica del Intercambio de Información 31
7.6.1. Descripción funcional del servicio 31
7.6.2. Descripción Técnica 32
7.7. Funcionalidad, Validación, Peticiones y Entrega de Datos 33
7.8. Requerimientos de Hardware 41
7.9. Consideraciones de la Arquitectura 42
7.10. Requerimientos de Licenciamiento 43
7.11. Requerimientos de Escalabilidad de la Infraestructura 45
7.12. Requerimientos de Seguridad 46
7.13. Requerimiento de Logs 48
7.14. Requerimiento de Archivos 54
8. REQUERIMIENTOS DE SOPORTE Y MANTENIMIENTO 61
8.1. Modalidad Housing o Colocation 61
8.2. Modalidad Colocation Compartido 61
8.3. Modalidad Infraestructura Propia 61
9. REQUERIMIENTO INFRAESTRUCTURA ALTA DISPONIBILIDAD 62
9.1 Alta disponibilidad en datacenter alterno del OAID principal en infraestructura propia (Activo/Activo – Activo/Pasivo) 62
9.2. Alta disponibilidad con un OAID alterno (Activo/Activo – Activo/Pasivo) 62
10. REQUERIMIENTO EN EL DESARROLLO DEL SOFTWARE 69
11. REQUERIMIENTO DE MODULOS DE AUTOGESTIÓN O MÓDULOS DESATENDIDOS 70
12. REQUERIMIENTOS DE SEGURIDAD EN DISPOSITIVOS MÓVILES 73

1. MODALIDAD DE ACCESO

Las modalidades de acceso y consulta a la réplica de la base de datos dispuesta por la REGISTRADURÍA, para el proceso de autenticación biométrica se definen a continuación:

1.1 Modalidad Housing o Colocation

La REGISTRADURÍA, contratará el servicio de Housing o Colocation con el proveedor del DataCenter, en donde dispondrá la base de datos, con el fin de instalar y alojar la base de datos de información biométrica.

La plataforma de hardware, software, licenciamiento y software de cotejo (MATCHER) será responsabilidad de la REGISTRADURÍA, para que las entidades autorizadas por la Ley inter-operen con la base de datos biométrica de la REGISTRADURÍA.

Esta modalidad tendrá viabilidad una vez recibidos los recursos por parte del Ministerio de Hacienda para dicho propósito y que se haya ejecutado el proceso de implementación.

1.2 Modalidad Colocation Compartido

La REGISTRADURÍA, contratará el servicio de Housing o Colocation con el proveedor del Data Center, en donde dispondrá la base de datos, con el fin de instalar y alojar la información biométrica de la REGISTRADURÍA

La plataforma de hardware, software y licenciamiento será responsabilidad de la REGISTRADURÍA, para que las entidades autorizadas por la Ley inter-operen con la base de datos biométrica de la REGISTRADURÍA.

Las entidades autorizadas por la Ley contratarán el servicio de Housing o Colocation con el proveedor del Data Center, en donde la Registraduría disponga la base de datos biométrica, con el fin de instalar y alojar en él su propia infraestructura, necesaria para inter-operar con el web service dispuesto por la REGISTRADURÍA para el proceso de autenticación biométrica

Las entidades autorizadas por la Ley y/o su aliado tecnológico (OAID), serán los responsables de realizar el cotejo (MATCHER), con la información suministrada por la REGISTRADURÍA a través del web service.

Esta modalidad tendrá viabilidad una vez recibidos los recursos por parte del Ministerio de Hacienda para dicho propósito y que se haya ejecutado el proceso de

implementación.

1.3 Modalidad Infraestructura Propia

La Entidad autorizada por la ley y/o su aliado tecnológico, deberá instalar en un datacenter TIER III o superior, o que homologue o supere las especificaciones técnicas de la norma TIA-942 TIER III y en la infraestructura física de una empresa que preste exclusivamente los servicios de multi-hospedaje, bajo su cuenta y riesgo, la plataforma tecnológica completa (sistema de almacenamiento, servidores de aplicación, base de de datos, auditoria, Firewall de acceso con su respectivo licenciamiento de hardware y software)), definida por la REGISTRADURÍA.

Las entidades autorizadas por la ley y/o su aliado tecnológico (OAID) serán los responsables de realizar el cotejo (MATCHER), con la información suministrada por la REGISTRADURÍA a través del web service.

Las especificaciones técnicas de la plataforma tecnológica que deberá proveer la entidad consultante, así como los lineamientos para el esquema de comunicaciones, serán informadas a las entidades interesadas autorizadas por la ley y/o a su aliado tecnológico que hayan presentado la prueba técnica satisfactoriamente.

***PARÁGRAFO**: La entidad autorizada que requiera acceder al servicio de autenticación biométrica bajo la modalidad de Infraestructura Propia, deberá disponer de un data center cetificado Tier 3 o superior o que homologue o supere las especificaciones de la norma TIA 942 Tier 3. en el territorio colombiano, para alojar en éste la réplica, es decir la base de datos biométrica que permita el acceso y la consulta a los datos que produce y administra la Registraduria Nacional del Estado Civil, así como el hardware, software y licenciamiento a proveer. La infraestuctura podrá ser suministrada por el aliado tecnológico (OAID).*

NOTA: Para un mejor entendimiento del presente documento, se deben considerar las definiciones contempladas en el numeral 7.5 ACRONIMOS / GLOSARIO.

La plataforma Tecnológica (hardware, software, licenciamiento y otras exigencias) definida por la REGISTRADURÍA, para los procesos de autenticación biométrica dactilar, deberá cumplir con los requerimientos y exigencias mínimas en lo relacionado con:

- Hardware de Servidores en Alta Disponibilidad (base de datos, almacenamiento, aplicaciones, herramientas de seguridad)
- Balanceadores de Carga en Alta disponibilidad
- Firewall Acceso y de Base de Datos en Alta disponibilidad
- UTM (Unified Threat Management) ó IDS
- Licenciamiento requerido
- Requerimientos de Soporte y Mantenimiento
- Servicio Web – Autenticación Biométrica en Producción
- Solución de Auditoría en Alta disponibilidad
- Centralización de Logs (peticiones, consultas, cotejos no satisfactorios), para consulta y descarga en tiempo real.

- Plataforma web de parametrización de usuarios, clientes, equipos y trámites, para consulta y descarga en tiempo real.
- MDM (Mobile Device Management)

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO

EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

2. HARDWARE

Para los servidores de base de datos, aplicaciones, Audit Vault y Firewall se permite servidores físicos o virtualizado, los cuales deben estar ubicados en un mismo rack.

2.1. Servidores

2.1.1. Base de datos

2.1.1.1. Hardware Almacenamiento para las bases de datos

SAN	
CAPACIDAD MÍNIMA	6 TB (EFECTIVAS CONFIGURACION EN RAID 5)
TIPO DE DISCOS DUROS	SAS 10K o superior o FlashArray
VELOCIDAD DE LOS PUERTOS FC	8GB mínimo
CANTIDAD	1

Nota 1: Teniendo en cuenta el incremento transaccional, la solución de almacenamiento debe ser escalable de acuerdo a cada OAID. En caso de requerirse una mayor capacidad de almacenamiento esta será solicitada por la REGISTRADURÍA.

Nota 2: El sistema de almacenamiento podrá ser compartido con diferentes sistemas de información que hagan parte del servicio de autenticación biométrica, previa autorización de LA REGISTRADURIA, para lo cual es el OAID debe aumentar la capacidad de almacenamiento mínima exigida.

2.1.1.2. Hardware servidores de base de datos

PROCESADOR	3.0 GHz o superior (4 cores mínimo)
CANTIDAD DE PROCESADORES	1 mínimo
MEMORIA RAM	32 GB mínimo
ALMACENAMIENTO	Mínimo de 300 GB en configuración RAID 5
TARJETA DE RED	REDUNDANTE
FUENTE DE PODER	REDUNDANTE
TARJETAS HBA	2 X 8G
SISTEMA OPERATIVO	AIX, Oracle Linux, Linux RedHat

	Enterprise
CANTIDAD DE SERVIDORES	2 (Mínimo para configuración RACK Alta disponibilidad)

Nota: La virtualización de los servidores de base de datos se podrá realizar en una máquina física, con las características mínimas requeridas en éste numeral para los servidores físicos, garantizando siempre alta disponibilidad y el uso de la tecnología soportada por el fabricante. Las maquinas físicas virtualizadas solo podrán ser utilizadas para el proceso de autenticación biométrica con la REGISTRADURÍA.

2.1.2. Aplicaciones

PROCESADOR	3.0 GHz o superior (4 cores mínimo)
CANTIDAD DE PROCESADORES	2
MEMORIA RAM	24 GB mínimo
ALMACENAMIENTO	Mínimo de 300 GB en configuración RAID 5
TARJETA DE RED	REDUNDANTE
FUENTE DE PODER	REDUNDANTE
SISTEMA OPERATIVO	LINUX REDHAT ENTERPRISE o Oracle Linux
CANTIDAD DE SERVIDORES	2 (Mínimo para configuración RACK Alta disponibilidad)

2.1.3. Oracle Audit Vault

PROCESADOR	3.0 GHz o superior (4 cores mínimo)
CANTIDAD DE PROCESADORES	2
MEMORIA RAM	32 GB mínimo
ALMACENAMIENTO	Mínimo de 300 GB en configuración RAID 5
TARJETA DE RED	REDUNDANTE
FUENTE DE PODER	REDUNDANTE
SISTEMA OPERATIVO	APPLIANCE ORACLE / ORACLE LINUX
CANTIDAD DE SERVIDORES	2 (ALTA DISPONIBIDAD)

2.1.4. Oracle Firewall

PROCESADOR	3.0 GHz o superior (4 cores mínimo)
CANTIDAD DE PROCESADORES	2
MEMORIA RAM	32 GB mínimo
ALMACENAMIENTO	Mínimo de 300 GB en configuración RAID 5
TARJETA DE RED	REDUNDANTE
FUENTE DE PODER	REDUNDANTE
SISTEMA OPERATIVO	APPLIANCE ORACLE / ORACLE LINUX
CANTIDAD DE SERVIDORES	2 (ALTA DISPONIBIDAD)

NOTA: La virtualización de Audit Vault y Oracle Firewall se podrá realizar en una máquina física, siempre y cuando el fabricante de dichas herramientas certifique la compatibilidad y performance de la máquina. En este sentido se deberá suministrar dos (2) servidores físicos con las características descritas en este numeral, para la virtualización e instalación de Audit Vault y Oracle Firewall en cada servidor.

NOTA 2: La incorporación o renovación del HARDWARE descrito en este documento por nuevas tecnologías que igualen o superen los requerimientos técnicos y de seguridad, deberán ser revisadas, evaluadas y autorizadas por la REGISTRADURÍA.

Todo tipo de cambio, que por renovación tecnológica del fabricante del hardware obligue a una actualización, debe ser aprobado por la REGISTRADURÍA.

2.2. Disponibilidad

La disponibilidad local mínima requerida para estos servidores debe ser del 99.98%

2.3. Responsabilidades de Administración

2.3.1. Housing o Colocation

La instalación, configuración y administración del hardware y software (sistemas operativos, motor de base de datos, web service), puesto a disposición por la REGISTRADURÍA, será responsabilidad de la misma.

2.3.2. Colocation Compartido

La instalación, configuración y administración del hardware y software (sistemas operativos, motor de base de datos, web service), puesto a disposición por la REGISTRADURÍA para el proceso de autenticación biométrica será responsabilidad de la misma.

La instalación, configuración y administración del hardware y software, que interopere con el web service dispuesto por la REGISTRADURÍA, es responsabilidad del OAID y/o CLIENTE.

2.3.3. Infraestructura Propia

La administración y suministro del hardware y software (sistemas operativos, motor de base de datos), licenciamiento, comunicaciones, internet, seguridad, y balanceo de carga es responsabilidad del OAID y/o CLIENTE.

Los costos asociados a la administración de los datos y aplicativos software (Web Service), que pone a disposición la REGISTRADURÍA, deberán ser asumidos por el OAID y/o CLIENTE.

El costo del suministro del hardware y software de auditoria serán asumidos por el OAID y/o CLIENTE.

La administración de los datos (Base de Datos y Sincronización) y aplicativo software (Web Service) puesto a disposición por la REGISTRADURÍA, será responsabilidad del OAID a través del ADMINISTRADOR que acredite el cumplimiento de los requerimientos técnicos habilitantes definidos a continuación:

2.3.3.1 Requerimientos técnicos habilitantes para la Administración.

2.3.3.1.1. Empresa

- Certificado de existencia y representación legal,expedido por la Cámara de Comercio vigente, con fecha de expedición no superior a 90 días calendario.
- Experiencia mínima de 5 años en administración de bases de datos Oracle, donde se especifique la calidad del servicio como bueno o excelente.
- Experiencia en gestión de altos volúmenes de información superior a 10.000.000 de registros, en bases de datos Oracle.
- Partner Oracle con certificación vigente.
- Dos (2) Certificaciones en donde indique el buen manejo y reserva de la información, además que se prestó el servicio a satisfacción.

2.3.3.1.2. Personal asignado al proyecto

- Ingeniero(s) de Sistemas, Electrónico o afines con Certificación Profesional Oracle OCP 19c o superior, con más de 5 años de experiencia como Oracle DBA.
- Certificación en Oracle Real Application Clusters (RAC) 19c. o superior, con experiencia comprobada mínima de un (1) año en instalación, configuración y administración de dicha herramienta.
- Experiencia mínima de un (1) año, en sincronización de bases de datos Oracle.
- Certificación en herramientas de auditoría de Oracle (Audit Vault, Database Vault, Advance Security), o experiencia comprobada mínima de un (1) año en instalación, configuración y administración de dicha herramienta.
- Experiencia especifica, mínima de dos (2) años, en Sistemas Operativos Linux Red Hat.
- Experiencia especifica, mínima de dos (2) años en instalación y administración de servidor de aplicaciones WildFly
- Experiencia en gestión de altos volúmenes de información superior a 10.000.000 de registros, en bases de datos Oracle.

NOTA 1: Las empresas que se encuentren habilitadas como administradores de base de datos y web service en los datacenter habilitados para el proceso de autenticación biométrica, solo deben acreditar los siguientes requisitos:

- Certificado de existencia y representación legal expedido por la Cámara de Comercio vigente, con fecha de expedición no superior a 90 dias calendario.
- Partner Oracle vigente.
- Certificación de continuidad del personal especificando nombres y apellidos y actividad a desarrollar dentro del proyecto. En el caso de presentar cambios en el personal debe acreditar los requisitos exigidos.

Nota 2: El personal asignado al proyecto solo puede dar soporte simultaneo a máximo (tres) datacenter dispuesto para autenticación biometrica con la REGISTRADURIA. ,

2.4. Sistema de Backup

2.4.1. Modalidad Housing o Colocation

El operador del servicio del DATA CENTER garantizará la ejecución de las rutinas de backup de los LOGs, así como el de los sistemas Operativos de los servidores.

- Los Requerimientos mínimos para el resguardo de esta conexión deben ser de tipo seguro VPN Firewall to Firewall, activación de protocolos de cifrado AES – 3DES o superior, establecimiento de reglas y herramientas de filtrado.
- A nivel interno LAN, deben existir técnicas de subdireccionamiento, aseguramiento de swicthes, router e implementación de VLAN que permitan independizar el tráfico y evitar posibles accesos indebidos a la información. El diagrama de la infraestructura debe ser presentado y aprobado por parte de la REGISTRADURÍA.
- Todo tipo de cambio que por renovación tecnológica del fabricante del hardware obligue a una actualización, debe ser aprobado por la REGISTRADURÍA.

4.2. Ancho de banda

Las características mínimas que el operador de datacenter garantizará son:

- Ancho de banda dedicado mínimo disponible 10 Mbps entre el datacenter de la REGISTRADURÍA y el datacenter del OAID.
- Disponibilidad 99.982%.
- Aplicación de protocolos y algoritmos de cifrado fuerte de datos para la transmisión de la información.

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO

5. LICENCIAMIENTO REQUERIDO

Teniendo en cuenta que la REGISTRADURÍA es responsable de la información y que al estar almacenada en una plataforma distinta para los fines misionales de identificación, es imprescindible que se licencien, además del sistema operativo y motor de base de datos, herramientas de software que garanticen y gestionen la confidencialidad de la información, de tal manera que permita el cifrado de la base de datos, segregar las funciones de administradores y usuarios y adicionalmente contar con una herramienta de auditoria que aloje sus trazas en un repositorio seguro, diferente al operativo y en donde puedan ser consultadas por la REGISTRADURIA.

El software a licenciar es el siguiente:

DESCRIPCIÓN	SISTEMA	VERSIÓN	CANTIDAD LICENCIAS	Modalidad (Responsable)		
				Housing o Colocation	Colocation Compartido	Propia
Licenciamiento Sistema operativo Servidores base de datos	Oracle Linux / AIX / RedHat Enterprise /	Vigente con soporte	Una por cada servidor	Registraduria	Registraduria	OAID

Licenciamiento Oracle	Oracle Enterprise Opción RAC "Perpetua", "Full use", conocida como Licenciamiento Hosting on Behalf REGISTRADURÍA.	19c o superior	Mínimo dos (2) por servidor o MV.			
S.O. Servidores de Acceso	Linux RedHat Enterprise / Oracle Linux	Vigente con soporte	Una (1) Suscripción por servidor			
APP. Servidores de acceso	WildFly	Vigente	Open Source			
Oracle Audit Vault y Data base Firewall	Oracle Linux	19c o superior	Misma cantidad de Licencias de Oracle por Servidor o MV			
Oracle Database Vault	Oracle Linux	19c o superior	Misma cantidad de Licencias de Oracle por Servidor o MV			
Oracle Advance Security	Oracle Linux	19c o superior	Misma cantidad de Licencias de Oracle por Servidor o MV			
Sharplex	Agente	Vigente	Mínimo una (1)			

Nota: El OAID deberá incrementar la cantidad de licencia cuando el porcentaje de carga de la base de datos supere el 70%. El aumento de licencias se debe realizar en cada uno de los servidores de base de datos, herramientas de seguridad y auditoria de Oracle en las mismas cantidades. El ADMINISTRADOR DE LA BASE DE DATOS deberá remitir al Grupo de Acceso a la Información y Protección de Datos Personales de la Registraduría, o quien haga sus veces, en los cinco primero días de cada mes, las estadísticas de carga de la base de datos del mes inmediatamente anterior. No remitir esta información en el tiempo establecido, se entenderá que el porcentaje de carga supero el límite establecido y el OAID deberá incrementar la cantidad de licencias en cada uno de los servidores.

El OAID debe demostrar anualmente a la REGISTRADURÍA, a más tardar el 31 de enero de cada año, que cada uno de los componentes de hardware y software cuentan con soporte y garantía vigente mediante documentos emitidos por el fabricante.

5.1. Productos imprescindibles de seguridad para protección de la base de datos

5.1.1. Audit Vault (Alta disponibilidad CLUSTER)

Se deberá habilitar esta solución para la consolidación, protección y gestión de registros de auditoría generados por las bases de datos. Mediante esta herramienta se definirán reglas para generar alertas y registros de auditoría sobre aquellas actividades de interés para la REGISTRADURÍA, tales como conexiones, consultas y cambios, entre otros. Se deberán activar las funciones de cifrado y de control de acceso, de manera que los registros de auditoría no puedan ser eliminados o modificados por ningún usuario, incluyendo usuarios privilegiados.

5.1.2. Database Vault

Mediante esta herramienta se ejecutará control de acceso altamente granular a la base de datos a partir de la restricción del acceso a los datos por parte de cualquier usuario, inclusive un usuario privilegiado, de acuerdo con los requerimientos de la REGISTRADURÍA. Se aplicarán esquemas de autorización multifactor mediante la definición de reglas, que contemplan elementos como la hora y el origen de la conexión y permitirán hacer seguimiento de quién está accediendo y a qué datos, a partir de registros de auditoría y reportes predefinidos. Se adiciona un nivel de protección a los datos sensibles, previniendo ataques internos y externos, facilitando la debida diligencia en términos de protección y privacidad de la información.

5.1.3. Advanced Security

Se activarán servicios de autenticación fuerte y el cifrado de los datos, sin afectar las aplicaciones. El cifrado puede realizarse en el almacenamiento (a nivel del tablespace completo de la aplicación o de algunas columnas seleccionadas), en las comunicaciones sobre la red y en los medios utilizados para las copias de respaldo, previniendo así posibles ataques que atenten contra la confidencialidad e integridad de la información, la privacidad de los datos de los ciudadanos y demás información sensible.

5.1.4. Database Firewall (Alta disponibilidad CLUSTER)

Se deberá implementar Database Firewall para vigilar el tráfico SQL entrante. Se deberá configurar como protección a amenazas de inyección SQL y ejecución de sentencias SQL no autorizadas. Esta solución deberá estar implementada para

cumplir las políticas de seguridad y alerta sobre las anomalías presentadas.

5.1.5. Shareplex

Se deberá instalar y configurar el agente Shareplex para realizar la réplicación de la base de datos (Replica_II) desde el datacenter de la REGISTRADURÍA y el datacenter dispuesto por el OAID.

5.2. Propiedad del Licenciamiento

5.2.1. Modalidad Housing o Colocation

El licenciamiento de todos los productos Oracle es a perpetuidad y de tipo "Full use" , este licienciamiento deberá ser utilizado exclusivamente para el acceso a los datos y a las bases de datos de la información que produce y administra la REGISTRADURÍA, en cuyo caso la propiedad de este licenciamiento deberá ser transferida a la REGISTRADURÍA.

Esta modalidad de licenciamiento "Perpetua", "Full use" es conocida como Licenciamiento Hosting on Behalf REGISTRADURÍA.

5.2.2. Modalidad Colocation Compartido

El licenciamiento de todos los productos Oracle es a perpetuidad y de tipo "Full use" , este licenciamiento deberá ser utilizado exclusivamente para el acceso a los datos y a las bases de datos de la información que produce y administra la REGISTRADURÍA, en cuyo caso la propiedad de este licenciamiento deberá ser transferida a la REGISTRADURÍA.

Esta modalidad de licenciamiento "Perpetua", "Full use" es conocida como Licenciamiento Hosting on Behalf REGISTRADURÍA.

5.2.3. Modalidad Infraestructura Propia

El licenciamiento de todos los productos Oracle es a perpetuidad y de tipo "Full use". Este licenciamiento deberá ser utilizado exclusivamente para el acceso a los datos y a las bases de datos de la información que produce y administra la REGISTRADURÍA.

En caso de la finalización previa del convenio con el CLIENTE y/o OAID o el(los) contrato(s) de servicio de Housing o Colocation con el Operador de Data Center, la propiedad de este licenclamiento deberá ser transferida a la REGISTRADURÍA. Esta modalidad de licenciamiento "Perpetua", "Full use" es conocida como Licenciamiento Hosting on Behalf REGISTRADURÍA.

Las licencias "Perpetua", "Full use" ORACLE Entreprise – Opción RAC – Opción Particioning 12c Release 2 o superior Full Use, deben estar a nombre de REGISTRADURÍA. El CLIENTE y/o OAID deben presentar un certificado del fabricante que así lo indique.

De igual forma el OAID será responsable de mantener vigentes los contratos de soporte del licenciamiento de base datos por el periodo de prestación del servicio, y remitir soporte que acredite la vigencia de la liencia a la REGISTARDURÍA a más tardar el 31 de enero de cada año.

Los costos asociados a la realización de estas actividades deben ser asumidos por el OAID.

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

6. REQUISITOS ADICIONALES

De acuerdo con lo previsto en el Decreto 2241 de 1986 y ante la prohibición del tratamiento de imágenes de huellas dactilares, el CLIENTE y/o OAID se comprometerán a realizar todo el ciclo de vida de la transacción biométrica mediante el uso de templates (ISO 19794-2, ANSI 378, PKMAT) y datos alfanumericos de manera cifrada, garantizando el no almacenamiento de éstas en ninguna base de datos u otro tipo de almacenamiento permanente o temporal.

6.1. Modalidad Housing o Colocation

La REGISTRADURÍA, a través del Operador de DATA CENTER que disponga, implementará lo relacionado con:

6.1.1. CANAL DE DATOS PARA LA INTERCONEXION DEL DATA CENTER DEL SERVICIO DE HOUSING o COLOCATION Y EL DATA CENTER PRINCIPAL DE LA REGISTRADURÍA.

6.1.2. FIREWALL Perimetral (Alta Disponibilidad) y Firewall de Base de Datos (Alta disponibilidad).

6.1.3. UTM ó IPS/IDS

6.1.4. SISTEMA DE ALMACENAMIENTO SAN

6.1.5. EJECUCIÓN OPERATIVA DE LABORES DE BACKUP

6.1.6. La instalación, configuración y administración del hardware y software (sistemas operativos, motor de base de datos), es responsabilidad del Operador de DATA CENTER.

6.1.7. La administración de los datos y aplicativo software puesto a disposición por la REGISTRADURÍA será responsabilidad de la misma.

6.1.8. La selección de los equipos de red debe hacerla el Operador del DATA CENTER. Dado que en la medida la plataforma crezca, las ampliaciones o modificaciones de la conectividad que permitan garantizar los servicios son su responsabilidad y garantizarán las condiciones necesarias para la operación.

6.1.9. El suministro de una plataforma web para descargar diariamente los logs de peticiones y respuestas, con su respectivo hash SHA-256.

6.1.10. Módulo de auditoria incluyendo correlacionador de eventos.

El CLIENTE y/o OAID implementará lo relacionado con:

6.1.11. Entregar a la REGISTRADURÍA el procedimiento que se aplicará en la captura

de la huella de los titulares de los datos.

6.1.12. El suministro de una plataforma web, para que la REGISTRADURÍA verifique en tiempo real (on-line) los usuarios autorizados, sedes e identificación de equipos de cómputo del usuario final dispuestos para el proceso de autenticación biométrica. La consulta debe permitir realizar reportes y/o la generación de archivos planos con su respectivo hash en SHA256. La plataforma debe generar logs para las transacciones de actualización y/o borrado de usuarios.

6.1.13. El Front-END, debe tener la funcionalidad de informar y requerir autorización del ciudadano titular de la información sobre el tratamiento de sus datos personales antes de realizar el cotejo, cuya autorización debe garantizar que se realizó de forma previa, expresa e informada y deberá almacenarse garantizando integridad, disponibilidad, confiabilidad y no repudio, a través de mecanismos electrónicos, cuya trazabilidad permita su fácil consulta. Este proceso deberá incorporar la estampa de tiempo por una entidad autorizada. El texto de autorización para el tratamiento de datos personales debe incluir como mínimo el NUIP del titular, el NUT, la fecha y hora de la estampa cronológica del documento y sede y código del cliente de la transacción o producto.

6.1.14. Los dispositivos biométricos dispuestos por el CLIENTE, deben estar homologados por la REGISTRADURÍA. Así mismo, cada unidad de dispositivo biométrico debe estar identificada por la REGISTRADURÍA, los cuales serán publicados en la página web de la REGISTRADURÍA. Cada dispositivo biométrico que sea ensamblado/producido/fabricado del modelo homologado por la REGISTRADURÍA deberá ser informado a la REGISTRADURÍA por el fabricante o distribuidor autorizado y cubrir los costos asociados a la publicación de cada dispositivo.

6.1.15. Suscrito el convenio o contrato entre la REGISTRADURÍA y el CLIENTE, los Acuerdos de Niveles de Servicio (ANS), se definirán entre el Operador del DATA CENTER y LA REGISTRADURÍA, con el objeto de llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, entre otros servicios que se requieran.

6.2. Modalidad Colocation Compartido

La REGISTRADURÍA, a través del Operador de DATA CENTER que disponga, implementará lo relacionado con:

6.2.1. CANAL DE DATOS PARA LA INTERCONEXION DEL DATA CENTER DEL SERVICIO DE HOSTING DEDICADO Y EL DATA CENTER PRINCIPAL DE LA REGISTRADURÍA.

6.2.2. FIREWALL Perimetral (Alta Disponibilidad) y Firewall de Base de Datos(Alta disponibilidad)

6.2.3. UTM ó IPS/IDS

6.2.4. SISTEMA DE ALMACENAMIENTO SAN

6.2.5. EJECUCIÓN OPERATIVA DE LABORES DE BACKUP

6.2.6. La instalación, configuración y administración del hardware y software (sistemas operativos, motor de base de datos) es responsabilidad del Operador de DATA CENTER.

6.2.7. La administración de los datos y aplicativo software puesto a disposición por la REGISTRADURÍA será responsabilidad de la misma.

6.2.8. La selección de los equipos de red debe hacerla el Operador del DATA CENTER. Dado que en la medida que la plataforma crezca las ampliaciones o modificaciones de la conectividad que permitan garantizar los servicios son su responsabilidad y garantizar las condiciones necesarias para la operación.

6.2.9. Módulo de auditoria incluyendo correlacionador de eventos.

El CLIENTE y/o OAID implementará lo relacionado con:

6.2.10. Entregar a la REGISTRADURÍA el procedimiento que se aplicará en la captura de la huella de los titulares de los datos

6.2.11. El suministro de una plataforma web para que la REGISTRADURÍA pueda consultar en tiempo real y descargar diariamente los logs de peticiones y respuestas, con su respectivo hash en SHA256 y el suministro de una plataforma para la extracción de logs de manera automática.

6.2.12. El OAID deberá disponer de una plataforma web de gestión de usuarios, sedes, equipos y trámites para que la REGISTRADURÍA consulte por diferentes criterios de busqueda y desactive en tiempo real (on-line) los usuarios, sedes y equipos de cómputo autorizados del usuario final dispuestos para el proceso de autenticación biométrica. La consulta debe permitir realizar reportes y/o la generación de archivos planos con su respectivo hash en SHA256. La plataforma debe generar logs para las transacciones de gestión de usuarios, sedes, equipos y trámites para ser consultada por la REGISTRADURÍA por diferentes criterios de busqueda. Dicha plataforma de gestión de usuarios, sedes y equipos deberá ser actualizada permanentemente por el CLIENTE y/o OAID. El OAID deberá validar que los usuarios, sedes, equipos y trámites se encuentren creados y activos antes de realizar la consulta a la base de datos dispuesta por la REGISTRADURÍA para el proceso de autenticación biométrica.

6.2.13. El Front-END, debe tener la funcionalidad de informar y requerir autorización

del ciudadano titular de la información sobre el tratamiento de sus datos personales antes de realizar el cotejo, cuya autorización debe garantizar que se realizó de forma previa, expresa e informada y el documento deberá almacenarse garantizando integridad, disponibilidad, confiabilidad y no repudio, a través de mecanismos electrónicos cuya trazabilidad permita su consulta en tiempo real por parte de la REGISTRADURÍA a traves de un portal web. Este proceso deberá incorporar en el documento la estampa de tiempo por una entidad autorizada en Colombia. El texto de autorización para el tratamiento de datos personales debe incluir como mínimo el NUIP del titular, el NUT, la fecha y hora de la estampa cronológica del documento y sede y código del cliente de la transacción o producto.

6.2.14. Los dispositivos biométricos dispuestos por el CLIENTE, deben estar homologados por la REGISTRADURÍA. Así mismo, cada unidad de dispositivo biométrico debe estar identificada por la REGISTRADURÍA, los cuales serán publicados en la página web de la REGISTRADURÍA. Cada dispositivo biométrico que sea ensamblado/producido/fabricado del modelo homologado por la REGISTRADURÍA deberá ser informado a la REGISTRADURÍA por el fabricante o distribuidor autorizado y cubrir los costos asociados a la publicación de cada dispositivo.

6.2.15. El OAID deberá permitir el acceso a la información y la instalación de los equipos necesarios en el DATACENTER para la consolidación y análisis de transacciones electrónicas por parte de CSIRT gobierno y/o SOC de la REGISTRADURÍA, previa autorización de la REGISTRADURÍA, teniendo en cuenta que la infraestructura dispuesta para el proceso de autenticación es considerada como crítica por el Estado Colombiano.

6.2.16. Suscrito el convenio o contrato entre LA REGISTRADURÍA y el CLIENTE, los acuerdos de niveles de servicio (ANS), se definirán entre el Operador de DATA CENTER, el CLIENTE y/o OAID, con objeto de llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, entre otros servicios que se requieran.

Los demás componentes corresponden al servicio de arrendamiento bajo la modalidad de Housing o Colocation que deberá suscribir el CLIENTE y/o OAID con el Operador del DATA CENTER.

6.3. Modalidad de Infraestructura Propia

El CLIENTE y/o OAID y/o ADMINISTRADOR DE LA BASE DE DATOS implementará lo relacionado con:

6.3.1. Canal de datos para la interconexion del data center del servicio infraestructura propia y el data center principal de la REGISTRADURÍA.

6.3.2. La conectividad "canal de datos" para la interconexión entre la infraestructura propia del OAID y la REGISTRADURÍA, debe ser gestionada por el operador del DATA CENTER y aplicar las políticas de seguridad de la información establecidas por la REGISTRADURÍA y estándares de seguridad informática.

6.3.3. Con la finalidad de cumplir con lo dispuesto por la REGISTRADURÍA en las políticas de seguridad informática y garantizar la seguridad de las comunicaciones entre el DataCenter de la REGISTRADURÍA y el Data Center del CLIENTE y/o OAID, el CLIENTE y/o OAID deberá suministrar un canal de datos cifrado que cumpla con las siguientes especificaciones técnicas:

a) Velocidad de conexión 10 Mbps o superior.
b) Disponibilidad mínima: 99.98%.

6.3.4. FIREWALL Perimetral de última Generación (Alta disponibilidad) y Firewall de Base de Datos(Alta disponibilidad)

6.3.5. UTM ó IPS/IDS

6.3.6. Sistema de almacenamiento SAN

6.3.7. Ejecución operativa de labores de backup.

6.3.8. La instalación, configuración y administración del hardware y software (sistemas operativos, motor de base de datos) es responsabilidad del CLIENTE y/o OAID.

6.3.9. La infraestructura será exclusiva por OAID. No se autoriza compartir la infraestructura entre OAID. Para las entidades que se presenten como uniones temporales, aplica la misma exigencia.

6.3.10. La administración de la base de datos puesta a disposición por la REGISTRADURÍA se realizará a través del ADMINISTRADOR DE BASE DE DATOS.

6.3.11. El software de administración del web service se realizará a través de la REGISTRADURÍA.

6.3.12. El Front-END, debe tener la funcionalidad de informar y requerir autorización del ciudadano titular de la información sobre el tratamiento de sus datos personales (ATDP) antes de realizar el cotejo, cuya autorización debe garantizar que se realizó de forma previa, expresa e informada y el documento deberá almacenarse garantizando integridad, disponibilidad, confiabilidad y no repudio, a través de mecanismos electrónico cuya trazabilidad permita la consulta en tiempo real, por parte de la REGISTRADURÍA, a través de un portal web. Este proceso deberá incorporar, en el documento, la estampa de tiempo por una entidad de certificación abierta autorizada en Colombia. El texto de autorización para el tratamiento de datos personales debe incluir como mínimo el NUIP del titular, el NUT, la fecha y hora de la estampa cronológica del documento y sede y código del cliente de la transacción o producto.

6.3.13. El OAID, deberá suministrar una plataforma web para que la REGISTRADURÍA consulte y descargue en tiempo real los Logs de peticiones y respuesta con diferentes criterios de búsqueda (rango de fechas, y/o Cliente, y/o NUIP y/o NUT y/o MAC), con su respectivo hash en SHA256. Los LOGs diarios de peticiones y respuestas, con su respectivo hash en SHA256, deberán ser dispuestos en un servidor para la consolidación por parte de la REGISTRADURÍA. Los registros de los LOGs de peticiones deben ser congruentes con los registros de los LOGs de consultas.

6.3.14. El OAID deberá disponer de una plataforma web de gestión de usuarios, sedes, equipos y trámites para la consulta por diferentes criterios de búsqueda por parte de la REGISTRADURÍA. Así mismo, la plataforma web deberá permitir a la REGISTRADURÍA desactivar en tiempo real (on-line) los usuarios, sedes, estaciones de captura y dispositivos biométricos autorizados por cada CLIENTE y dispuestos para el proceso de autenticación biométrica. La consulta debe permitir realizar reportes y/o la generación de archivos planos con su respectivo hash en SHA256. La plataforma web debe generar Logs para las transacciones de gestión de usuarios, sedes, equipos y trámites, para ser consultada por la REGISTRADURÍA por diferentes criterios de búsqueda. Dicha plataforma de gestión de usuarios, sedes, equipos y trámites deberá ser actualizada permanentemente por el CLIENTE y/o OAID. El OAID deberá validar que los usuarios, sedes y equipos se encuentren creados y activos antes de realizar la consulta a la base de datos dispuesta por la REGISTRADURÍA para el proceso de autenticación biométrica.

6.3.15. Todo equipo hardware, para procesamiento de aplicaciones, base de datos, seguridad, auditoria y demás funcionalidades deberán ser de marcas reconocidas en el mercado (No clones).

6.3.16. No se permite incorporar servidores re-utilizados (refurbished) en ningún caso, incluyendo los appliance a que haya lugar. Por lo anterior se requiere

que el OAID presente las respectivas certificaciones de los fabricantes con las respectivas fichas técnicas de la totalidad del hardware que hace parte de su infraestructura tecnológica, soporte y garantía.

6.3.17. El CLIENTE deberá entregar a la REGISTRADURÍA el procedimiento que se aplicará para la captura de la huella de los titulares de los datos.

6.3.18. El OAID deberá realizar pruebas de penetración (Hacking Ético y Pentesting) por lo menos dos (2) veces al año a la infraestructura técnológica dispuesta para el proceso de autenticación biométrica y cuando la REGISTRADURÍA lo requiera. Las pruebas deben ser realizadas por una entidad experta en seguridad informática certificada para estos fines. El OAID deberá remitir copia del informe final a la REGISTRADURÍA. Copia de los informes emitidos por la empresa de seguridad, debe ser remitido a más tardar el 31 de enero (primer informe) y el 31 de julio (segundo informe) de cada año. En caso de encontrase vulnerabilidades, están deben ser subsanadas por el OAID, para lo cual deberá remitir el cronograma de las actividades para subsanar la/las vulnerabilidades.

6.3.19. El OAID debe sustentar a la REGISTRADURÍA que el DATACENTER se encuentra certificado como "Tier III" (por el Uptime Institute) o superior, o que homologa o supera la norma TIA 942 – Tier III, presentando la documentación necesaria que así lo acredite por una entidad experta. La REGISTRADURÍA realizará la verificación y lista de chequeo para sustentar el cumplimiento de lo referido en este numeral, de acuerdo con la solicitud realizada por el CLIENTE. Lo anterior es prerrequisito para autorizar la instalación de la Base de Datos para autenticación biométrica.

6.3.20. Los acuerdos de niveles de servicio (ANS), se definirán entre el Operador del DATACENTER, OAID y/o el CLIENTE, con objeto de llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, entre otros servicios que se requieran.

6.3.21. El OAID deberá presentar a la REGISTRADURÍA el procedimiento para la recuperación de backup en el caso de requerir la restauración, que garanticen la continuidad de la operación. Asimismo, deberá presentar reportes mensuales de los logs de los backups generados, acordes con las políticas de backups definidas. La recuperación del backup debe ser autorizado por la REGISTRADURÍA

6.3.22. El OAID, deberá informar de manera inmediata a la REGISTRADURÍA cualquier evento o incidente de seguridad que afecte la disponibilidad, integridad y/o confidencialidad de la información y deberá abstenerse de ejecutar cualquier procedimiento de restauración sin la previa autorización de la REGISTRADURÍA.

6.3.23. Los dispositivos biométricos dispuestos por el CLIENTE deben estar homologados por la REGISTRADURÍA. Así mismo, cada unidad de dispositivo biométrico debe estar identificado por la REGISTRADURÍA, los cuales serán publicados en la página web de la REGISTRADURÍA. Cada dispositivo biométrico que sea ensamblado/producido/fabricado del modelo homologado por la REGISTRADURÍA deberá ser informado a la REGISTRADURÍA por el fabricante o distribuidor autorizado y cubrir los costos asociados a la publicación de cada dispositivo.

6.4. El OAID deberá permitir la instalación de los equipos (appliance – sondas) para el acceso a la información necesaria para la consolidación y análisis de transacciones electrónicas por parte de CSIRT gobierno y/o el SOC de la REGISTRADURÍA, previa autorización de la REGISTRADURÍA, teniendo en cuenta que la infraestructura dispuesta para el proceso de autenticación es considerada como infraestructura crítica por el Estado Colombiano. Los costos de operación serán asumidos por el OAID.

7. SERVICIO WEB–AUTENTICACIÓN BIOMETRICA – PRODUCCIÓN

La REGISTRADURÍA, a través de su aliado tecnológico dispondrá de un Web Service que estará en capacidad de procesar las solicitudes de los CLIENTES y/o OAID.

7.1. Objetivo General

Implementar el sistema informático, a través de servicios web, que permita a la REGISTRADURÍA, poner a disposición los datos biométricos y biográficos de los colombianos con el fin de posibilitar los servicios de autenticación biométrica 1:1.

7.2. Objetivos Específicos

- Disponer de una arquitectura de software y hardware, que permita cumplir con los requerimientos de concurrencia y disponibilidad definidos para el proyecto de servicios de autenticación biométrica.
- Disponer de un aplicativo software capaz de ofrecer al CLIENTE las minucias biométricas bien sea en formato ISO-FMR, ANSI-FMR o PKM, y los datos biográficos no sujetos a reserva legal.
- Instalar y configurar el aplicativo Web Service (WS) dispuesto por la REGISTRADURÍA, en los equipos de cómputo provisto por el CLIENTE y/o la REGISTRADURÍA, de acuerdo con la modalidad de acceso.

7.3. Antecedentes del Proyecto

La REGISTRADURÍA, en cumplimiento del artículo 159 de la Ley 1753 de 2015 y del artículo 18 del Decreto 019 de 2012, ha creado la viabilidad de poner a disposición datos biográficos y biométricos, de personas colombianas, con el propósito de realizar operaciones de verificación de Identidad (Cotejo 1:1), a partir de los datos recibidos desde las bases de datos de la entidad.

7.4. Alcance del Proyecto

El objetivo de la solución para los Servicios de Autenticación Biométrica es poner a disposición del CLIENTE, la base de datos de autenticación biométrica en un DATA CENTER certificado "Tier 3" o superior, o que cumpla, homologue o supere las especificaciones definidas en la norma ANSI/TIA-942 - TIERIII "Telecommunications Infrastructure Standard for Data Centers", el cual estará en la capacidad de soportar un flujo transaccional inicial de tres mil (3.000) Tx/min. Esta base de datos se llamará Réplica II.

La REGISTRADURÍA y/o el CLIENTE y/o OAID, dispondrá del hardware y software necesario de cómputo, base de datos, comunicaciones, conectividad, auditoria y esquemas de seguridad, de acuerdo con la modalidad de acceso, para que se realice la instalación y configuración necesaria para cumplir con la plataforma tecnológica requeridos para acceder al Servicio Web (WS) de consulta a la base de datos de autenticación biométrica.

7.5. Acrónimos / Glosario

Esta sección contiene una lista de todos los acrónimos y términos usados en este documento.

ACRÓNIMO	SIGNIFICADO
ADMINISTRADOR	Persona jurídica que instala, configura y administra el WS y REPLICA II.
ALFANUMÉRICO	Valor que puede contener dígitos (0..9), caracteres alfabéticos (a..z, A..Z) y/o caracteres especiales imprimibles.
ALIADO TECNOLOGICO	Empresa de tecnología presentada por una entidad pública o privada que ejerce la función de OPERADOR o ADMINISTRADOR DE BASE DE DATOS Y DE WEB SERVICE en el proceso de autenticación biométrica.
ANS	Acuerdos de Niveles de Servicio
ANSI	Instituto Nacional de Normalización Estadounidense. (ANSI por su sigla en inglés)
ANSI-FMR	Formato ANSI de minucias de huellas dactilares. Su mención en este documento estará relacionada con el formato de minucias de huellas dactilares ANSI INCITS-378.
ANSI EIA TIA-942	Telecommunications Industry Association's – Estándar Americano que especifica los requerimientos mínimos de telecomunicaciones

	para la infraestructura de data center y salas de computo.
APN	(Access Point Name). Configuración para que los dispositivos móviles puedan conectar a internet a través de un operador de telefónia móvil. En Colombia los operadores son: Tigo, Claro, Movistar, UNE, UFF, ETB, Virgin Mobile, Movil Exito, Avantel, entre otros
APLICANTE	Corresponde a la persona Colombiana que requiere ser autenticada.
ATDP	Autorización de Tratamiento de Datos Personales. Documento que debe ser informado al APLICANTE antes de consultar la base de datos Replica_II y almacenado electrónicamente para consulta en línea por la REGISTRADURÍA
AUTENTICACIÓN	Proceso de COTEJO 1:1 de minucias de huellas de un APLICANTE contra las minucias de huellas de un CANDIDATO.
BIOINTER	Base de datos biométrica dactilar y biográfica intermedia dispuesta a partir de la base de datos del Sistema de Identificación que produce y administra la REGISTRADURÍA.
BPS	Bits por segundo.
CANDIDATO	Corresponde a los datos del APLICANTE encontrados en la base de datos de REPLICA II
CASE-SENSITIVE	Indica que hay diferencias entre mayúsculas y minúsculas. Ejemplo: casa es diferente a Casa, a CASA, a CaSa, etc..
CICLO DE VIDA DE LA TRANSACCIÓN	Inicia desde el envío de la información para la consulta biométrica en la estación de captura al datacenter del OAID y finaliza cuando la estación de captura se recibe el resultado del cotejo biométrico del OAID.
CLIENTE	Entidad pública, particular que ejerza funciones públicas, o entidad autorizada por la ley, para el acceso a la información biográfica y biométrica de la REGISTRADURÍA.
CONEXIÓN GPRS	General Packet Radio Services (Servicios generales de paquetes por radio) o 2,5 G. Tecnología entre la segunda (2G) y la tercera (3G) generación de tecnología móvil digital. Se transmite a través de redes de telefonía móvil y envía datos a una velocidad de hasta 114 Kbp.
CONEXIÓN 3G	Tercera generación de transmisión de voz y datos a través de telefonía móvil mediante UMTS (Universal Mobile Telecommunications System o servicio universal de telecomunicaciones móviles).
CONEXIÓN 4G	Cuarta generación de tecnologías de telefonía móvil. Sucede a las tecnologías 2G y 3G. Las velocidades máximas de transmisión de datos deben estar entre 100 Mbit/s para una movilidad alta y 1 Gbit/s para movilidad baja
CONEXIÓN 5G	Quinta generación de tecnología celular, con mayor velocidad de carga y descarga, conexiones mas estables y con capacidad superior a las redes anteriores.
CONTRASEÑA FUERTE	Característica de las claves de acceso a un sistema de información que hace complejo descifralas tanto por humanos como por sistemas informáticos. La contraseña debe tener una longitud igual o superior a 8 caracteres compuesta por letras mayúsculas y minúsculas, números y caracteres especiales.
COTEJO 1:1	Proceso de verificación de correspondencia biométrica entre las minucias de huellas de un APLICANTE contra las minucias de huellas de un CANDIDATO.
DATACENTER	Centro de procesamiento de datos multi-hospedaje, en una

	Infraestrutura diferente a las instalaciones del OAID, ubicado en el territorio nacional Colombiano, donde se concentran los recursos necesarios del OAID para el acceso a la base de datos REPLICA II y el procesamiento de la información del CLIENTE. El data center debe ser instalado en la infraestructura de una empresa que preste exclusivamente los servicios de multi-hospedaje.
DISPOSITIVOS ELECTRÓNICO MÓVILES	Equipos electrónicos con capacidad de procesamiento y funcionalidades limitadas, que pueden ser transportados con facilidad y que cuentan con una capacidad de batería suficiente para funcionar autónomamente como Tablet, Tabléfonos y Teléfonos móviles.
ENROLAR	Registrar en una base de datos información relacionada con personas, usuarios o elementos para su posterior consulta.
GBPS	Giga Bits Por Segundo.
HIT	Coincidencia o acierto durante el COTEJO 1:1
IaaS	Infraestructura como servicio (Infrastructure as a Service) es un servicio en la nube (Cloud) en la cual el proveedor de la nube se encarga de la infraestructura (hardware, virtualización, seguridad física)
ID	Identificador o Identificación.
INCITS	International Committee for Information Technology Standards. (Comité Internacional para los Estándares de Tecnología de la Información).
ISO	International Organization Standard (Organización Internacional de Estandarización).
ISO-FMR	Formato ISO de minucias de huellas dactilares. Su mención en este documento estará relacionada con el formato de minucias de huellas dactilares ISO-FMR-19794-2:2011.
LAN	Local Área Network (Red de área local)
MINITABLETAS	Similares a la tabletas pero de menor tamaño, con tamaños entre 7 y 8 pulgadas.
NFC	(Near Field Communication) Comunicación de campo cercano. Comunicación inalámbrica de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos por acercamiento.
NIP	Número de Identificación Personal.
NO HIT	No coincidencia o no acierto durante el COTEJO 1:1.
NUIP	Número Único de Identificación Personal.
NUT	Número Único de Transacción: Número de transacción generado por cada OAID.
ON-PREMISE	Infraestructura de hardware y software que se instala y ejecuta en las instalaciones del CLIENTE
OAID	Operador de Autenticación de Identidad Digital Nivel 1 - Aliado tecnológico del CLIENTE o CLIENTE certificado por la REGISTRADURÍA con la infraestructura tecnológica para consumir el servicio web y realizar el cotejo biométrico con las minucias dactilares suministradas por la REGISTRADURÍA.
OTP	Password de un solo uso (One Time Password). Son códigos numéricos de un solo uso que se utilizan para autenticación.
PaaS	Plataforma como Servicio (Platform as a Service) es un servicio en la nube (Cloud) en la cual el proveedor de la nube (Amazon Web, Google, Oracle, Microsoft, IBM, Alibaba Cloud, etc) ofrece

	capacidades de infraestructura de aplicaciones como servicio. El proveedor se encarga de la infraestructura, del sistema operativo y del middleware.
PDAs	Personal Digital Assistant (Asistente Personal Digital) organizadores electrónicos u ordenadores de mano
PKM	Formato de minucias de huellas dactilares de IDEMIA (PK MAT) utilizado en el sistema de identificación de la REGISTRADURÍA.
PORTÁTIL CONVERTIBLE	Computador portátil que permite funcionar como tableta o como computador portátil normal.
RAC	Real Application Clusters.
REGISTRADURIA	Registraduria Nacional del Estado Civil.
REPLICA_II	Base de datos con información biográfica y biométrica dactilar dispuesta por la REGISTRADURÍA para autenticación biométrica dactilar
SaaS	Software como Servicio (Software as a Services) es un servicio en la nube (Cloud) en la cual el proveedor de la nube se encarga de la infraestructura, del sistema operativo del middleware y de las aplicaciones.
SAN	Storage Area Network (Red de área de almacenamiento)
SSL	Secure Sockets Layer. Protocolo diseñado para transmitir información de manera segura. Garantiza las relaciones de confianza entre usuario/empresa. Antecede al protocolo de cifrado TLS.
TABLETA O TABLET	Dispositivo portátil de mayor tamaño que un teléfono inteligente o PDA, en la que se interactúa mediante una pantalla táctil.
TELÉFONO INTELIGENTE	Teléfono celular con pantalla táctil, que permite conexión a internet, gestionar correos electrónicos e instalación de aplicaciones. Conocido también como smartphone.
TLS	Transport Layer Security. Seguridad de la capa de transporte. Protocolo de cifrado que proporciona comunicación segura en una red informática.
TOKEN DE SEGURIDAD	Dispositivo electrónico para facilitar el proceso de autenticación. Estos dispositivos se utilizan para generar códigos aleatorios y que utilizados como complemento a una constraeña.
TRANSACCIÓN BIOMETRICA	Ciclo de vida de la transacción desde la captura de la primera huella hasta el resultado de la consulta y/o cotejo 1:1
VPN	Virtual Private Network (VPN). Tecnología de red lógica de computadores que permite una extensión segura de la red de área local (LAN) sobre una red pública.
WI-FI	Mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.
WS	Servicio Web (Web Service) dispuesto por la REGISTRADURÍA para acceder a la REPLICA II.
SWITCH	Conmutador dispositivos que permite la interconexión de redes.
TCP	Transmission Control Protocol (Protocolo de Control de Transmisión).
TIER 3 O SEMEJANTE	Datacenter con certificación Tier 3 en cualquiera de sus modalidades emitida por el Uptime Institute ó que se certifique que cumple con TODAS las características de TIER 3 enunciadas en la norma TIA-942.
TX/min	Transacciones por minuto.
WAN	Wide Area Network (Red de área extendida).

7.6. Descripción Técnica del Intercambio de Información

De acuerdo con lo previsto en los Decretos 2241 de 1986 y 1581 de 2012, y ante la prohibición del tratamiento de imágenes de huellas dactilares, el CLIENTE y/o OAID se comprometerán a realizar la transacción biométrica mediante el uso de template correspondiente (ISO 19794-2, ANSI 378, PKMAT) y biográfica de manera cifrada, garantizando el no almacenamiento de éste en ninguna base de datos u otro tipo de almacenamiento.

El cifrado de las imágenes de huellas y templates debe realizarse desde el dispositivo biométrico y las llaves de cifrado solo pueden ser administradas por el OAID.

La extracción de las minucias debe realizarse con el SDK de un proveedor de tecnología biométrica de las organizaciones participantes del MINEX TEST (Última versión aprobada).

Las imágenes de las huellas no podrán ser expuestas al cliente o almacenadas. De requerir la presentación de la imagen de la huella por pantalla, la solución debe ser dispuesta solo por el OAID realizando ofuscación sobre la imagen, con la respectiva autorización de la REGISTRADURÍA.

La transacción biométrica deberá garantizar un tiempo de vida máximo de 2 minutos.

7.6.1. Descripción funcional del servicio

El servicio ofrece las siguientes funcionalidades:

- Recepción de información
- Entrega de información
- Validación del NUT.
- Validación del ID del OAID.
- Validación del ID del CLIENTE.
- Validación de la pareja OAID y CLIENTE.
- Validación del NUIP.
- Validación del ID del Dedo de la Huella 1.
- Validación del ID del Dedo de la Huella 2.
- Validación del Formato de las Minucias.
- Validación de Edad del CANDIDATO.

Además de las mencionadas funcionalidades, el servicio cuenta con las siguientes características

- **Validación**: Validación del CLIENTE y el OAID que acceden al servicio.
- **Gestión de Autorizaciones**: Permite el acceso a la REPLICA II al CLIENTE y al OAID (pareja CLIENTE- OAID) sólo para realizar aquellas consultas para las que han sido habilitados.

- **Seguridad.** Todas las consultas se realizarán con plenas garantías de seguridad, confidencialidad, integridad y protección de datos personales.
  - El sistema registrará todas las consultas realizadas, identificando siempre al OAID, al CLIENTE, las sedes, equipos asociados y usuarios finales.
  - El sistema garantizará la confidencialidad de los datos intercambiados.
  - Todas las comunicaciones que se realicen entre la REGISTRADURÍA y el OAID se configurarán sobre canales dedicados, protocolo https (TLS) y además se proporciona en el tramo troncal, medidas adicionales de cifrado de datos.
- **Trazabilidad**: Cada petición y su correspondiente respuesta se registra en el sistema.
- **Auditoría**: Todas las peticiones van identificadas con un identificador único (NUT), que permite su posterior recuperación ante posibles reclamaciones o auditorías del servicio.
- **Administración**: Para facilitar la gestión del CLIENTE y OAID (crear / modificar / habilitar / deshabilitar) el sistema debe contar con un módulo encargado de esta gestión. Para ello, se da la administración del sistema por parejas CLIENTE vs OAID.

7.6.2. Descripción Técnica

7.6.2.1. SOLUCIÓN

La plataforma actual se define como una arquitectura orientada a servicios (SOA) basada en los siguientes elementos:

- Funcionalidades mediante Servicios Web (WS) y presentación externa de las mismas expresadas en WSDL.
- No hay documentos XML intercambiados entre los servicios web (SOAP) y firmados electrónicamente mediante XMLDsig.
- Establecimiento de canales seguros mediante protocolo TLS.

7.6.2.2. Utilización de otros servicios

El sistema disponible para el proceso de Autenticación Biométrica usa los siguientes servicios:

- Sincronización de la Base de Datos REPLICA_II a partir de la Base de Datos BIOINTER.

7.6.2.3. Estándares

Se utilizarán los estándares abiertos siguientes en su versión estable más reciente:

- **Protocolos de transferencia de hipertexto**:
  RFC 2616: Hypertext Transfer Protocol – HTTP/1.1

- **Integración de datos y aplicaciones**:

Extensible Markup Language (XML)
Simple Object Access Protocol (SOAP) 1.1
Web Services Description Language (WSDL)
XML Schema Part 1: Structures & Part 2: Datatypes.

- **Seguridad**:
  Transport Layer Security TLS

7.7. Funcionalidad, Validación, Peticiones y Entrega de Datos

Réplica II Recepción de Información.

Descripción El WS recibirá de los CLIENTES los siguientes datos:

- NUT. Número único de transacción.
- ID del OAID. Este ID o código, corresponde al OAID el cual lo crea la REGISTRADURÍA y lo dará a conocer al CLIENTE para los fines pertinentes).
- ID del CLIENTE. Este ID o código, corresponde al CLIENTE el cual lo crea la REGISTRADURÍA y lo dará a conocer al CLIENTE para los fines pertinentes.
- NUIP del APLICANTE.
- ID del Dedo correspondiente a la Huella 1. (Código del dedo de la huella 1)
- ID del Dedo correspondiente a la Huella 2. (Código del dedo de la huella 2)
- Formato de minucias requerido para la autenticación (PKM, ISO-FMR o ANSI-FMR).

Estado Obligatorio
Categoría Funcional
Detalle El formato de plantilla para la solicitud de minucias requerido para la autenticación debe ser el aprobado por la REGISTRADURÍA durante la presentación de la prueba técnica (PKM, ISO-FMR o ANSI-FMR).

A continuación detalles de los valores esperados por parte del OAID:

Detalle	Tipo	Tamaño (Bytes)	Obligatorio
NUT generado por el OAID.	Cadena	12	Sí
ID del OAID.	Cadena	8	Sí
ID del CLIENTE.	Cadena	8	Sí
ID del APLICANTE (NUIP).	Cadena	11	Sí
ID de los dedos asociados a las huellas	Lista	1..2	Sí

solicitadas. Los valores permitidos deberán estar entre 1 y 10.	Numérica		
Formato de minucias requerido para la autenticación ("PKM", "ISO-FMR" o "ANSI-FMR").	Cadena	Variable	Sí

Aclaración: La solicitud debe contener el ID de al menos un dedo del APLICANTE. En caso contrario, se retornará la respuesta asociada a un error o ausencia de datos de entrada, tampoco se entregarán datos asociados al CANDIDATO.

A continuación, la lista de ID de Dedos:

Dedo	Descripción
1	Pulgar Derecho.
2	Índice Derecho.
3	Medio Derecho.
4	Anular Derecho.
5	Meñique Derecho.
6	Pulgar Izquierdo.
7	Índice Izquierdo.
8	Medio Izquierdo.
9	Anular Izquierdo.
10	Meñique Izquierdo.

Réplica II Captura de huellas desde el lector biométrico:
Descripción Captura de una o dos huellas del aplicante
Estado Obligatorio
Categoría Funcional
Detalle El sistema deberá incorporar la opción de seleccionar aleatoriamente los dedos de las manos que serán cotejados por el CLIENTE y/o el OAID contra la base de datos dispuesta por la REGISTRADURÍA y/o como última opción la captura de la huella diferente al impreso en el documento de identidad.

Réplica II Entrega de información.
Descripción El Servicio Web (WS) entregará los siguientes datos en caso de encontrar un registro asociado a la solicitud de búsqueda:

- NUIP.
- Nombre 1.

- Nombre 2.
- Apellido 1.
- Apellido 2.
- Partícula (Código + Descripción).
- Lugar de Expedición del Documento de Identificación.
- Fecha de Expedición del Documento de Identificación.
- Minucias, si existe, de la primera huella (PKM, ISO-FMR o ANSI-FMR).
- Minucias, si existe, de la segunda huella (PKM, ISO-FMR o ANSI-FMR).
- Vigencia del Documento de Identificación (Código + Descripción).
- NUT.
- ID del OAID.
- ID del CLIENTE.
- ID del LOG asociado a la solicitud búsqueda.
- Resultado de la Búsqueda.

Estado Obligatorio
Categoría Funcional
Detalle A continuación el detalle de la estructura a entregar:

Detalle	Tipo	Tamaño (Bytes)	Obligatorio
Resultado de la Búsqueda. Código de respuesta del proceso de búsqueda del WS al OAID.	Cadena	Variable	Sí
NUT generado por el OAID.	Cadena	12	No
ID del LOG asociado a la búsqueda.	Numérico	8	Sí
ID del OAID.	Cadena	50	No
ID del CLIENTE.	Cadena	50	No
Lista con los datos del CANDIDATO encontrado, conteniendo: ID del Valor y Valor Devuelto.	Lista Compuesta	1..11	No
Lista con los datos de las minucias del CANDIDATO en el formato solicitado, conteniendo: ID del dedo, Formato de las Minucias y Minucias.	Lista Compuesta	1..2	No

Relación de datos biográficos suministrados por el WS: correspondiente a la lista de los datos del CANDIDATO

Ítem	Detalle	Tipo	Tamaño (Bytes)
1	NUIP del CANDIDATO.	Cadena	11
2	Primer Nombre del CANDIDATO	Cadena	60
3	Segundo Nombre del CANDIDATO.	Cadena	60
4	Código de la partícula del CANDIDATO.	Cadena	1
5	Descripción de la partícula del CANDIDATO.	Cadena	256
6	Primer Apellido del CANDIDATO.	Cadena	60
7	Segundo Apellido del CANDIDATO.	Cadena	60
8	Lugar de Expedición del Documento.	Cadena	256
9	Fecha de Expedición del Documento.	Fecha	10
10	Código de la Vigencia del Documento de Identificación.	Cadena	2
11	Descripción de la Vigencia del Documento de Identificación.	Cadena	256

Aclaración: Si alguno de los datos anteriores no existe en la base de datos, la etiqueta asociada a dicho valor no será enviada.
Relación de datos biométricos suministrados por el WS correspondiente a la lista con los datos de las minucias del CANDIDATO:

Detalle	Tipo	Tamaño (Bytes)
ID del dedo.	Numérico	1
Formato de las minucias de la huella solicitada: "PKM", "ISO-FMR" o "ANSI-FMR". Estos valores son case-sensitive.	Cadena	Variable
Datos de las minucias de la huella solicitada; la cadena de datos irá codificada en Base64.	Cadena	Variable

Aclaración: Por cada minucia de huella solicitada y encontrada irá un conjunto de datos con la estructura de la tabla anterior.
En caso de no encontrar ninguna de las minucias de huellas solicitadas no se hará entrega de ningún dato asociado al candidato.

Aclaración: El Servicio Web (WS) entrega al OAID las minucias en formato ISO-FMR o ANSI-FMR o PKM y en Base 64, el OAID deberá convertir las minucias a Base 256 (Binario) antes de hacer el cotejo.

Réplica II Validación del NUT.

Descripción	Se hará una validación básica del NUT: no se validará el formato del valor del NUT, este valor se rechazará sólo cuando esté vacío o cuando contenga sólo espacios en blanco.
Estado	Obligatorio
Categoría	Funcional
Detalle	En caso de un error producto de la validación de este dato, el proceso de búsqueda se detendrá, se generará el LOG correspondiente y se enviará una respuesta de error al OAID.

Réplica II Validación del ID del OAID.

Descripción	Se hará una validación básica del ID del OAID contra una lista de referencia de OAID habilitados por la REGISTRADURÍA
Estado	Obligatorio
Categoría	Funcional
Detalles	La habilitación o inhabilitación de un OAID sólo será realizada por la REGISTRADURÍA. En caso de un error producto de la validación de este dato, el proceso de búsqueda se detendrá, se generará el LOG correspondiente y se enviará una respuesta de error al OAID.

Réplica II Validación del ID del CLIENTE.

Descripción	Se hará una validación básica del ID del CLIENTE contra una lista de referencia de CLIENTES habilitados por la REGISTRADURÍA
Estado	Obligatorio
Categoría	Funcional
Detalles	La habilitación o inhabilitación de un CLIENTE sólo será realizada por la REGISTRADURÍA. En caso de un error producto de la validación de este dato, el proceso de búsqueda se detendrá, se generará el LOG correspondiente y se enviará una respuesta de error al OAID.

Réplica II Validación de la pareja OAID y CLIENTE.

Descripción	Se hará una validación básica de la relación entre el OAID y EL CLIENTE contra una lista de referencia de parejas de OAID y CLIENTES habilitados.
Estado	Obligatorio
Categoría	Funcional
Detalles	La habilitación o inhabilitación de una pareja OAID y CLIENTE sólo será realizada por la REGISTRADURÍA. En caso de un error producto de la validación de este dato, el proceso de búsqueda se detendrá, se generará el LOG correspondiente y se enviará una respuesta de error al OAID.

Réplica II Validación del NUIP.

Descripción	Se hará una validación básica del NUIP del APLICANTE: no se

validará el formato del NUIP, este valor se rechazará sólo cuando esté vacío o cuando contenga sólo espacios en blanco.

Estado Obligatorio
Categoría Funcional
Detalles El NUIP podrá contener valores alfanuméricos.

En caso de un error producto de la validación de este dato, el proceso de búsqueda se detendrá, se generará el LOG correspondiente y se enviará una respuesta de error al OAID.

La responsabilidad del formato, del tipo de documento y de la validación del contenido del NUIP estará del lado del OAID.

RÉPLICA II hará la búsqueda con el NUIP tal cual como fue recibido.

Réplica II Validación del ID del Dedo de la Huella 1.
Descripción Se hará una validación básica del ID del Dedo de la Huella 1: sólo se permitirán valores entre uno (1) y diez (10).
Estado Obligatorio
Categoría Funcional
Detalles En caso de un error producto de la validación de este dato, el proceso de búsqueda se detendrá, se generará el LOG correspondiente y se enviará una respuesta de error al OAID.

Réplica II Validación del ID del Dedo de la Huella 2.
Descripción Se hará una validación básica del ID del Dedo de la Huella 2: sólo se permitirán valores entre uno (1) y diez (10).
Estado Obligatorio
Categoría Funcional
Detalles En caso de un error producto de la validación de este dato, el proceso de búsqueda se detendrá, se generará el LOG correspondiente y se enviará una respuesta de error al OAID.

Réplica II Validación del Formato de las Minucias.
Descripción Se hará una validación básica del Formato de las Minucias. Sólo se permitirán los formatos "PKM", "ISO-FMR" y "ANSI-FMR".

Adicionalmente se validará que el formato de minucias solicitado esté autorizado por la REGISTRADURÍA a la pareja OAID – Cliente de donde proviene la solicitud de búsqueda
Estado Obligatorio
Categoría Funcional
Detalles Estos valores son case-sensitive.
En caso de un error producto de la validación de este dato, el proceso de búsqueda se detendrá, se generará el LOG correspondiente y se enviará una respuesta de error al OAID.

Réplica II	Validación de Edad del CANDIDATO.
Descripción	La edad mínima del CANDIDATO para autorizar la entrega de sus datos al OAID dependerá de la edad acordada entre la REGISTRADURÍA y el CLIENTE.
Estado	Obligatorio
Categoría	Funcional
Detalles	La edad mínima del CANDIDATO que aplica a un CLIENTE sólo será realizada por la REGISTRADURÍA. No habrá un único rango de edad, sino que éste será según el perfil acordado entre REGISTRADURÍA y cada CLIENTE; sin embargo, para todos los casos, la edad mínima a acordar entre REGISTRADURÍA y cada CLIENTE deberá fijarse en un valor mayor o igual a 7 años. En caso de un error producto de la validación de este dato, el proceso de búsqueda se detendrá, se generará el LOG correspondiente y se enviará una respuesta de error al OAID.

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

Réplica II Tipos de Respuesta – Web Service (WS) – Códigos de Respuesta.

Descripción Los códigos de respuesta asociados a las solicitudes de:

Respuesta	Valor
CandidateNotFound	0
CandidateFound	1
CandidateFoundPartialFingers	2
CandidateNotAuthorizedByAge	3
CandidateFoundInvalidFingers	4
Error while saving transaction	13
InvalidOperatorId	110
OperatorDisabled	111
InvalidNut	120
InvalidNuipNip	130
InvalidFingerId	140
FingerDataNotEnough	142
InvalidClientId	150
ClientDisabled	151
InvalidFingerPrintFormat	160
FingerPrintFormatNotAuthorized	162
InvalidClientOperatorLink	170
ClientOperatorLinkDisabled	171
InactiveAgreement	172
ExpiredAgreement	173
MaxLimitOfTransactions	180
GroupStatusDisabled	181
InactiveAgreementGroup	182
ExpiredAgreementGroup	183
GroupNotFound	184
FingerPrintNotFound	200
FingerPrintConvertError	250
FingerPrintConvertToISOError	260
FingerPrintConvertToANSIError	270
CommunicationError	830
DataBaseError	840
UnknownError	999

Estado Obligatorio
Categoría Base de Datos/Tablas

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

7.8. Requerimientos de Hardware

Hardware Servicio de Acceso

Descripción Se deberá disponer como mínimo de la siguiente plataforma tecnológica para el proceso de autenticación biométrica:

Ítem	Cantidad	Modalidad (Responsable)		
		Housing o Colocation	Colocation Compartido	Propia
Switch Servicio de acceso - 2 Puertos de 1Gbps (mínimo) - Puertos Fast Ethernet	2	REGISTRADURÍA	REGISTRADURÍA	OAID
Servidores de aplicaciones	2 (mínimo)			
Balanceador de carga - A nivel de hardware - El operador del datacenter deberá suministrar el servicio de balanceo de carga en el acceso perimetral	2 (mínimo) Alta Disponibilidad			

Estado Obligatorio
Categoría Hardware

Hardware Hardware de Bases de Datos

Descripción Se deberá disponer de la siguiente plataforma tecnológica:

Ítem	Cantidad	Modalidad (Responsable)		
		Housing o Colocation	Colocation Compartido	Propia
Switch servidores base de datos - 2 Puertos de 1Gbps (mínimo) - Puertos Fast Ethernet	2	REGISTRADURÍA	REGISTRADURÍA	OAID
Servidores de Base de Datos	2 (mínimo) Alta disponibilida			

Estado Obligatorio
Categoría Hardware

Hardware Almacenamiento

Descripción Se deberá disponer de la siguiente plataforma tecnológica. La instalación y configuración de estos equipos es responsabilidad del OAID.

Ítem	Cantidad	Modalidad (Responsable)		
		Housing o Colocation	Colocation Compartido	Propia
Switch SAN - 8 Puertos de 1Gbps (mínimo) - Puertos Fast Ethernet	2	REGISTRADURÍA	REGISTRADURÍA	OAID
SAN	1			

Estado Obligatorio
Categoria Hardware

Hardware Hardware de Seguridad.

Descripción Se deberá disponer de tres (3) firewalls para el control de conexión entre la REGISTRADURÍA y el DATA CENTER.
Estado Obligatorio
Categoría Hardware
Detalles Un firewall corresponde al DATA CENTER y el otro estará en Sitio Central – Bogotá D.C.

Un tercer firewall de acceso a los Servicios Web (WS) será dispuesto por el OAID. (En alta disponibilidad)

La REGISTRADURÍA informará, según lo indicado en el presente documento, las especificaciones técnicas mínimas con la cual operador de comunicaciones debe prestar este servicio, esto con el fin de garantizar la validación de los paquetes de datos desde el Sitio Central hasta el DATA CENTER.

7.9. Consideraciones de la Arquitectura

La REGISTRADURÍA podrá revisar, ajustar y actualizar la arquitectura definida en el presente documento con el fin de mejorar, optimizar y escalar la solución acorde a los requerimientos establecidos para el proceso de autenticación biométrica y garantizar la integridad y seguridad de los datos almacenados .

EN BLANCO EN BLANCO EN BLANCO

7.10. Requerimientos de Licenciamiento

Licenciamiento Licenciamiento

Descripción Se deberá disponer del siguiente licenciamiento mínimo para poder instalar la solución.

DESCRIPCIÓN	SISTEMA	VERSIÓN	CANTIDAD	Modalidad (Responsable)		
				Housing o Colocation	Colocation Compartido	Propia
Licenciamiento Sistema operativo Servidores base de datos	Oracle Linux / AIX / Solaris / RedHat Enterprise /	Vigente	Una para cada servidor	Registraduría	Registraduría	OAID
Licenciamiento Oracle	Oracle Enterprise Opción RAC "Perpetua", "Full use", conocida como Licenciamiento Hosting on Behalf REGISTRADURÍA.	19c o superior	Una (1) por cada core activo Mínimo 2 por servidor Ó MV			
S.O. Servidores de Acceso	Linux Enterprise	7.0 o superior	Suscripción			
APP. Servidores de acceso	WildFly (Redhat / Oracle Linux)	30.0.0 superior	Suscripción			
Oracle Audit Vault y Data base Firewall	Oracle Linux	19c o superior	1 por vCPU de acuerdo con factor de licenciamiento Core-Procesador			
Oracle Database Vault	Oracle Linux	19c o superior	1 por vCPU de acuerdo con factor de licenciamiento Core-Procesador			
Oracle Advance Security	Oracle Linux	19c o superior	1 por vCPU de acuerdo con factor de licenciamiento Core-Procesador			
SharePlex	Oracle	19c o superior	Open Source			

El licenciamiento de Oracle deberá ser actualizado de acuerdo con el número de CORES activos de los servidores de base de datos.

Estado Obligatorio

Categoría Licenciamiento

Detalles Es de resaltar que la propiedad de la información es de la REGISTRADURÍA y que al estar almacenada en una plataforma que no está bajo su administración, es imprescindible que adicional a los requerimientos mínimos de licenciamiento que se exigen tanto para las modalidades de Housing o Colocation, Colocation Compartido o infraestructura propia, incluya herramientas de software que garanticen y gestionen la confidencialidad de la información, de tal manera que se permita cifrar la base de datos, segregar las funciones de administradores y usuarios y adicionalmente contar con una herramienta de auditoria que aloje sus trazas en un repositorio seguro, diferente al operativo y en donde puedan ser consultadas por la REGISTRADURÍA

Audit Vault

Se deberá implementar esta solución para la consolidación, protección y gestión de registros de auditoría generados por las bases de datos. Mediante esta herramienta se definirán reglas para generar alertas y registros de auditoría sobre aquellas actividades de interés para la REGISTRADURÍA, tales como conexiones, consultas y cambios, entre otros. Se deberán activar las funciones de cifrado y de control de acceso, de manera que los registros de auditoría no puedan ser eliminados o modificados por ningún usuario, incluyendo usuarios privilegiados.

Database Firewall

Se deberá implementar esta solución para vigilar el tráfico SQL entrante. Se deberá configurar como protección a amenazas de inyección SQL y ejecución de sentencias SQL no autorizadas. Esta solución deberá estar implementada para cumplir las políticas de seguridad y alerta sobre las anomalías presentadas.

Database Vault

Mediante esta herramienta se ejecutará control de acceso altamente granular a la base de datos a partir de la restricción del acceso a los datos por parte de cualquier usuario, inclusive un usuario privilegiado, de acuerdo con los requerimientos de la REGISTRADURÍA. Se aplicarán esquemas de autorización

multifactor mediante la definición de reglas que contemplan elementos como la hora y el origen de la conexión y permite hacer seguimiento de quién está accediendo,a qué datos, a partir de registros de auditoría y reportes predefinidos. Se adiciona un nivel de protección a los datos sensibles, previniendo ataques internos y externos, facilitando la debida diligencia en términos de protección y privacidad de la información.

Advanced Security

Se activarán servicios de autenticación fuerte y el cifrado de los datos, sin afectar las aplicaciones. El cifrado puede realizarse en el almacenamiento (a nivel del tablespace completo de la aplicación o de algunas columnas seleccionadas), en las comunicaciones sobre la red y en los medios utilizados para las copias de respaldo, previniendo así posibles ataques que atenten contra la confidencialidad e integridad de la información, la privacidad de los datos de los ciudadanos y demás información sensible.

SharePlex

Mediante la herramienta SharePlex se realizar la replicación de la base de datos (Replica_II) desde el datacenter de la REGISTRADURÍA y el datacenter dispuesto por el OAID.

7.11. Requerimientos de Escalabilidad de la Infraestructura

Licenciamiento	Escalabilidad de los Servicios Web y de la Base de Datos
Descripción	La arquitectura inicial deberá ser escalable de acuerdo a las necesidades, cumpliendo con las características mínimas de hardware y software exigidas por la REGISTRADURÍA en lo referente a servidores de aplicaciones y servidores de base de datos.
Estado	Obligatorio
Categoría	Escalabilidad
Detalles para	**Housing o Colocation y Colocation Compartido** La puesta a disposición del licenciamiento, software base, Base de datos y hardware necesario para lograr la escalabilidad, es responsabilidad de la REGISTRADURÍA. **Infraestructura Propia** La puesta a disposición del licenciamiento, sóftware base (sistema operativo, servidor de aplicaciones), base de datos y hardware necesario para lograr la escalabilidad, es responsabilidad del OAID.

	Todo escalamiento debe ser aprobado por la REGISTRADURÍA.
Escalabilidad	Escalabilidad Global de la Base de Datos
Descripción	La arquitectura de Oracle RAC podrá soportar un crecimiento hasta alcanzar los 100 nodos. Adicionalmente, el número de nodos estará limitado por el número de conexiones soportado por los switches.
Estado	Obligatorio
Categoría	Escalabilidad
Detalle	La puesta a disposición del licenciamiento "Perpetua", "Full use", software base, Base de datos y hardware necesario para lograr la escalabilidad.
Escalabilidad	Escalabilidad de los servidores de dominio de aplicaciones
Descripción	Los servidores de dominio de aplicaciones podrán escalar de manera horizontal y estará limitado por el número de conexiones soportado por los switches.
Estado	Obligatorio
Categoría	Escalabilidad

7.12. Requerimientos de Seguridad

Seguridad	Seguridad de acceso - DATA CENTER
Descripción	El DATA CENTER deberá contar un (1) firewall con modo de conexión "site to site", VPN, autenticación con certificados, con capacidad de cifrado, con alta disponibilidad y con un Troughtput de siete (7) Gbps sobre las interfaces de conexión.
Estado	Obligatorio
Categoría	Seguridad
Detalle para	**Housing o Colocartion y Colocation Compartido** La puesta a disposición, instalación, configuración y administración de los equipos de conexión y seguridad es de responsabilidad de la REGISTRADURÍA .
	Infraestructura Propia La puesta a disposición, instalación, configuración y administración de los equipos de conexión y seguridad es de responsabilidad del OAID.
Seguridad	Autenticación
Descripción	Sólo los OAID podrán acceder a los Servicios Web (WS) de consulta
Estado	Obligatorio

Categoría Seguridad.

Seguridad Formato de Identificadores de OAID
Descripción Los OAID estarán identificados con códigos de hasta ocho (8) caracteres alfanuméricos. Estos códigos serán asignados por la REGISTRADURÍA.

Un OAID podrá estar relacionado con uno (1) o varios CLIENTES

Estado Obligatorio

Categoría Seguridad

Seguridad Formato de Identificadores para CLIENTES.
Descripción Los CLIENTES estarán identificados con códigos de hasta ocho (8) caracteres alfanuméricos. Estos códigos serán asignados por la REGISTRADURÍA.

Un CLIENTE podrá estar relacionado con uno (1) o varios OAID.

Estado Obligatorio
Categoría Seguridad

Securidad Cifrado de Datos de Sincronización Diaria
Descripción Los datos de la sincronización diaria que se replica desde la BIOINTER al DATACENTER, viajarán por un canal seguro.
Estado Obligatorio
Categoría Seguridad

Detalle para **Housing o Colocation y Colocation Compartido**
La puesta a disposición, configuración, instalación y administración de los canales de datos es responsabilidad de la REGISTRADURÍA.

Infraestructura Propia
La puesta a disposición, configuración, instalación y administración de los canales de datos es responsabilidad del OAID.

Seguridad Canales de Datos
Descripción Se dispondrá de un canal de 10 Mbps para comunicación desde la REGISTRADURÍA al DATA CENTER. El nivel de cifrado deberá garantizarse "firewall to firewall", con disponibilidad de 99.98% (ver Detalle).
Estado Obligatorio
Categoría Seguridad

Detalle para **Housing o Colocation y Colocation Compartido**

La puesta a disposición, configuración, instalación y administración de los canales de datos es de responsabilidad de la REGISTRADURÍA.

Infraestructura Propia
La puesta a disposición, configuración, instalación y administración de los canales de datos es de responsabilidad del OAID.

Seguridad	Pruebas de vulnerabilidad (Hacking Ético y Pentesting)
Descripción	Evaluar el estado de la seguridad de la infraestructura dispuesta para el proceso de autenticación biométrica. Las pruebas deben ser realizadas por una entidad experta en seguridad informática certificada para estos fines.
Estado	Obligatorio
Categoría	Seguridad
Frecuencia	Mínimo dos (2) veces al año.
Detalle	**Housing o Colocation y Colocation Compartido:** REGISTRADURÍA **Infraestructura Propia**: OAID. EL OAID deberá remitir copia del informe final a la REGISTRADURÍA a más tardar el 31 de enero y 31 de julio de cada año, con las respectivas medidas de remediación.

7.13. Requerimiento de Logs

Log	Peticiones
Descripción	El sistema de consumo de servicio web, deberá implementar una trazabilidad de las peticiones realizadas. Cada operación a través del módulo de peticiones al Servicio Web (WS) debe quedar registrado en el sistema del OAID en un log conteniendo: 1. NUT (Numero único de transacción). 2. ID del OAID 3. ID del CLIENTE. 4. NUIP del APLICANTE. 5. ID del Dedo correspondiente a la Huella 1. 6. ID del Dedo correspondiente a la Huella 2. 7. Formato de minucias requerido para la autenticación (PKM, ISO-FMR o ANSI-FMR).

8. Fecha y Hora de la Operación.
9. Detalles de la Operación (código trámite).
10. Código del usuario final del CLIENTE que solicita la consulta
11. Dirección IP del usuario final del CLIENTE que solicita la consulta
12. Dirección MAC (PC) o IMEI (dispositivo móvil) del usuario final del CLIENTE que solicita la consulta
13. Consulta utilizando dispositivo móvil
14. Latitud en grados decimales de la ubicación del dispositivo móvil (Norte – Sur).
15. Longitud en grados decimales de la ubicación del dispositivo móvil (Este – Oeste)
16. Código de sede

Estado: Obligatorio
Categoría: Logs/Archivos
Retención: Tres (3) años
Formato: CSV separado por coma (,)
Nombre archivo: Log_peticiones_XXXXXXXXX_AAAAMMDD.csv
Donde:

- XXXXXXXXX: Nombre del OAID
- AAAAMMDD: Fecha de consumo al web service

Responsable: **Housing o Colocation**: REGISTRADURÍA.

Colocation Compartido e Infraestructura propia: OAID

Detalle: El archivo comprimido con su respectivo hash en SHA256, debe ser generado y almacenado diariamente asi:

- En un servidor dispuesto por el datacenter del OAID para ser descargar por red desde la REGISTRADURIA.
- Publicado en página web segura (https), con acceso restringido para consulta y descargue exclusivo de la REGISTRADURÍA

A continuación detalles de los campos del log:

Valor	Tipo	Tamaño (Bytes)	Detalle	Obligatorio
NUT	Cadena	12	NUT generado por el OAID.	Sí
OperatorId	Cadena	8	ID del OAID.	Sí
ClientId	Cadena	8	ID del CLIENTE.	Sí
ApplicantId	Cadena	10	ID del APLICANTE (NUIP).	Sí
FingersToGet	Lista Numérica	1..2	ID de los dedos asociados a las huellas solicitadas. Los valores permitidos deberán estar entre 1 y 10.	Sí
FingerPrintFormat	Cadena	Variable	Formato de minucias requerido para la autenticación ("PKM", "ISO-FMR" o "ANSI-FMR").	Sí
OperationDate	Fecha y Hora	17	Fecha y Hora de la Operación "yyyy-mm-dd hh:mm:ss,ms"	Sí

OperationDetails	Cadena	Variable	Detalles de la Operación Código de trámite del CLIENTE que solicita la consulta	Si
UserCode	Cadena	Variable	Código del usuario final del CLIENTE que solicita la consulta	Si
UserIP	Cadena	Variable	Dirección IP del usuario final del CLIENTE que solicita la consulta	Si
UserMac	Cadena	Variable	Dirección MAC (PC) o IMEI (dispositivo móvil) del usuario final del CLIENTE que solicita la consulta	Si
DpMovil	Cadena	Variable	Consulta utilizando dispositivos móviles. Un cero (0) para indicar que NO es dispositivo móvil. Un uno (1) para indicar dispositivo móvil.	SI
GdLatitud	Cadena	variable	Latitud en grados decimales de la ubicación del dispositivo móvil (Norte – Sur) para consulta con dispositivos móviles. Un cero (0) para indicar que NO es dispositivo móvil.	SI
GdLongitud	Cadena	variable	Longitud en grados decimales de la ubicación del dispositivo móvil (Este – Oeste) para consulta con dispositivos móviles. Un cero (0) para indicar que NO es dispositivo móvil.	Si
SedeCod	Cadena	variable	Código de la sede asociado al CLIENTE que solicita la consulta	

Log Consultas

Descripción El sistema de consumo de servicio web, deberá implementar una trazabilidad de las consultas realizadas.

Se debe generar en el Sistema del OAID un log resultado del COTEJO a la solicitud recibida por el WS de la REGISTRADURÍA. El log debe contener los siguientes datos:

1. Resultado de la Búsqueda. Código de respuesta del proceso de búsqueda del WS al OAID.
2. NUT.
3. ID de la consulta generado por el WS.
4. ID del OAID.
5. ID del CLIENTE.
6. NUIP del APLICANTE.
7. Fecha y hora de inicio de la transacción.
8. Fecha y hora de fin de la transacción.
9. ID del Dedo de la Huella 1 solicitada.
10. ID del Dedo de la Huella 2 solicitada.
11. Formato de minucias solicitado (ISO-FMR, ANSI-FMR, o PKM).

12. Resultado del cotejo para el dedo 1. (Responsabilidad del OAID)
13. Resultado del cotejo para el dedo 2. (Responsabilidad del OAID)
14. Fecha y hora de la operación. (Responsabilidad del OAID).
15. Nombre del servidor que solicita la consulta al WS.
16. Dirección IP del servidor que solicita la consulta al WS.
17. Dirección MAC del servidor que solicita la consulta al WS.

Estado: Obligatorio
Categoría: Logs/Archivos
Retención: Tres (3) años
Formato: CSV separado por coma (,)
Nombre archivo: Log_consulta_XXXXXXXXX_AAAAMMDD.csv
Donde:

- XXXXXXXXX: Nombre del OAID
- AAAAMMDD: Fecha de consumo al web service

Responsable: **Housing o Colocation:** REGISTRADURÍA.

Colocation Compartido e Infraestructura propia: OAID

Detalle: El archivo comprimido con su respectivo hash en SHA256, debe ser generado y almacenado diariamente asi:

- En un servidor dispuesto por el datacenter del OAID para ser descargar por red desde la Registarduría.
- Publicado en página web segura (https), con acceso restringido para consulta y descargue exclusivo de la Registraduría.

A continuación, detalles de los campos del log:

Ítem	Valor	Tipo	Tamaño (Bytes)	Detalle	Obligatorio
1	SearchStatus	Cadena	Variable	Resultado de la Búsqueda. Código de respuesta del proceso de búsqueda del WS al OAID.	Si
2	NUT	Cadena	12	NUT generado por el OAID.	Si
3	RequestId	Numérico	8	ID del LOG asociado a la búsqueda.	Si
4	OperatorId	Cadena	8	ID del OAID.	Si
5	ClientId	Cadena	8	ID del CLIENTE.	Si
6	AplicantId	Cadena	11	ID del APLICANTE (NUIP)	Si
7	StartDate	Fecha y Hora	17	Fecha y hora de inicio de la transacción "yyyy-mm-dd hh:mm:ss,ms"	si
8	EndDate	Fecha y	17	Fecha y hora de fin de la	Si

		Hora		transacción "yyyy-mm-dd hh:mm:ss,ms"	
9	IDFinger1	Numérico	2	ID del Dedo de la Huella 1 solicitada	Si
10	IDFinger2	Numérico	2	ID del Dedo de la Huella 2 solicitada	Si
11	FingerprintFormat	Cadena	variable	Formato de minucias solicitado (ISO-FMR, ANSI-FMR, o PKM).	Si
12	StatusFinger1	Numérico	1	Un cero (0) para indicar NO-HIT. Un uno (1) para indicar un HIT. Solo es obligatorio en caso de candidato encontrado.	Si
13	StatusFinger2	Numérico	1	Un cero (0) para indicar NO-HIT. Un uno (1) para indicar un HIT Solo es obligatorio en caso de candidato encontrado.	Si
14	OperationDate	Fecha y Hora	17	Fecha y Hora de la Operación "yyyy-mm-dd hh:mm:ss.ms"	Si
15	ServerName	Cadena	Variable	Nombre del servidor que solicita la consulta al WS	Si
16	ServerIP	Cadena	Variable	Dirección IP del servidor que solicita la consulta al WS	Si
17	ServerMac	Cadena	variable	Dirección MAC del servidor que solicita la consulta al WS	Si

El OAID deberá garantizar la integridad de la información registrada en los LOGs de **PETICIONES** y de **CONSULTAS**, los cuales deberán ser congruentes con los logs generados por el web service dispuesto por la REGISTRADURÍA.

Log Respuesta no satisfactoria

Descripción El sistema de consumo de servicio web, deberá implementar una trazabilidad de las consultas realizadas con resultado de cotejo no satisfactorio.

Se debe generar en el Sistema del OAID un log resultado no satisfactorio del COTEJO a la solicitud recibida por el WS de la REGISTRADURÍA. El log debe contener los siguientes datos:

1. NUT.
2. ID del OAID
3. ID del CLIENTE
4. NUIP del APLICANTE
5. Fecha y hora de inicio de la transacción
6. Score del cotejo dedo 1
7. Score del cotejo dedo 2
8. Minucia dedo 1 solicitada
9. Minucia dedo 2 solicitada

Estado Obligatorio
Categoría Logs/Archivos
Retención Tres (3) años
Formato CSV separado por coma (,)
Nombre archivo Log_consultaNoS_XXXXXXXXX_AAAAMMDD.csv
Donde:

- XXXXXXXXX: Nombre del OAID
- AAAAMMDD: Fecha de consumo al web service

Responsable **Housing o Colocation:** REGISTRADURÍA.

Colocation Compartido e Infraestructura propia: OAID.

Detalle El archivo comprimido con su respectivo hash en SHA256, debe ser generado y almacenado diariamente asi:

- En un servidor dispuesto en el datacenter del OAID para ser descargar por red desde la Registraduría Nacional
- Publicado en página web segura (https), con acceso restringido para consulta y descargue exclusivo de la REGISTRADURÍA

A continuación, detalles de los campos del log:

Ítem	Valor	Tipo	Tamaño (Bytes)	Detalle	Obligatorio
1	NUT	Cadena	12	NUT generado por el OAID.	Si
2	OperatorId	Cadena	8	ID del OAID.	Si
3	ClientId	Cadena	8	ID del CLIENTE.	Si
4	AplicantId	Cadena	11	ID del APLICANTE (NUIP)	Si
5	OperationDate	Fecha y Hora	17	Fecha y Hora de la Operación "yyyy-mm-dd hh:mm:ss,ms"	Si
6	ScoreFinger1	Cadena	8	Valor correspondiente al grado de similaridad del cotejo del dedo 1	Si
7	ScoreFinger2	Cadena	8	Valor correspondiente al grado de similaridad del cotejo del dedo 2	Si
8	MinuciaFinger 1	Cadena	Variable	Minucia cifrada de la dedo 1	Si
9	MinuciaFinger 2	Cadena	Variable	Minucia cifrada de la dedo 2	Si

7.14. Requerimiento de Archivos

Archivos Sedes

Descripción: El OAID deberá implementar un portal web seguro (https), donde se registren las sedes autorizadas por cada CLIENTE para acceder al servicio de autenticación biométrica.

Estado: Obligatorio

Categoría: Logs/Archivos

Retención: Permanente

Formato: CSV separado por coma (,)

Nombre archivo: Arch_Sedes_XXXXXXXXX_AAAAMMDD_HHMMSS.csv

Donde:

- XXXXXXXXX: Nombre del OAID
- AAAAMMDD: Fecha de generación de archivo.
- HHMMSS: Hora de generación del archivo.

Responsable: **Housing o Colocation**: REGISTRADURÍA.

Colocation Compartido e Infraestructura Propia: OAID

Detalle:

- El portal web debe permitir consultar y descargar los archivos por CLIENTE o CLIENTES y/o sedes y/o departamento y/o municipio y/o fechas de creación y/o modificación y/o estado
- El portal web debe tener acceso restringuido para consulta, descargue y desactivación de sedes por parte de la Registraduría.
- Los archivos deben entregarse comprimidos con su respectivo hash en SHA256.

A continuación detalles de los campos del archivo:

Item	Nombre del campo	Tipo	Tamaño (Bytes)	Detalle	Obligatorio
1	OperatorId	Cadena	8	id del OAID	Si
2	ClientId	Cadena	8	Id del Cliente.	Si
3	CodeSede	Varchar	Variable	Código de la sede donde el usuario final solicita la consulta.	SI
4	NameSede	Cadena	Variable	Nombre de la sede donde se realiza la transacción.	Si
5	AddressSede	Cadena	Variable	Dirección geográfica de la sede	Si
6	CodeDepto	Numérico	2	Código del Departamento/Pais donde se encuentra la sede, de acuerdo al código DIVIPOL Electoral de la REGISTRADURÍA	Si

7	CodeMpio	Numérico	3	Código municipio/ciudad donde se encuentra la sede, de acuerdo al código DIVIPOL Electoral de la REGISTRADURÍA	Si
8	StateSede	Numérico	1	Define el estado de vigencia de la Sede. Uno (1) para activo Cero (0) para inactivo.	Si
9	CreationDate	Fecha y Hora	17	Fecha y hora de creación del registro AAAA/MM/DD hh:mm:ss	Si
10	ModificationDate	Fecha y Hora	17	Fecha y hora de última modificación del registro. AAAA/MM/DD hh:mm:ss	Si

Archivos Usuarios

Descripción El OAID debe implementar un portal web seguro.(https), donde se registren los usuarios autorizados por cada CLIENTE para acceder al servicio de autenticación biométrica.

Estado Obligatorio

Categoría Logs/Archivos

Retención Permanente

Formato CSV separado por coma (,)

Nombre archivo Arch_Usuarios_XXXXXXXXX_AAAAMMDD_HHMMSS.csv

Donde:

- XXXXXXXXX: Nombre del OAID
- AAAAMMDD: Fecha y hora de generación de archivo.
- HHMMSS: Hora de generación del archivo.

Responsable **Housing o Colocation y:** REGISTRADURÍA.

Colocation Compartido e Infraestructura Propia: OAID

Detalle

- El portal web debe permitir consultar y descargar los archivos por CLIENTE o CLIENTES y/o fechas de creación y/o modificación y/o estado.
- El portal web debe tener acceso restringido para consulta, descargue y desactivación de usuarios por parte de la REGISTRADURÍA.
- Los archivos deben entregarse comprimidos con su respectivo hash en SHA256.

A continuación, detalles de los campos del archivo:

Item	Nombre del campo	Tipo	Tamaño (Bytes)	Detalle	Obligatorio
1	OperatorId	Cadena	8	Id del OAID	Si
2	ClientId	Cadena	8	Id del Cliente.	Si

3	CodeUser	Varchar	50	Código del usuario final del CLIENTE que solicita la consulta.	Si
4	NameUser	Cadena	Variable	Nombre del usuario final del CLIENTE que solicita la consulta.	Si
5	StateUser	Cadena	1	Define el estado de vigencia del usuario. Uno (1) para activo Cero (0) para inactivo.	Si
6	CreationDate	Fecha y Hora	17	Fecha y hora de creación del registro. Formato AAAA/MM/DD hh:mm:ss	Si
7	Modification Date	Fecha y Hora	17	Fecha y hora de la última modificación del registro. AAAA/MM/DD hh:mm:ss	Si

Archivos Estaciones de Captura

Descripción El OAID debe implementar un portal web seguro (https), donde se registra la información de estaciones de captura por cada CLIENTE para acceder al servicio de autenticación biométrica.

Estado Obligatorio

Categoría Logs/Archivos

Retención Permanente

Formato CSV separado por coma (,)

Nombre archivo Arch_Estaciones_XXXXXXXXX_AAAAMMDD_HHMMSS.csv

Donde:

- XXXXXXXXX: Nombre del OAID
- AAAAMMDD: Fecha de generación del archivo
- HHMMSS: Hora de generación del archivo.

Responsable **Housing o Colocation:** REGISTRADURÍA.

Colocation Compartido e Infraestructura Propia: OAID

Detalle

- El portal web debe permitir consultar y descargar los archivos por CLIENTE o CLIENTES y/o sedes y/o fechas de creación y/o modificación y/o estado y/o tipo dispositivo.
- El portal web debe tener acceso restringido para consulta, descargue y desactivación de equipos por parte de la REGISTRADURÍA.
- Los archivos deben entregarse comprimidos con su respectivo hash en SHA256.

A continuación, detalles de los campos del archivo:

Item	Nombre del campo	Tipo	Tamaño (Bytes)	Detalle	Obligatorio
1	OperatorId	Cadena	8	id del OAID	Si
2	ClientId	Cadena	8	Id del Cliente.	Si
3	HostName	Cadena	Variable	Nombre del host donde el usuario final solicita la consulta.	Si
4	CodeSede	Cadena	Variable	Código de la sede del Host que solicita la consulta	Si
5	UserMac	Cadena	Variable	Dirección MAC del usuario final del CLIENTE que solicita la consulta.	Si
6	UserIPIMEI	Cadena	Variable	Dirección IP o IMEI del usuario final del CLIENTE que solicita la consulta.	Si
7	DpMovil	Numérico	1	Define el tipo de dispositivo con el que se realiza el cotejo es móvil o fijo. Reportar uno (1) para móvil (Celulares, Tablet) y cero (0) para fijo.	Si
8	StateHost	Numérico	1	Define el estado de vigencia de la estación. Uno (1) para activo Cero (0) para inactivo.	Si
9	CreationDate	Fecha y Hora	17	Fecha y hora de creación del registro AAAA/MM/DD hh:mm:ss.ms	Si
10	ModificationDate	Fecha y Hora	17	Fecha y hora de última modificación del registro. AAAA/MM/DD hh:mm:ss.ms	Si

Archivos Dispositivos biométricos

Descripción El OAID debe implementar un portal web seguro (https), donde se registran los dispositivos biométricos (USB, WIFI, Dispositivo móvil Integrado) por cada CLIENTE para acceder al servicio de autenticación biométrica.

Estado Obligatorio

Categoría Logs/Archivos

Retención Permanente

Formato CSV separado por coma (,)

Nombre archivo Arch_Dispositivos_XXXXXXXXX_AAAAMMDD_HHMMSS.csv

Donde:

- XXXXXXXXX: Nombre del OAID
- AAAAMMDD: Fecha de generación del archivo

- HHMMSS: Hora de generación del archivo.

Responsable **Housing o Colocation:** REGISTRADURÍA.

Colocation Compartido e Infraestructura Propia: OAID

Detalle
- El portal web debe permitir consultar y descargar los archivos por CLIENTE o CLIENTES y/o marca y/o modelo y/o clase dispositivo y/o estado y/o fechas de creación (rangos) y/o modificación (rangos).
- El portal web debe tener acceso restringuido para consulta y descargue de dispositivos por parte de la REGISTRADURÍA.
- Los archivos deben entregarse comprimidos con su respectivo hash en SHA256.

A continuación, detalles de los campos del archivo:

Item	Nombre del campo	Tipo	Tamaño (Bytes)	Detalle	Obligatorio
1	OperatorId	Cadena	8	id del OAID	Si
2	ClientId	Cadena	8	Id del Cliente.	Si
3	MarkDevice	Cadena	Variable	Marca del dispositivo biométrico	Si
4	ModelDevice	Cadena	Variable	Modelo del dispositivo biométrico	Si
5	SerialDevice	Cadena	Variable	Número de serial del dispositivo biométrico	Si
6	ClassDevice			Clase de dispositivo biométrico: Uno (1) para dispositivos conectados por USB Dos (2) para dispositivos conectados por WIFI Tres (3) para dispositivos moviles integrados	Si
7	CodeIMEI	Cadena	Variable	Código IMEI que identifica la estación integrada. Valor cero (0) si es un dispositivo USB o WIFI	Si
8	CreationDate	Fecha y Hora	17	Fecha y hora de creación del registro AAAA/MM/DD hh:mm:ss	Si
9	ModificationDate	Fecha y Hora	17	Fecha y hora de última modificación del registro. AAAA/MM/DD hh:mm:ss	Si

Archivos Trámites

Descripción: El OAID debe implementar un portal web seguro (https), donde se registran los trámites por cada CLIENTE para acceder al servicio de autenticación biométrica.

Estado: Obligatorio

Categoría: Logs/Archivos

Retención: Permanente

Formato: CSV separado por coma (,)

Nombre archivo: Arch_Tramite_XXXXXXXXX_AAAAMMDD_HHMMSS.csv
Donde:

- XXXXXXXXX: Nombre del OAID
- AAAAMMDD: Fecha de generación del archivo.
- HHMMSSS: Hora de generación del archivo.

Responsable: **Housing o Colocation:** REGISTRADURÍA.
Colocation Compartido e InfraestructuraPropia: OAID

Detalle:

- El portal web debe permitir descargar los archivos por CLIENTE o CLIENTES y/o fechas de creación y/o modificación.
- Los archivos deben entregarse comprimidos con su respectivo hash en SHA256.

A continuación, detalles de los campos del log:

Item	Nombre del campo	Tipo	Tamaño (Bytes)	Detalle	Obligatorio
1	OperatorId	Cadena	8	ID del OAID	SI
2	ClientId	Varchar	8	Id del Cliente.	Si
3	TramiteCod	Cadena	Variable	Código de tramite del CLIENTE que solicita la consulta.	Si
4	TramiteName	Cadena	Variable	Descripción del trámite del CLIENTE que solicita la consulta	Si
5	CreationDate	Fecha y hora	17	Fecha y hora de creación del registro. AAAA/MM/DD hh:mm:ss	Si
6	ModificationDate	Fecha y hora	17	Fecha y hora de última modificación del registro AAAA/MM/DD hh:mm:ss. Por defecto debe ser la fecha de creación	Si

El OAID y/o el CLIENTE deben garantizar que la información de las sedes, estaciones de captura, dispositivos biométricos, usuarios y trámites asociados al CLIENTE se encuentren debidamente actualizados y que permitan a la REGISTRADURÍA su consulta en línea. El OAID deberá restringir el acceso al servicio de autenticación biométrica a los CLIENTES cuyas sedes, usuarios, estaciones de captura no se encuentren registrados o no se encuentren activos.

El no cumplimiento a estas disposiciones será evaluado por la REGISTRADURÍA para el proceso de renovación de la certificación del OAID.

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

8. REQUERIMIENTOS DE SOPORTE Y MANTENIMIENTO

8.1. Modalidad Housing o Colocation

La responsabilidad del soporte y mantenimiento será definida por la REGISTRADURÍA y el operador del DATA CENTER que preste el servicio de Housing o Colocation.

La división de responsabilidades de administración de hardware, software, conectividad, datos y aplicativo software deberá ser definida en los ANS.

8.2. Modalidad Colocation Compartido

La responsabilidad del soporte y mantenimiento en modalidad de Housing o Colocation deberá ser definida entre la REGISTRADURÍA, el operador del DATA CENTER que preste el servicio en modalidad de Housing o Colocation y el OAID.

8.3. Modalidad Infraestructura Propia

La REGISTRADURÍA, verificará las responsabilidades de soporte y mantenimiento para la modalidad de infraestructura propia. La REGISTRADURÍA auditará y controlará el manejo de los datos, aplicativo software y transacciones realizadas por el ADMINISTRADOR y el OAID.

El OAID y el CLIENTE tendrán la responsabilidad técnica, económica y operativa de brindar soporte, mantenimiento y administración a los sistemas y subsistemas hardware del DATA CENTER, elementos activos de red LAN del DATA CENTER, equipos de seguridad tipo firewall y comunicaciones, hardware de servidores de bases de datos, aplicaciones, sistema de almacenamiento, sistemas operativos y suministro del licenciamiento de base de datos y demás software que compone la arquitectura. Entre otras exigencias, como las mencionadas en el presente documento numeral 6.3.

La REGISTRADURÍA, podrá solicitar en cualquier momento al CLIENTE y al OAID la implementación técnica y/o procedimental de nuevas tecnologías de hardware, software, comunicaciones y seguridad que salvaguarden la información almacenada de uso indebido y/o acceso por parte de terceros.

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

9. REQUERIMIENTO INFRAESTRUCTURA ALTA DISPONIBILIDAD

El CLIENTE que requiera implementar un sistema de alta disponibilidad para garantizar un mayor nivel de servicio, podrán escoger alguna de las siguientes opciones, previa aprobación de la REGISTRADURÍA

9.1. Alta disponibilidad en datacenter alterno del OAID principal en infraestructura propia (Activo/Activo – Activo/Pasivo)

El CLIENTE que requiera implementar un sistema de alta disponibilidad en un datacenter alterno propuesto por su OAID, el OAID deberá proveer la infraestructura requerida en esta documento respecto a HARDWARE, SOFTWARE, BALANCEADORES DE CARGA, FIREWALL DE ACCESO, LICENCIAMIENTO REQUERIDO y REQUISITOS ADICIONALES. Dicha infraestructura deberá ser validada y aprobada por la REGISTRADURÍA, de acuerdo a la disponibilidad técnica para la sincronización de la base de datos.

El datacenter alterno propuesto por el OAID deberá estar ubicado en territorio colombiano que homologue o supere las especificaciones técnicas de la norma TIA-942 TIER III y debe ser diferente al datacenter principal del OAID.

El sistema deberá estar configurado por el OAID en la modalidad de ACTIVO/ACTIVO – ACTIVO/PASIVO , previa aprobación por parte de la REGISTRADURÍA.

El OAID, deberá suministrar el modelo de infraestructura y comunicaciones para la activación del datacenter alterno en la modalidad ACTIVO-ACTIVO – ACTIVO/PASIVO.

El OAID y/o el CLIENTE deberá configurar el balanceador de carga enter los datacenter y presentar a la REGISTRADURÍA la configuración de las reglas de balanceo.

La REGISTRADURÍA determinará las condiciones técnicas para la configuración del CLIENTE, del OAID y de la pareja CLIENTE-OAID en el web service dispuesto por la REGISTRADURÍA en el datacenter alterno del OAID.

9.2. Alta disponibilidad con un OAID alterno (Activo/Activo – Activo/Pasivo)

El CLIENTE que requiera implementar un sistema de alta disponibilidad ACTIVO/ACTIVO - ACTIVO/PASIVO con un OAID alterno, el OAID alterno deberá contar con la infraestructura requerida en este documento respecto a

HARDWARE, SOFTWARE, BALANCEADORES DE CARGA, FIREWALL DE ACCESO, LICENCIAMIENTO REQUERIDO y REQUISITOS ADICIONALES.

El CLIENTE debe suministrar el modelo de infraestructura y comunicaciones para la activación del datacenter alterno en la modalidad ACTIVO/ACTIVO – ACTIVO/PASIVO

Se deberá configurar el balanceador de carga entre los datacenter los dos OPERADORES y presentar a la REGISTRADURÍA la configuración de las reglas de balanceo.

La REGISTRADURÍA estudiará la solicitud del CLIENTE y de considerarlo viable, dará la viabilidad técnica, acogiéndose el CLIENTE y los OPERDORES BIOMÉTRICOS a los requerimientos legales y técnicos establecidos por la REGISTRADURÍA.

La REGISTRADURÍA determinará las condiciones técnicas para la configuración del CLIENTE, del OAID y de la pareja CLIENTE-OAID en el web service dispuesto por la REGISTRADURÍA en el datacenter del OAID alterno.

Para los casos en que el formato de minucias autorizado por la REGISTRADURÍA sea diferente entre OPERADORES, se podrá optar por alguna de las siguientes opciones, previa aprobación por parte de la REGISTRADURIA:

- El OAID PRINCIPAL deberá proveer en el datacenter del OAID alterno el hardware necesario para instalar y configurar el MATCHER en el formato de minucias autorizado por la REGISTRADURÍA.
- Realizar la captura directamente desde el dispositivo biométrico en el formato de minucias autorizado al OAID alterno. No se permite la transformación de formato de minucias.

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

10. REQUERIMIENTO DE DISPOSITIVOS BIOMÉTRICOS

Los dispositivos biométricos que los CLIENTES utilizarán en el proceso de autenticación biométrica deben cumplir los siguientes requisitos:

Dispositivo	Homologación dispositivo biométrico
Descripción	Prueba técnica de homologación de dispositivo biométrico
Estado	Obligatorio
Categoría	Dispositivo biométrico
Detalle	El fabricante del dispositivo biométrico, su representante en Colombia o un distribuidor autorizado por el fabricante en Colombia, solicitarán la prueba de homologación del dispositivo biométrico a la REGISTRADURÍA especificando el modelo del dispositivo. El fabricante del dispositivo biométrico deberá estar certificado internacionalmente en gestión de calidad en procesos productivos. La prueba de homologación se entenderá como satisfactoria si cumple la detección de dedo falso, la detección de dedo vivo, el cifrado de la minucia/imagen, FIPS 140-2 Nivel 2 o superior y la geolocalización del dispositivo (dispositivo móvil) .

Dispositivo	Producción e incorporación de dispositivos biométricos homologados
Descripción	Relación de dispositivos biométricos producidos por el fabricante del modelo homologado, en archivo plano con el siguiente contenido:
Estado	Obligatorio
Categoría	Dispositivo biométrico
Formato	CSV separado por coma (,)
Nombre archivo	Dispositivo_XXXXXXXXX_999999_AAAAMMDD_HHMMSS.csv Donde: • XXXXXXXXX: Fabricante dispositivo • 999999: Cantidad de dispositivos relacionados en el archivo • AAAAMMDD: Fecha de generación de archivo. • HHMMSS: Hora de generación del archivo.
Detalle	El fabricante del dispositivo biométrico o distribuidor autorizado debe remitir a la REGISTRADURÍA la lista de dispositivos biométricos fabricados del modelo homologado por la REGISTRADURÍA especificando el CLIENTE al cual fue suministrado.

El fabricante o distribuidor autorizado del dispositivo homologado debe cancelar a la REGISTRADURÍA la tarifa establecida para la publicación de cada dispositivo producido del modelo homologado.

El CLIENTE solo puede incorporar dispositivos biométricos homologados que se encuentren publicados en la página web de la REGISTRADURÍA, con su respectivo serial y/o identificación.

El CLIENTE solo podrá adquirir los dispositivos biométricos directamente al fabricante, al representante legal en Colombia, al distribuidor o reseller autorizado en Colombia.

El archivo plano debe contener la siguiente información:

1. Marca del dispositivo
2. Modelo del dispositivo
3. Serial del dispositivo
4. CLIENTE que adquiere el dispositivo
5. Nombre del distribuidor o reseller autorizado que realiza la venta del dispositivo
6. Fecha de venta del dispositivo al CLIENTE.

Dispositivo	Extracción de minucias
Descripción	Extracción de las minucias ISO-FMR, ANSI-FMR o PKMAT
Estado	Obligatorio
Categoría	Dispositivo biométrico
Detalle	La extracción de la minucia debe realizarse en los formatos ISO-FMR, ANSI-FMR o PKMAT. La extracción de las minucias debe realizarse con el SDK de un proveedor de tecnología biométrica de las organizaciones participantes del MINEX TEST (Última versión aprobada). La característica de SDK debe estar especificada en la ficha técnica presentada por el fabricante del dispositivo.

Dispositivo	Tecnología lector biométrico
Descripción	Incorporación de tecnologías en dispositivos biométricos de captura de una o dos huellas planas de alta calidad que cumplan los mínimos estándares de seguridad acreditados por entidades expertas en pruebas biométricas.
Estado	Obligatorio
Categoría	Dispositivo biométrico
Detalle	Cada modelo de dispositivo biométrico debe estar avalado por

el FBI (Requerimientos básicos PIV) y/o MINEX III Certified PIV y/o las respectivas pruebas biométricas certificadas por el NIST o por un laboratorio de pruebas biométricas acreditado por NIST NVLAP.

Dispositivo Detección de dedo vivo y huella falsa

Descripción Evaluar la configuración en el dispositivo biométrico la detección de dedo vivo y huella falsa.

Estado Obligatorio

Categoría Dispositivo biométrico

Detalle El dispositivo biométrico debe detectar por lo menos los siguientes materiales:

- Acetato
- Caucho
- Colbon/Pegamento
- Goma
- Latex liquido
- Papel
- Silicona Fria
- Silicona Orgánica
- Silicona Inorgánica

La detección de estos materiales no debe permitir la captura de la huella ni la generación de la respectiva minucia.

La característica de dedo vivo y huella falsa debe estar especificada en la ficha técnica presentada por el fabricante del dispositivo.

La REGISTRADURÍA determinará el cumplimiento de este requerimiento de acuerdo al sector donde se implementarán los lectores biométricos.

Dispositivo FIPS 140-2 Nivel 2 o superior

Descripción Implementación de estándares de seguridad FIPS 140-2 Nivel 2 o superior (Federal Information Processing Standard), que permita detectar la intrusión física del dispositivo, mediante sistemas de bloqueo físico

Estado Obligatorio

Categoría Dispositivo biométrico

Detalle El dispositivo biométrico para estaciones fijas y dispositivos móviles debe tener implementado el estándar de seguridad FIPS 140-2 Nivel 2 o superior, característica que debe estar especificada en la ficha técnica presentada por el fabricante.

Dispositivo	FIPS 140-2 Nivel 3 o superior
Descripción	Implementación de estándares de seguridad FIPS 140-2 Nivel 3 o superior (Federal Information Processing Standard), que incluye resistencia a la intrusión física con fines de desmontaje o modificación, de manera que dificulta los ataques, de tal manera que pueda ser capaz de borrar los parámetros del sistema.
Estado	Obligatorio
Categoría	Dispositivo biométrico
Detalle	El dispositivo biométrico para estaciones móviles debe tener implementado el estándar de seguridad FIPS 140-2 Nivel 3 o superior, característica que debe estar especificada en la ficha técnica presentada por el fabricante.

Dispositivo	Cifrado de minucia por hardware
Descripción	Configuración en el dispositivo biométrico del cifrado por hardware de la minucia/huella.
Estado	Obligatorio
Categoría	Dispositivo biométrico
Detalle	El dispositivo biométrico deberá entregar la minucia/huella al OAID cifrada.

Dispositivo	Custodia de la clave de cifrado.
Descripción	Resguardo de la clave de cifrado generada por el fabricante del dispositivo
Estado	Obligatorio
Categoría	Dispositivo biométrico
Detalle	Para el proceso de autenticación biométrica con la REGISTRADURÍA, el fabricante del dispositivo biométrico o el OAID generaran la clave de cifrado por cada CLIENTE siendo el OAID el responsable de custodia de la misma, quien garantizará que no la revelará ni entregará al CLIENTE ni a ningún otro actor del proceso. Los CLIENTES que requieran el uso de los dispositivos biométricos para usos diferentes al proceso de autenticación biométrica con la REGISTRADURÍA, deberán generar llaves de cifrado diferentes a las utilizadas en el citado proceso. Para todos los casos, la minucia deberá entregarse cifrada desde el dispositivo biométrico.

Dispositivo	Renovación de la clave de cifrado

Descripción	Sustitución o cambio de la clave de cifrado por parte del fabricante del dispositivo biométrico en caso de verse comprometida la confidencialidad de la clave de cifrado.
Estado	Obligatorio
Categoría	Dispositivo biométrico
Detalle	El fabricante del dispositivo biométrico debe generar y entregar nueva clave de cifrado al OAID por cada CLIENTE en caso de verse comprometida la confidencialidad de la clave.

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

11. REQUERIMIENTO EN EL DESARROLLO DEL SOFTWARE

Software	Requerimientos de software
Descripción	Aspectos a tener en cuenta en el desarrollo de software
Estado	Obligatorio
Categoría	Desarrollo de software
Detalle	1. No se permite el almacenamiento de datos biográficos y biométricos de los colombianos en los dispositivos fijos, móviles, en memorias externas SD, micro SD u otros medios. 2. Se deben utilizar algoritmos de cifrado FIPS 140-2 3. El acceso a la consulta biométrica debe realizarse a través de un Front End con autenticación de usuario y contraseña fuerte para autenticarse cada vez que se ingrese al sistema. 4. Para acceso desde dispositivos móviles, se debe complementar la autenticación de usuario y contraseña fuerte con uno o más factores de autenticación de un solo uso (OTP) con un tiempo máximo de vida de 2 minutos, que se generará de manera aleatoria para autenticarse cada vez que el usuario ingrese al sistema. El 5. Se debe contar con un software que permita incorporar dispositivos, usuarios, sedes y trámites. 6. Se deben generar registros de eventos y pistas de auditoría de forma detallada. 7. El software debe validar la identificación del usuario, sede y dispositivo antes de consumir el servicio de autenticación biométrica. 8. Manejo de la memoria, evitando overflows e interceptación de datos almacenados en texto claro en la memoria del dispositivo. 9. Limpiar la memoria del dispositivo al iniciar y al finalizar la sesión o por terminación anormal de la sesión. 10. Realizar ofuscación del código fuente y ocultar las clases y propiedades sensibles para la aplicación. 11. El software debe tener implementado el manejo de timeout. Para una sesión abierta desatendida el timeout máximo es de 5 (cinco) minutos. 12. Terminación de sesiones huérfanas. 13. Restringir sesiones simultáneas de un mismo usuario desde diferentes dispositivos. 14. Almacenar en los LOGs la geo-posición (latitud y longitud) en valores decimales cuando se realice la consulta en dispositivos móviles o cuando lo considere la Registraduría.
Software	Integración software del OAID y el CLIENTE

Descripción	Aspectos a tener en cuenta en la integración del software de OAID y el CLIENTE cuando el datacenter del CLIENTE se encuentre ubicado fuera del territorio colombiano en infraestructura On-premices o infraestructura CLOUD (IaaS, PaaS o SaaS) en regiones o países con adecuados niveles de protección de datos personales e incluidos en la circular de la Superintendencia de Industria y Comercio.
Estado	Obligatorio
Categoría	Desarrollo de software
Detalle	1. Los datos biométricos capturados desde la estación final del cliente mediante el dispositivo biométrico deberán transmitirse directamente desde la estación de captura al datacenter del OAID. 2. El OAID no podrá retornar datos biográficos asociados a NUIP del ciudadano. Solo podrá retornará al cliente la siguiente información: – NUIP – NUT – Resultado el cotejo (Satisfactorio/No Satisfactorio) – Código y/o descripción del estado de vigencia del documento – Fecha y hora del resultado del cotejo

12. REQUERIMIENTO DE MODULOS DE AUTOGESTIÓN O MÓDULOS DESATENDIDOS

Autogestión	Gabinete o caja
Descripción	Unidad donde se incorporan los componentes de hardware (estación de trabajo, dispositivo biométrico, cables, etc) requeridos para el proceso de autenticación biométrico sin la presencia permanente de un operario.
Estado	Obligatorio
Categoría	Hardware/Autogestión
Detalle	1. El gabinete debe tener implementado estándares de seguridad FIPS 140-2 Nivel 3 o superior que incluye protección contra intrusiones en módulos desatendidos que operan en entornos no gestionados. 2. El hardware debe estar asegurado al gabinete. 3. El cableado ni las conexiones deben estar expuestos a los usuarios. 4. El hardware asociado al proceso de autenticación biométrica debe estar aislado de otros componentes que se encuentren dentro del gabinete.

Autogestión	Estación de trabajo
Descripción	Adaptación de la estación de trabajo en el gabinete para módulos de autogestión.
Estado	Obligatorio
Categoría	Hardware/Autogestión
Detalle	Se puede adaptar el siguiente hardware como estación de trabajo: • PC compuesto de monitor, CPU y/o teclado y lector biométrico homologado por la REGISTRADURÍA • Tableta y lector biométrico WIFI homologado por la REGISTRADURÍA • Dispositivo biométrico integrado (Tableta y lector biométrico homologado por la REGISTRADURÍA)
Autogestión	Dispositivo biométrico
Descripción	Adaptación de lector biométrico homologado por la REGISTRADURÍA en el gabinete para módulos de autogestión.
Estado	Obligatorio
Categoría	Hardware/Autogestión
Detalle	Se puede adaptar los dispositivos biométricos homologados por la REGISTRADURÍA (movil integrado o USB - estación fija) que se encuentran publicados en la página web de la REGISTRADURÍA.
Autogestión	Monitoreo.
Descripción	Control centralizado del hardware de módulo de autogestión
Estado	Obligatorio
Categoría	Seguridad/Autogestión
Detalle	Habilitar sistema MDM (Mobile Device Management) licenciado, que permita asegurar, monitorear y administrar el hardware del módulo de autogestión. Debe permitir hacer instalación de aplicaciones de manera remota, localización y rastreo satelital del dispositivo, sincronización de archivos, bloqueo de funciones del dispositivo, borrado remoto, reportes de datos y acceso a dispositivos de manera remota. Se debe habilitar acceso a la REGISTRADURÍA al sistema MDM para monitoreo y administración (desactivación) de equipos La REGISTRADURÍA solicitará los usuarios que considere

necesarios en esta herramienta, para ejercer las labores de monitoreo y control.

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

EN BLANCO EN BLANCO

EN BLANCO EN BLANCO EN BLANCO

13. REQUERIMIENTOS DE SEGURIDAD EN DISPOSITIVOS MÓVILES

Móviles Requisitos imprescindibles

Descripción Requerimientos de seguridad que se deben tener en cuenta en dispositivos móviles

Estado Obligatorio

Categoría Dispositivos móviles

Detalle

1. Los dispositivos móviles asignados para el proceso de autenticación biométrica utilizados deben ser de propiedad del CLIENTE, del OAID o en comodato.
2. Los dispositivos móviles deben ser asignados exclusivamente para el proyecto. La incorporación de funcionalidades adicionales sobre estos dispositivos debe ser verificadas y avaladas por la REGISTRADURÍA.
3. El CLIENTE debe tener documentada, implementada y socializada las políticas de seguridad para dispositivos móviles.
4. El CLIENTE debe establecer un procedimiento de registro, bloqueo o desbloqueo de los dispositivos móviles de forma remota. Estas acciones deben tener un gestor centralizado.
5. La solución tecnológica debe garantizar que en ninguna de las etapas del proceso se pueda compilar (acopiar), sustraer, interceptar, modificar, recolectar, almacenar, replicar o complementar bases de datos a partir de la información biométrica obtenida de manera directa o indirecta en cualquier parte del proceso.
6. Se debe garantizar que la transacción que incorpora información biográfica y biométrica tiene un tiempo de vida útil no superior a un (1) minuto. Expirado el tiempo de vida útil se deberá garantizar la eliminación de la información recopilada.
7. Los lectores biométricos utilizados en el proceso deben estar homologados por la REGISTRADURÍA.
8. Los dispositivos móviles utilizados para el proceso de autenticación biométrica deben estar homologados por la REGISTRADURÍA
9. El CLIENTE debe presentar documento de análisis y acciones de mitigación de riesgos para la implementación de dispositivos móviles para el proceso de autenticación biométrica, documento que será evaluado por la REGISTRADURÍA.

Móviles Restricciones

Descripción Configuraciones no autorizadas en dispositivos móviles.

Estado Obligatorio

Categoría Dispositivos móviles

Detalle Teniendo en cuenta que los dispositivos móviles empleados para el proceso de autenticación biométrica contra la base de datos dispuesta por la REGISTRADURÍA serán utilizados en sitios diferentes a las sedes de atención fijas, se prohíbe en dichos dispositivos:

1. Configuración y/o acceso a redes inalámbricas WI-FI públicas.
2. Configuración y/o acceso a redes inalámbricas WI-FI que no cuente con cifrado de seguridad WPA o superior.
3. Configuración de dispositivos adicionales no autorizados a través de cualquier tipo de conexión.
4. Conexión mediante redes inalámbricas de área personal o WPAN (Wireless Personal Área Network) o tecnología Bluetooth (estándar IEEE 802.15).
5. Configuración y acceso a dispositivos Bluetooth.
6. Configurar la funcionalidad NFC.
7. Instalación de software no autorizado por REGISTRADURÍA.
8. Lectura de geolocalización por software.
9. Conexión del dispositivo biométrico a la estación biométrica mediante cable, bluetooth, NFC, entre otras

Móviles Conexiones Permitidas

Descripción Medios de conexión para acceder al proceso de autenticación biométrica.

Estado Obligatorio

Categoría Dispositivos móviles

Detalle

1. Redes de Datos
   Para el proceso de autenticación biométrica mediante dispositivos móviles, se permiten los siguientes medios de conexión a redes de datos:
   - Telefonía Móvil 3G
   - Telefonía Móvil 4G o superior
   - WI-FI

2. Dispositivo lector de huella biométrico. Se permiten las siguientes conexiones:

   - Conexión mediante tecnología 2G o GPRS, 3G, 4G o superior.
   - Conexión mediante tecnología WIFI. Estos dispositivos deberán entregarse configurados por el fabricante para conectarse a la MAC Address del dispositivo móvil donde ser realiza la validación del APLICANTE.

Se deberán implementar mecanismos de seguridad para garantizar un transporte de datos seguros, mediante el cifrado del canal.

Móviles Infraestructura

Descripción Aspectos a tener en cuenta en la infraestructura

Estado Obligatorio

Categoría Dispositivos móviles

Detalle
1. Para conexiones móviles con tecnología 3G, 4G o superior es necesario configurar una red APN restringida. De acuerdo a la criticidad del sector, la REGISTRADURÍA evaluará el reemplazo de la APN por otros medios que garanticen la seguridad en la transmisión.
2. Conexión vía VPN, TLS con certificados digitales válidos, cifrando la sesión y el transporte de datos entre el dispositivo y el servidor.
3. La infraestructura de control que permite el acceso a los dispositivos móviles puede estar instalada en el data center dispuesto para el proceso de autenticación biométrica o en el datacenter del CLIENTE, previa autorización de la REGISTRADURÍA.
4. La red que permite el acceso a los dispositivos móviles debe estar segmentada con relación a la infraestructura del OAID.

Móviles Seguridad

Descripción Aspectos a tener en cuenta en la seguridad del dispositivo

Estado Obligatorio

Categoría Dispositivos móviles

Detalle
1. Se debe implementar cifrado de disco completo y de particiones del dispositivo móvil (FDE - Full Disk Encryption)
2. Se debe utilizar FIPS 140-2 Nivel 2 o superior
3. Configurar contraseñas fuertes y de dos o más factores de autenticación.
4. Bloqueo del dispositivo por intentos fallidos al sistema operativo o al software. Se debe establecer el procedimiento de desbloqueo a nivel centralizado.
5. Deberá existir un procedimiento para administración de cuentas de usuarios para establecer fecha de vencimiento de credenciales y periodos de inactividad.
6. Instalar software antivirus, antispam, antimalware y firewall licenciado.
7. Reconectar a VPN después de 5 minutos de inactividad.
8. Activar la geolocalización del dispositivo. No se permite

desactiva la geolocalización.

9. Para dispositivos móviles con sistema operativo Android, la versión mínima autorizada es dos versiones anteriores a la versión vigente. Se debe garantizar la actualización permanente de versión de acuerdo a este requerimiento. Para versiones inferiores, la REGISTRADURÍA evaluará los cumplimientos mínimos de seguridad.
10. Para dispositivos móviles con sistema operativo Windows, la versión mínima autorizada es Windows 10.
11. Para dispositivos móviles con sistema operativo iOS, la versión mínima autorizada es dos versiones anteriores a la versión vigente. Se debe garantizar la actualización permanente de versión de acuerdo a este requerimiento. Para versiones inferiores, la REGISTRADURÍA evaluará los cumplimientos mínimos de seguridad.
12. Para otros sistemas operativos, la versión será evaluada por la REGISTRADURÍA.

Móviles	Geolocalización
Descripción	Configuración del método de localización o ubicación en el dispositivo móvil
Estado	Obligatorio
Categoría	Dispositivos móviles
Detalle	Habilitar el uso de la ubicación del dispositivo móvil a través de la configuración del método o modo de ubicación en GPS, AGPS o precisión alta

Móviles	Monitoreo.
Descripción	Control centralizado del dispositivo móvil
Estado	Obligatorio
Categoría	Seguridad/Móviles
Detalle	Habilitar sistema MDM (Mobile Device Management) licenciado, que permita asegurar, monitorear y administrar el dispositivo móvil. Debe permitir hacer instalación de aplicaciones de manera remota, localización y rastreo satelital del dispositivo, sincronización de archivos, bloqueo de funciones del dispositivo, borrado remoto, reportes de datos y acceso a dispositivos de manera remota. Se debe habilitar acceso a la REGISTRADURÍA al sistema MDM para monitoreo y administración (desactivación) de equipos La REGISTRADURÍA solicitará los usuarios que considere

necesarios en esta herramienta, para ejercer las labores de monitoreo y control.

Los OPERADORES que se encuentren en producción antes de la expedición de este anexo técnico, deberán remitir la relación de hardware y el soporte de licenciamiento con el cual continuarán prestando el servicio de autenticación biométrica dactilar, treinta (30) días después de la expedición de este documento.

El presente anexo técnico No 2, versión 1.0, reemplaza de forma integral el anexo técnico No. 2 la versión 2.0 de la resolución 5633 de 2016, el cual queda sin efectos a partir de la fecha.

Aprobado por:

ALEXANDER VEGA ROCHA
Registrador Nacional del Estado Civil

DIDIER ALBERTO CHILITO VELASCO
Registrador Delegado para el Registro Civil e Identificación

Versión Proyectada por:
Ing. Efrain Antonio Piñeros
Ing. Mario Diaz Carrasco
Versión Revisada por:
Ing. Javier Antonio Sánchez Roldán

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DIRECCIÓN LOGÍSTICA Y FINANCIERA
GRUPO CENTRAL DE CUENTAS

GS – 2026 – **/ DILOF – GUCUE – 29.25**

Bogotá D.C., 05 ENE 2026

Señores
DUEÑOS DE LA NECESIDAD Y ESTRUCTURADORES ESTUDIOS PREVIOS DILOF
Carrera 59 26- 21 CAN
Bogotá D.C.

Asunto: aspectos a tener en cuenta en la elaboración de los estudios previos vigencia 2026

En atención a la nota 1 del numeral 1 ETAPA DE PLANEACIÓN del capítulo III ETAPAS DEL PROCESO DE CONTRATACIÓN de la Resolución Nro. 03049 de 2014 *"por la cual se adopta el Manual de Contratación de la Policía Nacional"*, de manera atenta me permito presentar el listado del tratamiento del IVA de acuerdo con el Estatuto Tributario, haciéndose necesario precisar los alcances del procedimiento fiscal de los productos clasificados como exentos, excluidos y grabados por dicho tributo.

1. Productos Exentos de IVA

Son aquellos que, conforme al artículo 477 del E.T., no están sujetos al cobro del IVA, pero, aun así, su venta y/o comercialización puede estar sujeta a ciertas condiciones para efectos fiscales; los principales productos exentos para la Policía Nacional incluyen:

"(…) 3. Las municiones y material de guerra o reservado y por consiguiente de uso privativo y los siguientes elementos pertenecientes a las Fuerzas Militares y la Policía Nacional:

a) Sistemas de armas y armamento mayor y menor de todos los tipos, modelos y calibres con sus accesorios repuestos y los elementos necesarios para la instrucción de tiro, operación, manejo y mantenimiento de los mismos.
b) Todo tipo de naves, artefactos navales y aeronaves destinadas al servicio del Ramo de Defensa Nacional, con sus accesorios, repuestos y demás elementos necesarios para su operabilidad y funcionamiento.
c) Municiones, torpedos y minas de todos los tipos, clases y calibres para los sistemas de armas y el armamento mayor y menor que usan las Fuerzas Militares y la Policía Nacional.
d) Material blindado
e) Semovientes de todas las clases y razas destinadas al mantenimiento del orden público, interior o externo.
f) Materiales explosivos y pirotécnicos, materias primas para su fabricación y accesorios para su empleo.
g) Paracaídas y equipos de salto para Unidades Aerotransportadas, incluidos los necesarios para su mantenimiento.
h) Elementos, equipos y accesorios contra motines.
i) Los equipos de ingenieros de combate con sus accesorios y repuestos.
j) Equipos de buceo y de voladuras submarinas, sus repuestos y accesorios.
k) Equipos de detección aérea, de superficie y submarina sus accesorios, repuestos, equipos de sintonía y calibración.

l) Elementos para control de incendios y de averías, sus accesorios y repuestos.
m) Herramientas y equipos para pruebas y mantenimiento del material de guerra o reservado.
n) Equipos, software y demás implementos de sistemas y comunicaciones para uso de las Fuerzas Militares y la Policía Nacional.
o) Otros elementos aplicables al servicio y fabricación del material de guerra o reservado.
p) Los servicios de diseño, construcción y mantenimiento de armas, municiones y material de guerra, con destino a la fuerza pública, así como la capacitación de tripulaciones de las Fuerza Pública, prestados por las entidades descentralizadas del orden nacional de sector defensa.

PARÁGRAFO 1. No se consideran armas y municiones destinadas a la defensa nacional los uniformes, prendas de vestir, textiles, material térmico, carpas, sintelitas, menaje, cubertería, marmitas, morrales, chalecos, juegos de cama, toallas, ponchos y calzado de uso privativo de las Fuerzas Militares y de Policía Nacional. (...)"

2. Productos Excluidos de IVA

Son aquellos que no están sujetos al cobro del IVA, pero no se permite recuperarlo sobre las compras o insumos relacionados; es decir que, aunque no se paga el impuesto al vender estos productos, el vendedor no puede descontarlo de lo que haya pagado por sus adquisiciones.

De acuerdo al artículo 476 del E.T., se incluyen servicios médicos, algunos tipos de bienes raíces y ciertos productos de consumo básico que no cumplen con las condiciones para ser exentos; los principales bienes o servicios excluidos para la Policía Nacional son:

"(...) 9. El servicio de transporte público, terrestre, fluvial y marítimo de personas en el territorio nacional, y el de transporte público o privado nacional e internacional de carga marítimo, fluvial, terrestre y aéreo. Igualmente, se excluye el transporte de gas e hidrocarburos.

10. El transporte aéreo nacional de pasajeros con destino o procedencia de rutas nacionales donde no exista transporte terrestre organizado. Esta exclusión también aplica para el transporte aéreo turístico con destino o procedencia al departamento de La Guajira y los municipios de Nuquí, en el Departamento de Chocó, Mompox en el Departamento de Bolívar, Tolú, en el Departamento de Sucre, Miraflores en el Departamento del Guaviare y Puerto Carreño en el departamento del Vichada.

14. Los servicios de alimentación, contratados con recursos públicos, destinados al sistema penitenciario, de asistencia social, de escuelas de educación pública, a las Fuerzas Militares, Policía Nacional, Centro de Desarrollo Infantil, centros geriátricos públicos, hospitales públicos, comedores comunitarios.

20. Adquisición de licencias de software para el desarrollo comercial de contenidos digitales, de acuerdo con la reglamentación expedida por el Ministerio de Tecnologías de la Información y Comunicaciones.

21. Suministro de páginas web, servidores (hosting), computación en la nube (cloud computing).

30. Los servicios de reparación y mantenimiento de naves y artefactos navales tanto marítimos como fluviales de bandera colombiana, excepto los servicios que se encuentran en el literal P) del numeral 3 del artículo 477 de este Estatuto. (...)"

3. Productos Grabados con IVA

Son aquellos que sí están sujetos al cobro de este impuesto sobre su venta y/o comercialización, de acuerdo al artículo 468 del Estatuto Tributario, estos productos deben incluir el IVA en su precio de venta, la obligación de recaudarlo y el pago recae sobre el vendedor o proveedor de bienes y servicios.

Los productos grabados tienen una tarifa general del 19%, salvo algunas excepciones en las cuales pueden aplicarse tarifas diferenciales del (5%), conforme al artículo 468-1.

"(...) ***Nota 1.*** *Los siguientes bienes están gravados con la tarifa del cinco por ciento (5%):*

09.01	Café, incluso tostado o descafeinado; cáscara y cascarilla de café, sucedáneos del café que contengan café en cualquier proporción, excepto el de la subpartida 09.01.11
10.01	Trigo y morcajo (tranquillón), excepto el utilizado para la siembra.
10.02.90.00.00	Centeno.
10.04.90.00.00	Avena.
10.05.90	Maíz para uso industrial.
10.06	Arroz para uso industrial.
10.07.90.00.00	Sorgo de grano.
10.08	Alforfón, mijo y alpiste, los demás cereales.
11.01.00.00.00	Harina de trigo o de morcajo (tranquillón)
11.02	Harina de cereales, excepto de trigo o de morcajo (tranquillón)
11.04.12.00.00	Granos aplastados o en copos de avena
12.01.90.00.00	Habas de soya.
12.07.10.90.00	Nuez y almendra de palma.
12.07.29.00.00	Semillas de algodón.
12.07.99.99.00	Fruto de palma de aceite
12.08	Harina de semillas o de frutos oleaginosos, excepto la harina de mostaza.
15.07.10.00.00	Aceite en bruto de soya
15.11.10.00.00	Aceite en bruto de palma
15.12.11.10.00	Aceite en bruto de girasol
15.12.21.00.00	Aceite en bruto de algodón
15.13.21.10.00	Aceite en bruto de almendra de palma
15.14.11.00.00	Aceite en bruto de colza
15.15.21.00.00	Aceite en bruto de maíz
16.01	Únicamente el salchichón y la butifarra
16.02	Únicamente la mortadela
17.01	Azúcar de caña o de remolacha y sacarosa químicamente pura, en estado sólido, excepto la de la subpartida 17.01.13.00.00
17.03	Melaza procedente de la extracción o del refinado de la azúcar.
18.06.32.00.90	Chocolate de mesa.
19.02.11.00.00	Pastas alimenticias sin cocer, rellenar ni preparar de otra forma que contengan huevo.
19.02.19.00.00	Las demás pastas alimenticias sin cocer, rellenar, ni preparar de otra forma.
19.05	Los productos de panadería a base de sagú, yuca y achira.
21.01.11.00	Extractos, esencias y concentrados de café.
21.06.90.69.00	Preparaciones edulcorantes a base de sustancias sintéticas o artificiales.
21.06.90.61.00	Preparaciones edulcorantes a base de estevia y otros de origen natural.
23.01	Harina, polvo y pellets, de carne, despojos, pescados o de crustáceos, moluscos o demás invertebrados acuáticos, impropios para la alimentación humana, chicharrones.

23.02	Salvados, moyuelos y demás residuos del cernido, de la molienda o de otros tratamientos de los cereales o de las leguminosas incluso en pellets.
23.03	Residuos de la industria del almidón y residuos similares, pulpa de remolacha, bagazo de caña de azúcar y demás desperdicios de la industria azucarera, heces y desperdicios de cervecería o de destilería, incluso en «pellets».
23.04	Tortas y demás residuos sólidos de la extracción del aceite desoja (soya), incluso molidos o en «pellets».
23.05	Tortas y demás residuos sólidos de la extracción del aceite de maní cacahuete, cacahuate), incluso molidos o en «pellets».
23.06	Tortas y demás residuos sólidos de la extracción de grasas o aceites vegetales, incluso molidos o en «pellets», excepto los de las partidas 23.04 o 23.05.
23.08	Materias vegetales y desperdicios vegetales, residuos y subproductos vegetales, incluso en «pellets», de los tipos utilizados para la alimentación de los animales, no expresados ni comprendidos en otra parte.
23.09	Preparaciones de los tipos utilizados para la alimentación de los animales.
44.03	Madera en bruto, incluso descortezada. desalburada o escuadrada.
52.01	Algodón sin cardar ni peinar
73.11.00.10.00	Recipientes para gas comprimido o licuado, de fundición, hierro o acero, sin soldadura, componentes del plan de gas vehicular.
82.01	Layas, palas, azadas, picos, binaderas, horcas de labranza, rastrillos y raederas, hachas, hocinos y herramientas similares con filo, tijeras de podar de cualquier tipo, hoces y guadañas, cuchillos para heno o para paja, cizallas para setos, cuñas y demás.
82.08.40.00.00	Cuchillas y hojas cortantes para máquinas agrícolas, hortícolas o forestales.
84.09.91.60.00	Carburadores y sus partes (repuestos) componentes del plan de gas vehicular.
84.09.91.91.00	Equipo para la conversión del sistema de alimentación de combustible para vehículos automóviles a uso dual (gas/gasolina) componentes del plan de gas vehicular.
84.09.91.99.00	Repuestos para kits del plan de gas vehicular.
84.14.80.22.00	Compresores componentes del plan de gas vehicular.
84.14.90.10.00	Partes de compresores (repuestos) componentes del plan de gas vehicular.
84.19.31.00.00	Secadores para productos agrícolas
84.19.50.10.00	Intercambiadores de calor; pasteurizadoras
84.24.82.90.00	Fumigadoras para uso agrícola
84.29.51.00.00	Cargador frontal
84.32	Máquinas, aparatos y artefactos agrícolas, hortícolas o silvícolas, para la preparación o el trabajo del suelo o para el cultivo.
84.34	Únicamente máquinas de ordeñar y sus partes.
84.36.21.00.00	Incubadoras y criadoras.
84.36.29	Las demás máquinas y aparatos para la avicultura.
84.36.91.00.00	Partes de máquinas o aparatos para la avicultura.
84.38.80.10.00	Descascarilladoras y despulpadoras de café
85.01	Motores y generadores eléctricos para uso en vehículos eléctricos, híbridos e híbridos enchufables, motocicletas eléctricas y bicicletas eléctricas.
85.07	Acumuladores eléctricos, incluidos sus separadores, aunque sean cuadrados o rectangulares para uso en vehículos eléctricos, híbridos e híbridos enchufables, motocicletas eléctricas y bicicletas eléctricas.
85.04	Cargadores de baterías de vehículos eléctricos, híbridos e híbridos enchufables, motocicletas eléctricas y bicicletas eléctricas incluso aquéllos que vienen incluidos en los vehículos, los de carga rápida (electrolineras) y los de recarga domiciliaria.
85.04	Inversores de carga eléctrica para uso en vehículos eléctricos, híbridos e híbridos enchufables.
87.02	Vehículos automóviles eléctricos, para transporte de 10 o más personas, incluido el conductor, únicamente para transporte público.
87.03	Los taxis automóviles eléctricos, únicamente para transporte público.

87.04	Vehículos automóviles eléctricos, híbridos e híbridos enchufables para el transporte de mercancías.
87.05	Vehículos automóviles eléctricos, híbridos e híbridos enchufables para usos especiales excepto los concebidos principalmente para el transporte de personas o mercancías.
87.06	Chasis de vehículos automotores eléctricos de las partidas 87.02 y 87.03, únicamente para los de transporte público.
87.07	Carrocerías de vehículos automotores eléctricos de las partidas 87.02 y 87.03, incluidas las cabinas, únicamente para los de transporte público.
87.11	Motocicletas eléctricas (incluidos los ciclomotores) cuyo valor exceda de 50 UVT.
87.12	Bicicletas y Bicicletas eléctricas (incluidos los triciclos de reparto) cuyo valor exceda de 50 UVT.
89.01	Transbordadores, cargueros, gabarras (barcazas) y barcos similares para transporte de personas o mercancías.
89.04	Remolcadores y barcos empujadores.
89.06.90	Los demás barcos y barcos de salvamento excepto los de remo y los de guerra.
90.25.90.00.00	Partes y accesorios surtidores (repuestos), componentes del plan de gas vehicular.
90.31	Unidades de control para motores eléctricos de uso en vehículos eléctricos, híbridos e híbridos enchufables.
90.32	Unidades de control de las baterías y del sistema de enfriamiento de las baterías para uso en vehículos eléctricos, híbridos e híbridos enchufables.
96.19	Compresas y tampones higiénicos.

Por lo anterior, si los productos no se encuentran en la clasificación de exentos ni excluidos, estarán grabados con el impuesto, asimismo, en los casos donde surjan dudas respecto al impuesto al valor agregado IVA para bienes o servicios que no se hayan contratado en vigencias anteriores, o la interpretación de la norma no sea clara, como lo establece la Resolución Nro.03049 de 2014, el Área Financiera de esta Dirección brindará la respectiva asesoría.

Atentamente,

Coronel **WILSON GILBERTO BARRIOS PERDOMO**
Director Logístico y Financiero (E)
Administrador Policial TP 3380

Elaboró: TE. WINNY SUSTAMANTE CÓRDOBA
DILOF - GUCUE

Revisó: MY. DORA JAQUELYN ESTUPIÑAN MARTINEZ
DILOF - GUCUE

Revisó: MY. RUBIA SMITH JIMENEZ DIAZ
DILOF – ARFIN (E)

Fecha elaboración: 04/01/2026
Ubicación L:\1. GUGED - 2026\ Comunicaciones oficiales 2026

Carrera 59 No. 26-21 CAN, Bogotá
Teléfonos 5159000 Ext 9809
diraf.arfin-gucue1@policia.gov.co
www.policia.gov.co

INFORMACIÓN PÚBLICA

GS-2026-007251-OFTIC

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
OFICINA TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
GRUPO DES OPERA TECNO DE INFOR Y COMUNICACIONES

CEA.3.0-07
16-ECD-003

SUTIC-GUDES - 20.1

Bogotá D.C., 30 de julio de 2026

Señor teniente coronel
CESAR AUGUSTO SÁNCHEZ SALINAS
Jefe Oficina de Tecnologías de la Información y las Comunicaciones (E)
Carrera 59 No 26 - 21 CAN
Bogotá D.C.

Asunto: solicitud comité de evaluación de requerimientos tecnológicos (CERT).

De manera atenta y respetuosa me dirijo a mi coronel, con el fin de solicitar la autorización para la presentación en Comité de Evaluación de Requerimientos Tecnológicos (CERT), el proyecto de "FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.", con el fin de emitir concepto de viabilidad por parte de este comité.

Atentamente,

...

FIRMA DIGITAL

Firmado digitalmente por:
Nombre: Luis Fernando Romero Roa
Grado: Mayor
Cargo: Subjefe Tecnologias De La Informacion Y Las Comunicaciones
Cédula: 7185190
Dependencia: Grupo Des Opera Tecno De Infor Y Comunicaciones
Unidad: Oficina Tecnologias De La Informacion Y Las Comunicaciones
Correo: luis.romero1084@correo.policia.gov.co
30/07/2026 6:24:35 p. m.

Anexo: si

Carrera 59 No 26 - 21 CAN
Teléfono: 5159437
oftic.gudes@policia.gov.co
www.policia.gov.co

INFORMACIÓN PÚBLICA

GS-2026-007279-OFTIC

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
OFICINA TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
GRUPO DES OPERA TECNO DE INFOR Y COMUNICACIONES

CEA.3.0-07
16-ECD-003

SUTIC-GUDES - 20.1

Bogotá D.C., 31 de julio de 2026

Señor teniente coronel
WILLIAM GABRIEL DÍAZ CIFUENTES
Jefe Área Contratación
Carrera 59 26-21 CAN
Bogotá D.C.

Asunto: solicitud concepto ambiental proceso contractual

Respetuosamente me permito solicitar a mi coronel, tenga a bien ordenar a quien corresponda se emita concepto ambiental para el proceso cuyo objeto es *"FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE LA SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL"*, para lo cual me permito anexar especificaciones técnicas objeto del contrato.

Lo anterior con el fin de presentar mencionado proceso ante el Grupo de Contratos de la Dirección Logística y Financiera.

Atentamente,

...

FIRMA DIGITAL

Firmado digitalmente por:
Nombre: Luis Fernando Romero Roa
Grado: Mayor
Cargo: Subjefe Tecnologias De La Informacion Y Las Comunicaciones
Cédula: 7185190
Dependencia: Grupo Des Opera Tecno De Infor Y Comunicaciones
Unidad: Oficina Tecnologias De La Informacion Y Las Comunicaciones
Correo: luis.romero1084@correo.policia.gov.co
31/07/2026 3:05:58 p. m.

Anexo: si

Carrera 59 No 26 - 21 CAN
Teléfono: 5159437
oftic.gudes@policia.gov.co
www.policia.gov.co

INFORMACIÓN PÚBLICA

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DIRECCION LOGISTICA Y FINANCIERA
AREA CONTRATACION

CEA.3.0-07
16-ECD-003

SULOF-ARCON - 3.1

Bogotá D.C., 04 de agosto de 2026

Señor mayor
LUIS FERNANO ROMERO ROA
Subjefe tecnologías de la información y las comunicaciones
Carrera 59 Nro. 26-21 CAN
Bogotá D, C.

Asunto: concepto ambiental y de seguridad y salud en el trabajo para el fortalecimiento de la infraestructura de datos mediante la implementación de la solución shareplex, para la optimización y migración de las bases de datos de la registraduría nacional del estado civil

En atención a la solicitud oficial **GS-2026-007279-OFTIC**, mediante el cual se solicita el concepto ambiental y de seguridad y salud en el trabajo para el objeto **"FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE LA SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL. "**, que deberá ser incluido en el proceso de contratación, en atención a que *"Se debe dar cumplimiento a las obligaciones y requerimientos mínimos, conforme a la Resolución No. 03049 del 30/07/2014 "Por la cual se adopta el Manual de Contratación de la Policía Nacional" y a la Resolución No. 00090 del 15/01/2018 "Por la cual se actualiza, modifica y complementa el Manual de Contratación de la Policía Nacional, adoptado mediante Resolución 03049 de 2014", según aplique; se recomienda lo siguiente:*

REQUISITOS AMBIENTALES
ESPECIFICACIONES TECNICAS:

- La Policia Nacional consultará el Registro Único de Infractores Ambientales (RUIA), expedido a través del enlace oficial del Ministerio de Ambiente:https://vital.minambiente.gov.co/SILPA_UT_PRE/RUIA/ConsultarSancion.aspx?Ubic=ext.,; En caso de presentarse como unión temporal o consorcio, se realizara con cada uno de sus integrantes, con el fin de verificar que no tengan sanciones ambientales que puedan afectar la correcta ejecución del proceso.

OBLIGACIONES DEL CONTRATISTA:

- El contratista deberá garantizar que toda la información y documentación entregada a la Policía Nacional que se realicen en formato digital, utilizando medios reutilizables, y ajustándose a los lineamientos de la Directiva Presidencial 04 de 2012 sobre eficiencia administrativa y la Política de Cero Papel en la Administración Pública, (Aplica cuando el contrato contemple la presentación de informes o documentación extensa).En Caso de ser necesaria a la entrega de archivos físicos en papel garantizar su buen uso.

SEGURIDAD Y SALUD EN EL TRABAJO
EN LAS ESPECIFICACIONES TÉCNICAS:

- El contratista deberá acreditar el cumplimiento de los Estándares Mínimos del Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST), conforme a lo establecido en el Decreto 1072 de 2015 y la Resolución 0312 de 2019 del Ministerio del Trabajo. Para tal efecto, deberá presentar la **calificación oficial de los Estándares Mínimos correspondiente al cierre del año inmediatamente anterior**, la cual podrá ser acreditada mediante cualquiera de las siguientes alternativas, ambas válidas conforme a la normativa vigente y a la Circular 027 de 2026:

- ✓ Calificación de la autoevaluación de los estándares mínimos radicada ante la Administradora de Riesgos Laborales (ARL), o
- ✓ Calificación de la autoevaluación de los estándares mínimos radicada ante el Ministerio del Trabajo. (plazo establecido hasta el 31 de Julio, de acuerdo a la circular 027 de 2026)

Este requisito deberá entregarlo al supervisor del contrato y dichos soportes serán anexados al informe de supervisión correspondiente y posteriormente cargados en la plataforma SECOP II como evidencia del cumplimiento de las obligaciones ambientales contractuales.

Nota:

- ✓ Los proponentes extranjeros que no tengan sucursal en Colombia estarán exceptuados de la obligación de presentar esta información, debe declararlo bajo una declaración juramentada indicando esta condición y entregar al supervisor del contrato en cumplimiento de este criterio.
- ✓ Para personas naturales sin personal a cargo, no será exigible este requisito, debe declararlo bajo una declaración juramentada indicando esta condición y entregar al supervisor del contrato en cumplimiento de este criterio.

Atentamente,

FIRMA DIGITAL

Firmado digitalmente por:
Nombre: Jeimmy Johana Herrera Medina
Grado: Contrato Por Prestacion De Servicios-04
Cargo: Contrato Por Prestacion De Servicios-04
Cédula: 1032482327
Dependencia: Area Contratacion
Unidad: Direccion Logistica Y Financiera
Correo: jeimmyj.herrera@correo.policia.gov.co
4/08/2026 3:17:07 p. m.

Anexo: no

Carrera 59 26-21 CAN
Teléfono: 5159000
diraf.guged@policia.gov.co
www.policia.gov.co

INFORMACIÓN PÚBLICA

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
OFICINA TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
GRUPO ARQUITECTURA TECNOLOGICA

CEA.3.0-07
16-ECD-003

Fecha:	Bogotá D.C., 06 de agosto de 2026		
Hora de inicio:	14:30 horas	**Hora de finalización:**	17:30 horas
Lugar:	Oficina de Tecnologías de la Información y las Comunicaciones videoconferencia vía Teams.		

ACTA - 002344 - SUTIC-GARTE - 2.7

QUE TRATA DE LA SUSTENTACIÓN DE LAS ESPECIFICACIONES TÉCNICAS QUE CONFORMAN EL PROYECTO FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL - OFTIC - GUDES

ORDEN DEL DÍA

1. Verificación de asistentes
2. Lectura del acta anterior
3. Verificación de los compromisos
4. Temas a tratar
   4.1. Normatividad
   4.2. Información y sustentación del proyecto
   4.3. Recomendaciones, sugerencias y observaciones realizadas en GEPOL y en Comité CERT
   4.4. Decisión del Comité CERT
   4.5. Ficha técnica aprobada

DESARROLLO

1. Verificación de asistentes

Conforme a lo dispuesto en la Resolución Nro. 01990 del 24/07/2026 "*Por la cual se reglamenta la conformación y funcionamiento del Comité Evaluador de Requerimientos Tecnológico de la Policía Nacional*", y procedimiento 1DT-PR-0019 del 27/04/2026, denominado "*Evaluación de Tecnologías de la Información y las Comunicaciones - TIC*", se procede a verificar la asistencia de los funcionarios que hacen parte del Comité Evaluador de Requerimientos Tecnológicos CERT – OFTIC e invitados.

Mediante Orden del día No. 01 del 01 de enero de 2026, se realiza el nombramiento de los integrantes del Comité Evaluador de Requerimientos Tecnológicos CERT.

Por lo anterior, se confirma la asistencia a la presente reunión del siguiente personal:

INTEGRANTES COMITÉ EVALUADOR DE REQUERIMIENTOS TÉCNICOS – CERT				
No.	**GR**	**NOMBRES Y APELLIDOS**	**CARGO**	**UNIDAD**
1	MY	Luis Fernando Romero Roa	Jefe GUDES	GUDES – OFTIC
2	MY	Julio Cesar Jiménez Fandiño	Jefe GARTE	GARTE – OFTIC
3	MY	John Darío Restrepo Correa	Jefe GUSIN	GUSIN – OFTIC
4	MY	Claudia Yaneth Rodríguez Puentes	Jefe GUSOF	GUSOF – OFTIC
5	MY	Edwin Javier Ramírez Gil	Jefe GUSAP	GUSAP-OFTIC
6	MY	Jhon Alexander Mendez Mendoza	Jefe CSIRT	CSIRT – OFTIC
7	CT	Rigoberto Muñoz Restrepo	Jefe GUPES	GUPES – OFTIC
8	ST	Luis Alfonso Barrera Moreno	Jefe GUTEC (E)	GUTEC – OFTIC

9	ST	Paula Carolina Orosco Buitrago	Integrante GURAD	GURAD – OFTIC
10	ST	Asdrubal Andrés Vélez Vélez	Jefe GUDAS (E)	GUDAS – OFTIC
11	IJ	José Luis Bello Zapata	Integrante GRUMA	GRUMA - OFTIC
12	IT	Jennifer Paola Herran Romero	Responsable Planeación	GUSAP – OFTIC
INVITADOS				
13	IJ	Nelson Enrique Reyes Rincón	Secretario Comité CERT	OFTIC – GARTE

2. Lectura del acta anterior

No aplica

3. Verificación de los compromisos

No aplica

4. Temas a tratar

4.1 Normatividad

4.4.1. Resolución No. 05884 del 27 de diciembre 2019 "Por la cual se expide el Manual para la Administración de los Recursos Logísticos de la Policía Nacional de Colombia",

(...) Capítulo 8. Subcomponente Tecnologías de la Información y las Comunicaciones

El presente capítulo tiene como finalidad describir los principales aspectos a tener en cuenta en la adquisición, implementación y administración de las Tecnologías de las Información y las Comunicaciones en la Policía Nacional; de igual forma, generar directrices para su mantenimiento, conservación y una adecuada gestión integral de los Residuos de Aparatos Eléctricos y Electrónicos (RAEEs), acciones que deberán seguir las unidades de Policía, con la finalidad de prevenir y/o minimizar impactos que puedan ocasionar daños de la plataforma tecnológica institucional y garantizar la sostenibilidad de los recurso.

8.6. Parámetros para la adquisición de tecnologías de la información y las comunicaciones en la Policía Nacional

- *La adquisición de Tecnologías de la Información y las Comunicaciones mediante los planes anuales de adquisiciones, convenios, comodatos, sesiones, donaciones, Planes Integrales de Seguridad y Convivencia Ciudadana (PISCC), Fondo Nacional de Seguridad y Convivencia Ciudadana (FONSECON), Fondos de Seguridad Territorial (FONSET), así como a través de instituciones gubernamentales y privadas en las unidades policiales en el ámbito nacional, deberá contar con la viabilidad técnica de la Oficina de Telemática.*
- *El concepto de viabilidad será elaborado y expedido por el Comité de Evaluación de Requerimientos Tecnológicos (CERT), que se encuentra conformado por funcionarios de los diferentes grupos que integran la Oficina de Telemática, para lo cual se tendrá en cuenta el lleno de los requisitos establecidos por esta instancia. (...)*

4.4.2. 1DT-PR-0019 "Evaluación de Tecnologías de la Información y las Comunicaciones".

(...) ***Convocar Comité Evaluador de Requerimientos Tecnológicos (CERT):***
Se activa cuando la necesidad requiere un análisis integral y colegiado por la complejidad o el impacto del requerimiento. Está compuesto por profesionales de diversas disciplinas, lo que permite emitir conceptos más integrales, identificar riesgos técnicos o de usabilidad, y garantizar mayor legitimidad y transparencia en el proceso de evaluación. Esta modalidad promueve la participación, el consenso y decisiones menos susceptibles a conflictos de interés. (...)

4.4.3. Resolución Nro. 01990 del 24/07/2026 "Por la cual se reglamenta la conformación y funcionamiento del Comité Evaluador de Requerimientos Tecnológico de la Policía Nacional".

(...) ***ARTÍCULO 6. SESIONES DEL COMITÉ.*** *El Comité Evaluador de Requerimientos Tecnológicos de la Policía Nacional (CERT), sesionará de forma ordinaria dos veces por semana, siempre y cuando existan*

solicitudes que deban ser objeto de evaluación; y de forma extraordinaria cuando existan temas de carácter especial que lo ameriten, previa autorización del Subjefe de la Oficina de Tecnologías de la Información y las Comunicaciones y por convocatoria de la secretaría técnica. (...)

4.2 Información y sustentación del Proyecto.

El Grupo Despliegue y Operaciones de Tecnologías de la Información y las Comunicaciones GUDES - OFTIC, mediante comunicación oficial No. GS-2026-007413-OFTIC del 04/08/2026, solicita convocar sesión del Comité Evaluador de Requerimientos Tecnológicos – CERT, así:

UNIDAD: Grupo Despliegue y Operaciones de Tecnologías de la Información y las Comunicaciones GUDES - OFTIC.

Proyecto: ***"FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL".***

A continuación, el señor mayor Luis Fernando Romero Roa, Jefe Grupo Despliegue y Operaciones de Tecnologías de la Información y las Comunicaciones GUDES - OFTIC, realiza la presentación del presente proyecto, el cual se adjunta a la presente acta:

Nota: Se deja constancia que se realizó la exposición del proyecto en mención y la presentación de este se encuentra adjunta en la comunicación oficial No. GS-2026-007413-OFTIC del 04/08/2026.

4.3 Recomendaciones, sugerencias y observaciones realizadas en GEPOL y en el Comité CERT.

A continuación, se presentan las sugerencias, observaciones, recomendaciones y consideraciones técnicas registradas en el Gestor de Contenidos Policiales (GEPOL) al comunicado oficial No. GS-2026-007413-OFTIC del 04/08/2026, así como aquellas formuladas durante la sustentación y evaluación del proyecto ante la instancia correspondiente. Por lo cual, se sugiere que deban ser atendidas e incorporadas en las fases de planeación, ejecución e implementación, con el fin de garantizar el cumplimiento de los lineamientos institucionales, la viabilidad técnica de la solución propuesta, la interoperabilidad con la arquitectura tecnológica institucional y el adecuado desarrollo del proyecto.

✓ **Asesor Jurídico**

De manera atenta y respetuosa me permito solicitar que, en el evento que la decisión del comité resulte viable para el presente proyecto, se informe a la unidad solicitante que tienen el deber de dar cumplimiento a lo establecido en el artículo 61 de la C.P. que encarga al estado la obligación de proteger la propiedad intelectual mediante las formalidades que establezca la ley; es por ello que, en la etapa de planeación contractual, deben establecerse las estipulaciones correspondientes para garantizar el respeto por los Derechos de Autor y la propiedad intelectual bajo lo consagrado en la Ley 23/1982, Ley 178/1994 y todas aquellas que la modifiquen, adicionen o deroguen, al igual que los lineamientos trazados en este aspecto por la UAE Dirección Nacional de Derecho Autor y la Superintendencia de Industria y Comercio. Dicho lo anterior, para los eventos de adquisición de Tecnologías de la Información y las Comunicaciones y/o partes, la unidad solicitante debe requerir certificados de autenticidad, certificados de distribuidor autorizado y/o las facturas, que garanticen que los elementos tecnológicos que se adquieren han respetado la propiedad intelectual de la persona natural o jurídica que la elaboró. De esta manera, podrá establecer las restricciones y facultades que en su favor ha señalado el titular de la obra. El proveedor está obligado a garantizar a la entidad la legitimidad de las licencias, salvaguardándola de cualquier responsabilidad por el uso del programa autorizado. Finalmente se informa a la unidad que adelanta la gestión ante en el comité, que las sugerencias de ajustes o correcciones realizadas por los miembros del comité CERT son mandatorios y la viabilidad va enlazada a las correcciones de los yerros identificados. En el evento que la unidad se aparte de los mismos, deberá justificar las razones que lo motivan y correrá por su cuenta y riesgo las inconsistencias que se generen en la operacionalización de los mismos.

✓ **Grupo Mesa de Ayuda**

Una vez revisado el proyecto y las fichas técnicas que lo soportan, el Grupo de Mesa de Ayuda no presenta observaciones ni recomendaciones específicas, toda vez que la necesidad corresponde a un requerimiento propio de la unidad solicitante y no involucra elementos, equipos o infraestructura que requieran validación técnica dentro de la misionalidad de este Grupo. No obstante, se recomienda que, durante la estructuración del Estudio de Conveniencia y Oportunidad, se garantice el cumplimiento de los principios de pluralidad de oferentes, selección objetiva, transparencia y neutralidad, de conformidad con la Constitución Política de Colombia, la Ley 80 de 1993, la Ley 1150 de 2007, la Ley 1474 de 2011, la Ley 1882 de 2018, la Ley 2294 de 2023 y demás normas que regulan la contratación estatal. Asimismo, deberá observarse lo dispuesto en el Decreto 1082 de 2015 y, cuando resulte aplicable, en el Decreto 310 de 2021 respecto de los Acuerdos Marco de Precios y demás instrumentos de agregación de demanda, así como las directrices internas vigentes de la Policía Nacional y los lineamientos expedidos por Colombia Compra Eficiente.

✓ **Grupo Soporte y Apoyo**

Por parte del Grupo de Soporte y Apoyo no se presentan observaciones al proyecto. No obstante, se encuentra pendiente la sustentación ante el Comité CERT, instancia en la que podrían generarse comentarios, observaciones o recomendaciones que contribuyan al fortalecimiento y ajuste de la propuesta, de ser necesario.

✓ **Grupo Comunicaciones Unificadas**

Por parte del Grupo de Comunicaciones Unificadas (GUDAS) no se tiene OBSERVACIONES ni sugerencias específicas respecto a este proceso

✓ **Grupo Administración de Servicio de Infraestructura en la Nube**

El Grupo de Administración de Servicios de Infraestructura en la Nube (GUSIN), una vez revisada la ficha técnica y demás documentación soporte del proyecto y desde una perspectiva técnica alineada con las funciones inherentes del grupo, no se tienen observaciones sobre los bienes a adquirir; a su vez la unidad solicitante realizó actividades de acompañamiento y validación de prerrequisitos a la necesidad tecnológica, estableciendo que los requerimientos técnicos expuestos se adaptan a la necesidad de la unidad de policía. estableciendo que los requerimientos técnicos expuestos se adaptan a la necesidad de la unidad de policía; no obstante, se recomienda garantizar la transparencia, competitividad y eficiencia en el proceso de contratación mediante el cumplimiento de los principios de la Ley 80 de 1993, la Ley 1150 de 2007 y el Decreto 1082 de 2015. Queda pendiente la exposición detallada por parte de la unidad responsable.

✓ **Grupo Desarrollo de Software**

Para el Grupo Desarrollo de Software, tras revisar las fichas técnicas y la documentación del proyecto, no se presentan observaciones sobre los elementos a adquirir, considerando que los requerimientos técnicos se ajustan a la necesidad identificada por la unidad solicitante, la cual realizó el acompañamiento y validación de requisitos. Queda pendiente la exposición por parte del responsable del proyecto.

✓ **Grupo Arquitectura Tecnológica**

Por parte del Grupo de Arquitectura Tecnológica se realizó la verificación de las especificaciones técnicas y sus adjuntos, no se presentan observaciones al respecto. Es importante destacar que, por tratarse de un equipo especializado que apoyará las labores misionales de la unidad. Todas las observaciones, solicitudes de aclaración, recomendaciones, comentarios y demás aspectos que se deriven de la revisión de la solicitud presentada por la unidad en el GEPOL o en el sistema que haga sus veces, realizadas por los jefes de grupo de la OFTIC o sus delegados, tendrán carácter reservado. Lo

anterior, en razón a que dichos elementos se generan en el marco del proceso de validación de especificaciones técnicas y constituyen parte del soporte documental que fundamenta las decisiones adoptadas por el Comité CERT. En consecuencia, estas observaciones deberán ser tratadas con el mismo nivel de confidencialidad y reserva aplicable a las actas y a los comunicados oficiales emitidos por el Comité CERT.

✓ **Grupo Potencia Eléctrica y Seguridad Electrónica**

Me permito informar que, después de verificar los documentos anexos, no se tienen observaciones, por parte del Grupo de Potencia Eléctrica y Seguridad Electrónica. Lo anterior, conforme a lo establecido en el procedimiento 1DT-PR-0013 "Mantenimiento y soporte técnico a sistemas de respaldo de energía" y Resolución 0259 del 25-01-2023 en su artículo 16, por la cual se define la estructura orgánica de la oficina de tecnologías de la información y las comunicaciones. Asimismo, la Oficina de Tecnologías de la Información y las Comunicaciones (OFTIC) emite conceptos sobre fichas técnicas para la adquisición de bienes y servicios que hacen parte de su misionalidad, conforme a lo establecido en la Resolución No. 0259 del 25 de enero de 2023. En este sentido, cualquier análisis relacionado con estudios previos, anexos o demás ítems vinculados a las etapas precontractual, contractual y postcontractual debe abordarse conforme a los lineamientos normativos y procedimientos establecidos.

✓ **Grupo Despliegue y Operaciones de Tecnologías de la Información y las Comunicaciones**

Por parte de GUDES no se tienen observaciones. Pendiente CERT.

✓ **Responsable Planeación Administrador Riesgos**

De manera respetuosa, me permito informar que se realizó la revisión de la presentación del requerimiento. En lo que respecta a la matriz de riesgos, no se identificaron observaciones puntuales ni aspectos que requieran ajustes adicionales

✓ **Grupo Proyección e Innovación Tecnológica**

El Grupo de Proyección e Innovación Tecnológica (GUTEC) no presenta observaciones frente al presente proceso, toda vez que no involucra elementos, equipos o infraestructura que requieran viabilización mediante prueba de concepto (PoC); en todo caso, se recomienda que en la estructuración del Estudio de Conveniencia y Oportunidad se garanticen los principios de pluralidad de oferentes, selección objetiva, transparencia y neutralidad, de conformidad con la normatividad de contratación estatal vigente (Leyes 80 de 1993, 1150 de 2007, 1474 de 2011, 1882 de 2018 y 2294 de 2023), el Decreto 1082 de 2015 y, cuando resulte aplicable, el Decreto 310 de 2021 sobre Acuerdos Marco de Precios, así como los lineamientos de Colombia Compra Eficiente.

✓ **Grupo Red de Radio**

Se llevó a cabo la verificación del proyecto, sin que se generaran observaciones por parte del Grupo Red de Radio, dado que el mismo no contempla elementos específicos orientados a la sostenibilidad o modernización de la red de radios de la unidad solicitante. Se está a la espera de la realización del Comité Evaluador de Requerimientos Tecnológicos (CERT), con el fin de obtener una explicación más detallada sobre el alcance y justificación técnica del proyecto.

✓ **Grupo Seguridad de la Información y Respuesta a Incidentes Informáticos**

Una vez revisada la documentación técnica del proyecto, desde la perspectiva del CSIRT, no se evidencian observaciones específicas en materia de seguridad de la información que impidan su avance, por lo cual el proyecto se considera técnicamente VIABLE, siempre que su implementación, operación y administración se realicen en estricto cumplimiento de las directrices, políticas y controles establecidos en el Manual del Sistema de Gestión de Seguridad de la Información (SGSI), adoptado mediante la Resolución No. 04408 del 26 de diciembre de 2024, garantizando la confidencialidad, integridad y disponibilidad de la información institucional. Así mismo, conforme a la caracterización del

proceso de Direccionamiento Tecnológico, se recuerda que los elementos y servicios deberán ser adquiridos e implementados bajo dichos lineamientos, asegurando la transparencia, competitividad y eficiencia del proceso contractual, en cumplimiento de los principios establecidos en la Ley 80 de 1993, la Ley 1150 de 2007 y el Decreto 1082 de 2015, especialmente en lo relacionado con la pluralidad de oferentes. Finalmente, se sugiere presentar el proyecto ante el comité correspondiente, con el fin de acoger posibles observaciones adicionales

✓ **Comité Evaluador de Requerimientos Tecnológicos**

Teniendo en cuenta la información presentada durante la sustentación del proyecto, así como el análisis técnico efectuado sobre la solución propuesta, a continuación, se establecen algunas recomendaciones y consideraciones, las cuales, se sugiere que deben ser atendidas por la unidad responsable, con el fin de garantizar el cumplimiento del Direccionamiento Tecnológico Institucional, la alineación con la arquitectura tecnológica de la Policía Nacional, la interoperabilidad de los componentes tecnológicos y la adecuada ejecución e implementación del proyecto:

1. Una vez obtenida la viabilidad del presente proyecto, la unidad solicitante **deberá consultar** si la tecnología que se pretende adquirir se encuentra dentro de los componentes de aprobación por parte del Comité de Integración de Tecnologías de Información y Comunicaciones – CITI del Sector Defensa, los cuales se encuentran relacionados en la **Circular No. M20230511004862** del 11/05/2025 del Ministerio de Defensa Nacional o la que haga sus veces; **en caso afirmativo**, deberá realizar los trámites correspondientes para presentarlo ante mencionado Comité, en cumplimiento a la resolución número 4317 del 28 de junio del 2022 "*Por la cual se conforma y se asignan unas funciones al Comité de Integración de Tecnologías de Información y Comunicaciones del Sector Defensa, relacionadas con la adopción de criterios sectoriales para la aprobación de proyectos de tecnología y los recursos asociados a ellos*", artículo 7, literal A "Emitir concepto frente a las necesidades o proyectos con componente tecnológico cualquiera que sea su fuente de financiación presentados por las unidades del Sector, soportados en estudios de viabilidad técnica, legal y financiera del proyecto".
2. Las especificaciones técnicas avaladas por OFTIC son el resultado de un proceso de análisis y validación orientado a garantizar su alineación con la arquitectura tecnológica institucional, los estándares de interoperabilidad, seguridad de la información y uso eficiente de los recursos públicos. En consecuencia, cualquier modificación, adición o eliminación de los requisitos técnicos aprobados deberá contar previamente con la revisión y aprobación técnica de esta oficina asesora; de lo contrario, podrá afectar la validez del concepto de viabilidad emitido, de conformidad con lo establecido en la Comunicación Oficial No. **GS-2026-007024-OFTIC** del 22/07/2026.
3. El concepto de viabilidad emitido por el Comité Evaluador de Requerimientos Tecnológicos (CERT) se circunscribe **exclusivamente a la evaluación de la iniciativa desde la óptica técnica**, realizada con fundamento en los lineamientos, procedimientos y disposiciones institucionales vigentes en materia de adquisición y evaluación de tecnologías de la información y las comunicaciones, entre ellas la Resolución 03049 de 2014 y sus modificaciones, la Resolución 05884 de 2019 y sus modificaciones, la Resolución 00011 de 2025 y sus modificaciones, el procedimiento 1DT-PR-0019 "Evaluación de Tecnologías de la Información y las Comunicaciones" y demás directrices aplicables. En consecuencia, dicho concepto no constituye autorización, aprobación o aval respecto de aspectos administrativos, financieros, presupuestales, jurídicos o contractuales, siendo responsabilidad exclusiva de la unidad dueña de la necesidad garantizar la correcta planeación, adquisición, selección de proveedores, definición de marcas, cantidades, valores y fuentes de financiación, así como el cumplimiento de la normatividad legal e institucional vigente en cada una de estas materias.
4. Los Jefes y Responsables GUTIC deberán garantizar la observancia y cumplimiento integral de las especificaciones técnicas viabilizadas por la Oficina de Tecnologías de la Información y las Comunicaciones (OFTIC), absteniéndose de efectuar modificaciones, adiciones o supresiones no autorizadas y gestionando formalmente ante dicha dependencia cualquier requerimiento de ajuste para su correspondiente evaluación y pronunciamiento técnico. En consecuencia, la alteración de especificaciones previamente aprobadas, la utilización de fichas técnicas diferentes a las avaladas,

la inclusión de requisitos no autorizados o la ejecución de adquisiciones tecnológicas sin la respectiva viabilidad técnica podrá constituir un presunto incumplimiento de los deberes funcionales asociados a la planeación, estructuración y gestión de requerimientos tecnológicos institucionales, sin perjuicio de las responsabilidades administrativas, disciplinarias, fiscales, civiles o penales a que haya lugar, de conformidad con la normatividad vigente.

5. El concepto técnico de viabilidad del comité tendrá una vigencia de seis (06) meses para proyectos financiados con recursos de la Policía Nacional y doce (12) meses para proyectos financiados con recursos del FONSET o FONSECON. Dicho término inicia a partir de la suscripción del acta por parte del Comité CERT o al término de la anualidad. Lo anterior, en atención al **Artículo 10. Vigencia de la viabilidad** de la Resolución Nro. 01990 del 24/07/2026 "*Por la cual se reglamenta la conformación y funcionamiento del Comité Evaluador de Requerimientos Tecnológico de la Policía Nacional*".

6. En el evento de adquirir software o licenciamiento se recomienda que durante la etapa de estructuración del proyecto se analice y determine con precisión el alcance de las licencias de uso que serán adquiridas por la entidad. Esto permitirá establecer de manera clara las restricciones y facultades otorgadas por el titular de los derechos de autor sobre la obra. Así mismo, sean incorporados los siguientes ítems frente al proyecto: **1.** El contratista entregará certificación de distribuidor autorizado o mayorista certificado en la distribución del producto. **2.** El contratista se compromete a entregar certificación de autenticidad de la licencia, una vez se adjudique el contrato. **3.** El proveedor está obligado a garantizar a la entidad la legitimidad de las licencias, salvaguardándola de cualquier responsabilidad por el uso del programa autorizado **4.** El contratista al que se adjudique el contrato deberá entregar al supervisor certificación expedida por el distribuidor autorizado o mayorista que garantice el soporte por la cantidad de (x) año(s). **Nota**: el supervisor deberá solicitar los certificados al contratista y deberán incorporarse en el seguimiento de parte de la supervisión en la plataforma SECOP II y en la carpeta física del archivo postcontractual. Lo anterior, en cumplimiento a la circular conjunta 004 de 2006, emitida por la Dirección Nacional de Derechos de Autor y la Procuraduría General de la Nación.

7.

- Certificado de autenticidad del software adquirido.

- Documento que acredite al proveedor como distribuidor autorizado.

8. Se recuerda el cumplimiento al procedimiento **1DT-PR-0016** "*Implementación Proyectos de Tecnología de la Información y las Comunicaciones", una vez ejecutado el proyecto.*

9. En los procesos de adquisición tecnológica se deberá garantizar la pluralidad de oferentes, la selección objetiva y la neutralidad contractual, conforme a lo dispuesto en el artículo 2, literal a), de la **Ley 1150 de 2007**, permitiendo la participación de diferentes proveedores, salvo cuando exista justificación técnica relacionada con la compatibilidad e integración con plataformas institucionales existentes o cuando se trate de soluciones únicas disponibles en el mercado. Asimismo, deberá observarse el cumplimiento del **Decreto 310 de 2021**, en lo referente a la obligatoriedad y aplicación de los Acuerdos Marco de Precios y demás disposiciones que regulen los mecanismos de adquisición estatal vigentes.

10. Se deberá observar y dar cumplimiento a las disposiciones establecidas en el **Decreto 0618 del 17 de junio de 2026**, "*Por el cual se establece el Plan de Austeridad del Gasto para los órganos que hacen parte del Presupuesto General de la Nación*", garantizando que las adquisiciones y demás actuaciones asociadas al proyecto se encuentren alineadas con los principios de eficiencia, racionalización y optimización de los recursos públicos.

11. Conforme a lo establecido en el artículo 4, numeral 4, de la Ley 80 de 1993, la Entidad debe adelantar revisiones periódicas a las obras ejecutadas, los servicios prestados y los bienes suministrados, con el fin de verificar el cumplimiento de las condiciones de calidad ofrecidas por el

contratista. En caso de evidenciarse incumplimientos o deficiencias, se recomienda promover las acciones de responsabilidad correspondientes contra el contratista y sus garantes, según aplique. Asimismo, dichas revisiones deberán realizarse como mínimo una vez cada seis (6) meses durante la vigencia de las garantías contractuales.

12. DECLARACIÓN DE CONFIDENCIALIDAD Y COMPROMISO CON LA SEGURIDAD DE LA INFORMACIÓN SERVIDOR PÚBLICO. (1DT-FR-0015)

- EL SERVIDOR PÚBLICO se obliga en forma directa e irrevocable ante la POLICÍA NACIONAL a no revelar, divulgar o facilitar para actividades ajenas a su cargo o función, a ninguna persona natural o jurídica, sea esta pública o privada, y a no utilizar para su propio beneficio o para beneficio de terceros, la información relacionada con el ejercicio de sus funciones, así como también las políticas y/o cualquier otra información vinculada con sus funciones.
- EL SERVIDOR PÚBLICO asume la obligación de mantener la confidencialidad acordada en el presente acuerdo de confidencialidad por el tiempo que dure vigente la relación laboral y por un plazo adicional de dos (2) años contados a partir de la extinción del vínculo laboral o contractual.
- La violación o el incumplimiento del acuerdo de confidencialidad por parte EL SERVIDOR PÚBLICO, generará las acciones de tipo penal, disciplinario, administrativo y fiscal a que haya lugar.
- Si una orden judicial obligará al EL SERVIDOR PÚBLICO a divulgar información confidencial, este se compromete a dar aviso previo a su superior inmediato de modo que la POLICÍA NACIONAL pueda impugnar la solicitud o procurar una orden judicial que lo proteja.
- El SERVIDOR PÚBLICO reconoce que esta información tiene un valor intangible, que no es generalmente dado a conocer al público o a terceros que podrían usarla en contra de la POLICÍA NACIONAL, de sus integrantes, de los habitantes de Colombia o del mismo Estado y que la información está sujeta a un esfuerzo razonable de la POLICÍA NACIONAL para mantener su reserva y confidencialidad. Así mismo, EL SERVIDOR PÚBLICO no hará ninguna duplicación o copia del material confidencial.
- El SERVIDOR PÚBLICO devolverá inmediatamente todo material confidencial que se le haya entregado o asignado cuando así lo requiera o lo solicite la POLICÍA NACIONAL.
- El SERVIDOR PÚBLICO se compromete a no utilizar información o material confidencial una vez finalizada la relación laboral.

Recomendaciones del Comité CERT

Se recomienda oficiar a la Registraduría Nacional del Estado Civil con el fin de conocer su planificación tecnológica y los eventuales cronogramas de actualización, migración o sustitución del software actualmente utilizado para la replicación e intercambio de información biométrica. Lo anterior, con el propósito de mitigar riesgos asociados a la adquisición de licenciamiento por un periodo de tres (3) años, considerando la posibilidad de que la plataforma tecnológica sea modificada antes de la finalización del contrato.

La materialización de este riesgo podría generar la imposibilidad de continuar utilizando el licenciamiento adquirido, ocasionando subutilización de los recursos públicos invertidos, afectaciones en la continuidad operativa de los procesos de validación biométrica y la eventual necesidad de efectuar nuevas adquisiciones tecnológicas para garantizar la interoperabilidad con la infraestructura definida por la Registraduría. Por tal motivo, se considera pertinente obtener un pronunciamiento oficial de dicha entidad que permita reducir la incertidumbre y fortalecer la toma de decisiones durante la etapa de planeación contractual.

4.4. Decisión del Comité CERT

Teniendo en cuenta lo establecido en la Resolución Nro. 01990 del 24/07/2026, en especial el **artículo 7. Requisitos para la aprobación de las especificaciones técnicas**. La aprobación de las especificaciones técnicas sometidas a consideración del Comité Evaluador de Requerimientos Tecnológicos de la Policía Nacional (CERT) requerirá el voto favorable y unánime de la totalidad de sus integrantes. Por lo anterior, el secretario técnico del Comité procede a solicitar la votación por parte de cada uno de los integrantes, así;

Registro Votación:

GUPES	GUSAP	GUTEC	GUSOF	GUSIN	GUDAS	CSIRT	GRUMA	RIESGOS	GARTE	GURAD	GUDES
1	1	1	1	1	1	1	1	1	1	1	1

Nota. Se toma el 1 como concepto viable y el 0 como no viable.

Una vez finalizada la votación, se obtiene la siguiente decisión:

"Se emite concepto de viabilidad ***exclusivamente desde la perspectiva técnica y en el ámbito de competencia*** *del Comité Evaluador de Requerimientos Tecnológicos (CERT), teniendo en cuenta lo descrito en los comentarios registrados en el Gestor de Contenidos Policiales (GEPOL), así como las recomendaciones, sugerencias y observaciones formuladas durante el desarrollo del Comité CERT, las cuales se encuentran descritas en el numeral 4.3 de la presente acta".*

4.5. Ficha técnica aprobada

Se deja constancia de que las especificaciones técnicas aprobadas por el Comité Evaluador de Requerimientos Tecnológicos (CERT) corresponde a los elementos relacionados en el cuadro de cantidades contenido en la presentación adjunta a la comunicación oficial electrónica No. GS-2026-007413-OFTIC del 04/08/2026, por lo anterior, no deben ser modificadas, ni se deben adicionar ítems que no fueron socializados y/o conocidos durante la sesión del comité, en caso de ser requerida una nueva especificación técnica se debe activar nuevamente el procedimiento 1DT-PR-0019.

COMPROMISOS:

Relación de los compromisos adquiridos por los participantes

Actividad	Responsable	Fecha de entrega
1. Emitir respuesta a la solicitud presentada.	PT. Julián Camilo Riveros Martínez	15/08/2026
2. Para el desarrollo del proyecto, se debe tener en cuenta y notificar al responsable de la estructuración, las recomendaciones y consideraciones descritas en los comentarios realizados en el GEPOL (ítem 4.2) y en el ítem 4.3 de la presente acta.	Jefe Grupo Despliegue y Operaciones de Tecnologías de la Información y las Comunicaciones	Durante el desarrollo del proyecto
3. Realizar seguimiento a la ejecución del proyecto.	Jefe Grupo Despliegue y Operaciones de Tecnologías de la Información y las Comunicaciones	Hasta la finalización del proyecto

CONVOCATORIA

El Comité Evaluador de Requerimientos Tecnológicos (CERT), sesionará de manera ordinaria los días martes y jueves de cada semana, y también de manera extraordinaria de acuerdo con lo ordenado por el mando institucional.

...

FIRMA DIGITAL

Firmado digitalmente por:
Nombre: Julio Cesar Jimenez Fandiño
Grado: Mayor
Cargo: Jefe Grupo Arquitectura Tecnologica
Cédula: 79884264
Dependencia: Grupo Arquitectura Tecnologica
Unidad: Oficina Tecnologias De La Informacion Y Las Comunicaciones
Correo: julio.jimenez1126@correo.policia.gov.co
11/08/2026 11:31:22 a. m.

Anexo: uno (lista de asistencia en 02 folios)

Carrera 59 No 26 - 21 CAN
Teléfono: 5159551
oftic.garte@policia.gov.co
www.policia.gov.co

INFORMACIÓN PÚBLICA CLASIFICADA

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
OFICINA TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
GRUPO ARQUITECTURA TECNOLOGICA

CEA.3.0-07
16-ECD-003

Fecha:	Bogotá D.C., 06 de agosto de 2026		
Hora de inicio:	14:30	**Hora de finalización:**	17:30
Lugar:	Oficina de Tecnologías de la Información y las Comunicaciones videoconferencia vía Teams.		

Acta - 002344- SUTIC-GARTE - 2.7

QUE TRATA DE LA SUSTENTACIÓN DE LAS ESPECIFICACIONES TÉCNICAS QUE CONFORMAN EL PROYECTO FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL - OFTIC - GUDES

ASISTENTES

GR	NOMBRES Y APELLIDOS	UNIDAD O DEPENDENCIA	CORREO ELECTRÓNICO	CEDULA DE CIUDADANÍA	TELÉFONO	NOTIFICACIÓN
MY	ROMERO ROA LUIS FERNANDO	OFTIC GUDES	luis.romero1084@correo.policia.gov.co	7185190	3008536992	07/08/2026 14:31
MY	RESTREPO CORREA JOHN DARIO	OFTIC GUSIN	john.restrepo@correo.policia.gov.co	71794221	3108644754	07/08/2026 20:14
MY	RODRIGUEZ PUENTES CLAUDIA YANETH	OFTIC GUSOF	claudia.rodriguez1449@correo.policia.gov.co	37841449	3187948759	07/08/2026 14:48
MY	RAMIREZ GIL EDWIN JAVIER	OFTIC GUSAP	edwin.ramirez1091@correo.policia.gov.co	1121839552	3194238798	07/08/2026 14:00
MY	MENDEZ MENDOZA JHON ALEXANDER	OFTIC CSIRT	jhon.mendez1103@correo.policia.gov.co	1110452448	3016588335	07/08/2026 15:28
CT	MUÑOZ RESTREPO RIGOBERTO	OFTIC GUPES	rigoberto.munoz@correo.policia.gov.co	6391966	3156310960	07/08/2026 15:41
CT	RONDON LUNA JULIAN DAVID	OFTIC GRUMA	julian.rondonl@correo.policia.gov.co	1121901406	3143473244	07/08/2026 14:18
ST	BARRERA MORENO LUIS ALFONSO	OFTIC GUTEC	luis.barreram@correo.policia.gov.co	1032498207	3124976564	07/08/2026 14:06
ST	OROSCO BUITRAGO PAULA CAROLINA	OFTIC GURAD	paula.orosco@correo.policia.gov.co	1098731964	3229463858	07/08/2026 12:07
ST	VELEZ VELEZ ASDRUBAL ANDRES	OFTIC GUDAS	andres.velez@correo.policia.gov.co	1112791398	3184426271	07/08/2026 14:13
IJ	REYES RINCON NELSON ENRIQUE	OFTIC GARTE	nelson.reyes4050@correo.policia.gov.co	1069944050	3132043552	07/08/2026 18:32
IT	HERRAN ROMERO JENNIFFER PAOLA	ECSAN GUTIC	jennifer.herran@correo.policia.gov.co	1022939460	3112834816	07/08/2026 14:18

Acta - 002344- SUTIC-GARTE - 2.7

QUE TRATA DE LA SUSTENTACIÓN DE LAS ESPECIFICACIONES TÉCNICAS QUE CONFORMAN EL PROYECTO FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL - OFTIC - GUDES

Carrera 59 No 26 - 21 CAN
Teléfonos 5159551
oftic.garte@policia.gov.co
www.policia.gov.co

INFORMACIÓN PÚBLICA CLASIFICADA

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
GRUPO COMUNICACIONES UNIFICADAS

GS-2026- 009589 **-SUTIC - GUDES 20.1**

Bogotá D.C., 07 de agosto de 2026

Señora presidente
MARÍA INÉS AGUDELO VALENCIA
Bolsa Mercantil de Colombia S.A
Calle 113 # 7-21 Torre A Piso 15. Edif. Teleport BusinessPark
Bogotá D.C.

Asunto: Solicitud de información para la adquisición del "FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE LA SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL"

De manera respetuosa me dirijo a la Dirección bajo su administración, con el propósito de dar a conocer que la Policía Nacional de Colombia requiere la adquisición del *"FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE LA SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL"*, y de conformidad con lo dispuesto en el artículo 2° del Decreto 310 del 25/03/2021 por el cual se modifica el artículo 2.2.1.2.1.2.12. del Decreto 1082 de 2015 Único Regiamentario del Sector Administrativo de Planeación Nacional, así *"(...) Planeación de una adquisición en la bolsa de productos: Cuando no exista un Acuerdo Marco de Precios para el bien o servicio requerido, las entidades estatales deben estudiar, comparar e identificar las ventajas de utilizar la bolsa de productos para la adquisición respectiva frente a la subasta inversa o a la promoción de un nuevo Acuerdo Marco de Precios con la Agencia Nacional de Contratación Pública -Colombia Compra Eficiente- para tales bienes o servicios, incluyendo el análisis del Proceso de Selección del comisionista, los costos asociados a la selección, el valor de la comisión y de las garantías (...)"*; la Oficina de Tecnologías de la Información y las comunicaciones, solicita de su valiosa colaboración en el sentido de despejar los siguientes interrogantes:

1. ¿La Bolsa Mercantil de Colombia S.A., oferta actualmente los aspectos Generales y técnicos de la ficha técnica del anexo?

2. ¿La Policía Nacional de Colombia se encuentra o no exenta del impuesto de valor agregado por la utilización del mecanismo de compra a través de Bolsa de Productos?

3. ¿Cuál es el valor económico por concepto de costos indirectos de comisión BMC, comisión representante, garantías liquidas, tarifas administrativas, compensaciones y liquidaciones o la denominación que se le diere a los costos generados por la utilización del mecanismo de compra a través de Bolsa de Productos?

4. ¿Cuál es el valor histórico de precios, registrados sobre el: *"FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE LA*

SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL"?

5. Con el fin de realizar un análisis simétrico entre cantidades y el valor unitario, donde ya se incluya los costos generados por la utilización del mecanismo de adquisición de la solución a través de Bolsa de Productos, solicito muy respetuosamente dar a conocer la dicha información.

Atentamente,

Patrullera **VIVIANA EIZABETH BURBANO ROMERO**
Estructurador Estudio Previo

Intendente **WILSON ALEJANDRO HENAO ARIAS**
Estructurador Estudio Previo

Fecha de elaboración: 010/08/2026
Ubicación: \\srvfilesponal3\OFITE\AITEC\GRUIM

Carrera 59 No. 26 21, Bogotá
Teléfonos 5159910
Humberto.meza4690@correo.policia.gov.co
www.policia.gov.co

INFORMACIÓN PÚBLICA

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
GRUPO DE COMUNICACIONES UNIFICADAS

GS-2026- 007696 **-SUTIC - GUDES - 20.1**

Bogotá D.C., 07 de agosto 2026.

Doctor
CRISTÓBAL PADILLA TEJEDA
Director de Colombia Compra Eficiente
Carrera 7 No. 26 – 20 Piso 17,10 y 8, Edificio Tequendama.
Bogotá D.C.

Asunto: solicitud de información para la adquisición del *" FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE LA SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL".*

De manera atenta y respetuosa me dirijo a la Dirección bajo su digno cargo, con el propósito de informar que la Policía Nacional de Colombia para la vigencia 2026, requiere realizar proceso contractual para la adquisición del *"FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE LA SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL";* en ese sentido, de acuerdo con el artículo 2.2.1.2.1.2.7 del Decreto Único Reglamentario 1082 de 2015, las entidades estatales de Rama Ejecutiva del Poder Público del orden nacional, obligadas aplicar la ley 80 de 1993 y la Ley 1150 de 2007 o las normas que las modifiquen, aclaren, adicionen o sustituyan, están obligadas a adquirir bienes y servicios de características técnicas uniformes a través del acuerdo marco de precios vigentes.

Por lo anterior y teniendo en cuenta la naturaleza jurídica del Ministerio de Defensa Nacional, las entidades ejecutoras y delegatarias deben hacer uso de los Acuerdos Marco de Precios en la forma dispuesta por Colombia Compra Eficiente; en consecuencia, se realizó la verificación en la Tienda Virtual del Estado Colombiano, evidenciando que actualmente no existe un Acuerdo Marco de Precios o Instrumento de Agregación de Demanda que permita la adquisición e implementación de la solución tecnológica SharePlex, la migración de bases de datos Oracle 12c a Oracle 19c y los servicios especializados asociados, conforme a los requerimientos técnicos establecidos por la Registraduría Nacional del Estado Civil para la operación del servicio de autenticación biométrica bajo la modalidad de infraestructura propia.

En tal virtud, la Policía Nacional de Colombia requiere adelantar el correspondiente proceso contractual, toda vez que la implementación de la solución SharePlex constituye un requisito técnico obligatorio establecido en el Anexo Técnico No. 2 de la Resolución 27145 de 2023, el cual exige la instalación y configuración de esta herramienta para realizar la replicación y sincronización de las bases de datos entre el centro de datos de la Registraduría Nacional del Estado Civil y la infraestructura tecnológica de la Policía Nacional.

De este modo, al realizar el contraste entre los requerimientos técnicos del proyecto "FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE LA SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL" y los Acuerdos Marco de Precios vigentes administrados por Colombia Compra Eficiente, se evidencia que ninguno contempla integralmente el suministro de licenciamiento, implementación, configuración, puesta en funcionamiento, migración

tecnológica y servicios especializados requeridos para garantizar la replicación, sincronización y administración de las bases de datos biométricas en cumplimiento de los lineamientos definidos por la Registraduría Nacional del Estado Civil.

Así mismo, teniendo en cuenta las responsabilidades asignadas a la Policía Nacional como operador de autenticación biométrica bajo la modalidad de infraestructura propia, resulta indispensable fortalecer la capacidad tecnológica institucional mediante la implementación de herramientas especializadas que permitan garantizar la disponibilidad, integridad, confidencialidad y sincronización permanente de la información biométrica utilizada en los procesos de identificación ciudadana, consulta de antecedentes, policía judicial, inteligencia, contrainteligencia y demás actividades misionales de la Institución.

En este contexto, solicitamos muy respetuosamente se informe si actualmente existe un Acuerdo Marco de Precios o Instrumento de Agregación de Demanda vigente que permita satisfacer la necesidad relacionada con el proyecto "FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE LA SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL", incluyendo el suministro de licenciamiento, migración tecnológica, implementación, configuración y puesta en operación de la solución SharePlex. En caso de no existir, se solicita informar lo correspondiente para adelantar el proceso contractual que permita atender oportunamente la necesidad institucional.

Del mismo modo, de ser viable la estructuración de un acuerdo o instrumento de agregación de demanda para este tipo de soluciones especializadas, agradeceremos informar los tiempos estimados para su desarrollo, considerando que la necesidad institucional se encuentra directamente asociada al cumplimiento de los requisitos técnicos establecidos por la Registraduría Nacional del Estado Civil y a la continuidad de los servicios de autenticación biométrica que soportan la operación policial a nivel nacional.

Atentamente,

Patrullera **VIVIANA EIZABETH BURBANO ROMERO**
Estructurador Estudio Previo

Intendente **WILSON ALEJANDRO HENAO ARIAS**
Estructurador Estudio Previo

Fecha de elaboración: 010/08/2026
Ubicación: \\srvfilesponal3\OFITE\AITEC\GRUIM

Carrera 59 No. 26 21, Bogotá
Teléfonos 5159910
Oftic.gudes@policia.gov.co
www.policia.gov.co

INFORMACIÓN PÚBLICA

OFTIC GUDES

De: Radica aquí tu PQRSF <jira@bmcpqrs.atlassian.net>
Enviado el: viernes, 21 de agosto de 2026 10:01 a.m.
Para: OFTIC GUDES
Asunto: PQRSF-1172 solicitud de información para la contratación del FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE LA SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL EST...

No suele recibir correo electrónico de jira@bmcpqrs.atlassian.net. Por qué es esto importante

Recibe un cordial saludo

Te informamos que se recibió un comentario de **Deisy Milena Mora Alvarado** a tu solicitud de radicado con el ID **PQRSF-1172:**

Intendente Henao, buenos días.

Reciba un cordial saludo

De acuerdo con su solicitud presentada en el anexo, atentamente me permito indicar lo siguiente:

1. A través del Mercado de Compras Públicas – MCP de la Bolsa Mercantil de Colombia – BMC, sí es posible adquirir los servicios relacionados en el anexo (Infraestructura de datos mediante la implementación de la solución Shareplex). Las características técnicas que requiere cada uno de los productos y/o servicios que se pretenden adquirir a través del escenario de la Bolsa Mercantil de Colombia, son definidos por la entidad compradora, así como el precio y todas las demás condiciones propias de la negociación.

En línea con lo señalado anteriormente, los aspectos técnicos de los productos y/o servicios objeto de adquisición, son definidas e incorporadas directamente por la entidad compradora en la Ficha Técnica de Negociación (FTN) y en la Ficha Técnica de Producto (FTP), garantizando que el proceso se estructure conforme a sus necesidades particulares

1. El MCP constituye un escenario de negociación; en consecuencia, corresponde a los participantes determinar de manera directa la carga impositiva aplicable a los productos o servicios objeto de negociación.

1. Los costos asociados a una negociación en el escenario de la Bolsa Mercantil se componen de 2 rubros como se puede apreciar en la imagen, y se causan sobre el valor del cierre de la negociación:

Costos Asociados

	Renta Disponible	Renta Fija Mercado Secundario
Registro en Bolsa y Compensación y liquidación	0.45% + IVA	0.51% + IVA
Sociedades Comisionistas de Bolsa	Libre + IVA	

Es importante resaltar que el costo de la comisión de la Sociedad Comisionista de Bolsa está directamente relacionado con el presupuesto asignado por la Entidad para la adquisición.

1. Las operaciones celebradas a través del escenario de la Bolsa Mercantil de Colombia se encuentran publicadas en la página web http://www.bolsamercantil.com.co , los invitamos a visitar nuestro portal y consultar la información requerida.

1. El Mercado de Compras Públicas de la Bolsa Mercantil de Colombia, **no cotiza precios de productos o servicios** que las entidades estatales deseen adquirir. Somos un escenario de negociación a través del cual las entidades públicas pueden adquirir bienes, productos y servicios de características técnicas uniformes, utilizando la modalidad de selección abreviada bajo la causal de Bolsa de Productos; esto en el marco de la Ley 1150 de 2007, el Decreto Único 1082 de 2015 y el Reglamento de Funcionamiento y Operación aprobado por la Superintendencia Financiera de Colombia.

Sin otro particular, en los anteriores términos damos por absuelta su consulta, no sin antes indicar que, cualquier inquietud adicional, con gusto será atendida._

Servicio al Cliente
Dirección de Sostenibilidad
Tel: (601) 629 2529 Ext. 880
WhatsApp: 320 8330986
Calle 113 # 7 – 21 Teleport Business Park torre A - piso 15
www.bolsamercantil.com.co
Bolsa Mercantil de Colombia Oficial

Nota de confidencialidad: este mensaje (incluyendo cualquier anexo) contiene información confidencial de BMC Bolsa Mercantil de Colombia S.A. y se encuentra protegida por la Ley. Sólo puede ser utilizada por el personal o compañía a la cual está dirigido. Si usted no es el receptor autorizado, o por error recibe este mensaje, favor borrarlo inmediatamente. Cualquier retención, difusión, distribución, copia o toma de cualquier acción basada en ella, se encuentra estrictamente prohibido.

Nota de privacidad: La BMC Bolsa Mercantil de Colombia S.A es responsable y/o encargado del tratamiento de sus datos, por ello, ha puesto a su disposición información sobre sus derechos, finalidades de tratamiento y canales de atención en nuestra política de tratamiento de datos personales, la cual puede consultar ingresando a www.bolsamercantil.com.co.

Agencia Nacional
de Contratación Pública
Colombia Compra Eficiente

Bogotá D.C., 12 de agosto de 2026

Colombia Compra Eficiente
Radicado No. 2_2026_08_12_008568
Anexos: No Con copia: No
Fecha: 12/08/2026 13:44:35

Señora
VIVIANA ELIZABETH BURBANO ROMERO
oftic.gudes@policia.gov.co
Ciudad

ASUNTO: Respuesta a Petición con Número de Radicado 1_2026_08_11_010568

Respetada señora Burbano,

La Agencia Nacional de Contratación Pública – Colombia Compra Eficiente –, en ejercicio de las competencias otorgadas por los Decretos 4170 de 2011 y 1822 de 2019 y de conformidad con las modalidades del derecho de petición contempladas en la Ley 1755 de 2015, así como lo establecido en la resolución N° 469 del 2025 expedida por esta Agencia, damos respuesta a su radicado No. 1_2026_08_11_010568 fecha 11 de agosto de 2026 en donde indica:

PETICIÓN REALIZADA

*"De manera atenta y respetuosa, la Policía Nacional, a través de la Oficina de Tecnologías de la Información y las Comunicaciones, se permite solicitar información relacionada con la existencia de un Acuerdo Marco de Precios u otro instrumento de agregación de demanda vigente que permita adelantar un proceso contractual cuyo objeto corresponda a la adquisición, implementación, configuración, migración y soporte de una solución tecnológica para la replicación de bases de datos basada en la herramienta **SharePlex**, así como los componentes tecnológicos requeridos para garantizar la continuidad y operación de los servicios de autenticación biométrica institucional.*

La necesidad surge en el marco del proyecto de fortalecimiento de la infraestructura tecnológica que soporta los procesos de autenticación biométrica y verificación de identidad de la Policía Nacional, mediante la modernización de las plataformas de bases de datos asociadas a la información suministrada por la Registraduría Nacional del Estado Civil (RNEC), garantizando el cumplimiento de los lineamientos técnicos establecidos en la Resolución No. 27145 de 2023 y su Anexo Técnico No. 2.

En particular, la Institución requiere una solución de replicación de bases de datos que permita la sincronización permanente de la información, soporte ambientes Oracle Standard Edition y Enterprise Edition, sea compatible con sistemas operativos Linux y Windows y cuente con soporte técnico especializado por un término mínimo de tres (3) años. Asimismo, se requiere la ejecución de actividades de instalación, configuración, migración de bases de datos Oracle desde la versión 12c hacia Oracle 19c, pruebas de funcionamiento y puesta en operación en ambiente de producción. [

Por lo anterior, agradecemos informar si actualmente existe un instrumento de compra administrado por esa Agencia que permita atender las necesidades anteriormente descritas; en caso afirmativo, solicitamos indicar el nombre del acuerdo o instrumento, su estado de vigencia, el enlace de consulta y los lineamientos aplicables para adelantar la adquisición correspondiente.

(...)

En consecuencia, se requiere conocer si estas necesidades pueden ser atendidas mediante los mecanismos de contratación estandarizados administrados por Colombia Compra Eficiente, con el fin de optimizar los tiempos del proceso contractual, asegurar el cumplimiento de la normativa vigente y garantizar la adquisición de bienes y servicios tecnológicos a través de los instrumentos de contratación pública disponibles."

Conforme lo anterior, la Agencia Nacional de Contratación Pública-Colombia Compra Eficiente- informa que el artículo 25 de la Ley 80 de 1993 señala que la planeación es un principio fundamental en la contratación estatal. Este principio implica que cada entidad debe realizar una adecuada planeación de sus procesos contractuales para asegurar la eficiencia, eficacia y transparencia en la utilización de los recursos públicos.

En línea con lo antes señalado, la jurisprudencia del Consejo de Estado también ha establecido que la responsabilidad de la planeación no puede ser delegada a otra entidad, ya que esto podría generar conflictos de interés y desalineación con las necesidades específicas de la entidad contratante.

En este sentido, la tarea de asegurar que algún bien o servicio en un Mecanismo de Agregación de Demanda, así como la decisión de utilizar o no algún Mecanismo de Agregación de Demanda, corresponde enteramente a la entidad contratante, quedando en manos de Colombia Compra Eficiente únicamente la posibilidad de pronunciarse en términos generales relacionados con agregación de demanda.

Conforme lo anterior y considerando la necesidad por usted expuesta, le invitamos a consultar el minisitio del IAD Software por Catálogo II mediante el siguiente enlace https://www.colombiacompra.gov.co/archivos/portfolio-item/iad-sda-de-software-por-catalogo-ii. En este minisitio la Entidad podrá consultar el catálogo, las guías de uso y los demás documentos del proceso y así mismo puede crear una solicitud de información (RFI) para indagar con proveedores del Mecanismo de Agregación de Demanda los servicios que requiera soportar, para de esta manera contar con más herramientas para determinar si con la oferta de servicios del MAD, se satisface las condiciones técnicas requeridas por la Entidad.

Además, aprovechamos la oportunidad de manifestar la entera disposición de la Agencia Nacional de Contratación Pública –Colombia Compra Eficiente– para atender las peticiones o solicitudes, así como para brindar el apoyo que se requiera en el marco de nuestras funciones a través de nuestros diferentes canales de atención:

- Línea nacional gratuita o servicio a la ciudadanía (Mesa de servicio): 01800 0520808
- Línea en Bogotá (Mesa de servicio): +57 601 7456788
- Correo de radicación de correspondencia: ventanilladeradicacion@colombiacompra.gov.co
- Formulario web para PQRSD: https://www.colombiacompra.gov.co/pqrsd/informacion-importante-antes-de-formular-una-pqrsd

Evalúa el servicio que ofrece la Agencia por el canal de atención de PQRSD en el siguiente enlace:https://forms.office.com/r/pPHyWVs2SZ .¡Ayúdanos a mejorar porque el compromiso es de todos!

Por último, lo invitamos a seguirnos en las redes sociales en las cuales se difunde información institucional:

Twitter: @colombiacompra
Facebook: ColombiaCompraEficiente
LinkedIn: Agencia Nacional de Contratación Pública - Colombia Compra Eficiente
Instagram: @colombiacompraeficiente_cce

Cordialmente,

JUAN PABLO VELÁSQUEZ SILVA
Asesor Experto G-08

Elaboro:	**Sandra Zamora Guzmán** **Administrador MAD**
Revisó:	**Eduardo Ortiz** **Analista T2-04**
Aprobó:	**Juan Pablo Velasquez Silva** **Asesor Experto G-08**

OFTIC GUDES

De:	OFTIC GUDES
Enviado el:	lunes, 10 de agosto de 2026 11:59 a.m.
Para:	'ventanillaunicaderadicacion@colombiacompra.gov.co'; 'lineaetica@colombiacompra.gov.co'; 'diana.silva@colombiacompra.gov.co'
Asunto:	solicitud de información catálogo de acuerdos marco
Datos adjuntos:	GS-2026-007596-OFTIC Solicitud Colombia Compra Eficiente.pdf

POLICÍA NACIONAL
Dirección General
Oficina de Tecnologías de la Información y las Comunicaciones
OFTIC

CORREO No. 0836 / OFTIC – GUDES 10/08/2026

Dios y Patria, cordial saludo.

De manera atenta y respetuosa me dirijo a la Dirección bajo su digno cargo, con el propósito de informar que la Policía Nacional de Colombia para la vigencia 2026, requiere realizar proceso contractual para la adquisición del "**FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE LA SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL**"; acorde con el artículo 2.2.1.2.1.2.7 del Decreto Único Reglamentario 1082 de 2015, las entidades estatales de Rama Ejecutiva del Poder Público del orden nacional, obligadas aplicar la ley 80 de 1993 y la Ley 1150 de 2007 o las normas que las modifiquen, aclaren, adicionen o sustituyan, están obligadas a adquirir bienes y servicios de características técnicas uniformes a través del acuerdo marco de precios vigentes.

Atentamente,

El contenido de este manual y sus anexos es propiedad de la POLICÍA NACIONAL DE COLOMBIA, son documentos para uso del destinatario y puede contener información con un nivel de clasificación de reserva legal. Si usted no es el destinatario autorizado por la Institución, por favor cualquier distribución o copia de esta comunicación está terminantemente prohibida. Cualquier revisión, retransmisión, diseminación o uso del mismo, así como cualquier acción que se tome respecto a la información contenida por personas o entidades diferentes al propósito original es ilegal.

CEA-3.0-07
16-ECD-003

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
OFICINA TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
GRUPO ARQUITECTURA TECNOLOGICA

SUTIC-GARTE - 20.10

Bogotá D.C., 11 de agosto de 2026

Señor mayor
LUIS FERNANDO ROMERO ROA
Jefe Grupo Despliegue y Operaciones de Tecnologías de la Información y las Comunicaciones
Oficina de Tecnologías de la Información y las Comunicaciones
Carrera 59 No 26 - 21 CAN
Bogotá D.C.

Asunto: respuesta a solicitud viabilidad proyecto solicitado mediante comunicado oficial GS-2026-007413-OFTIC del 04/08/2026

De manera atenta y respetuosa me dirijo al señor mayor, con el propósito de informar que, en atención a la solicitud realizada mediante la comunicación oficial del asunto, el Comité Evaluador de Requerimientos Tecnológicos – CERT, llevado a cabo el día 06/08/2026 como consta en el Acta No. AC-2026- 002344-OFTIC; emite concepto de **viabilidad a las fichas técnicas**, para continuar con el proyecto el cual tiene como objeto "***FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL***", es importante tener en cuenta las recomendaciones, sugerencias y observaciones realizadas a través de los comentarios generados en el Gestor de Contenidos Policiales – GEPOL, así mismo, las establecidas en el numeral 4.3, del acta de aprobación.

Atentamente,

...

FIRMA DIGITAL

Firmado digitalmente por:
Nombre: Julio Cesar Jimenez Fandiño
Grado: Mayor
Cargo: Jefe Grupo Arquitectura Tecnologica
Cédula: 79884264
Dependencia: Grupo Arquitectura Tecnologica
Unidad: Oficina Tecnologias De La Informacion Y Las Comunicaciones
Correo: julio.jimenez1126@correo.policia.gov.co
11/08/2026 8:20:26 p. m.

Anexo: no

Carrera 59 No 26 - 21 CAN
Teléfono: 5159551
oftic.garte@policia.gov.co
www.policia.gov.co

INFORMACIÓN PÚBLICA

GS-2026-008006-OFTIC

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
OFICINA TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
GRUPO DES OPERA TECNO DE INFOR Y COMUNICACIONES

CEA.3.0-07
16-ECD-003

SUTIC-GUDES - 20.1

Bogotá D.C., 21 de agosto de 2026

Señora teniente coronel
JENNY PATRICIA MORALES PUENTES
Jefe área financiera DILOF
Carrera 59 26-21 CAN
Bogotá D.C.

Asunto: solicitud indicadores financieros

De manera atenta y respetuosa me permito solicitar a mi coronel, tenga a bien ordenar a quien corresponda se emitan los indicadores financieros, para la estructuración del estudio previo cuyo objeto es el *"FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE LA SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL"*, con clasificación UNSPSC de la siguiente manera:

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE	CÓDIGO CIIU	DESCRIPCIÓN ACTIVIDAD CIIU
43231500	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software funcional específico de la empresa	6202	Actividades de consultoría informática y actividades de administración de instalaciones informáticas
43232300	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de consulta y gestión de datos	6202	Actividades de consultoría informática y actividades de administración de instalaciones informáticas

Así mimo, se anexan los RUP- Registro único de proponentes de diferentes empresas registradas en el SECOP 2 con los Clasificadores de Bienes y Servicios de las Naciones Unidas - UNSPSC, códigos CIIU, análisis del sector y estudio previo, requeridos para el desarrollo del proceso.

Atentamente,

FIRMA DIGITAL

Firmado digitalmente por:
Nombre: Wilson Alejandro Henao Arias
Grado: Intendente
Cargo: Implementador (A) Tecnologico (A)
Cédula: 1057304501
Dependencia: Grupo Des Opera Tecno De Infor Y Comunicaciones
Unidad: Oficina Tecnologias De La Informacion Y Las Comunicaciones
Correo: wilson.henao3082@correo.policia.gov.co
22/08/2026 11:06:44 a. m.

Anexo: si

Carrera 59 No 26 - 21 CAN
Teléfono: 5159437
oftic.gudes@policia.gov.co
www.policia.gov.co

INFORMACIÓN PÚBLICA

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DIRECCIÓN LOGÍSTICA Y FINANCIERA
GRUPO PRESUPUESTO GENERAL

GS – 2026 – /DILOF – GUPEG – 29.25

Bogotá D.C., 24 de agosto de 2026

Señor Intendente
WILSON ALEJANDRO HENAO ARIAS
Implementador Tecnológico
Oficina de Tecnologías de la Información y las Comunicaciones
Carrera 59 26 -21
Bogotá D.C.

Asunto: respuesta a la comunicación oficial GS-2026-008006-OFTIC

En atención a la comunicación oficial del asunto, respetuosamente enviar a mi intendente el resultado del análisis del sector realizado al proceso ***"FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE LA SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL"***, esto para tener en cuenta y anexar al estudio previo, así:

1. **Consideraciones exento**

- Normativas

a. Decreto 1082 de 2015.
b. Guía para la elaboración de Estudios del Sector versión G-EES-03.
c. Manual para determinar y verificar los requisitos habilitantes en los procesos de contratación versión M-CCE-EICP-MA-04, versión 3.

- La información financiera que se tomará para el presente análisis del sector será con cifras 2025 y proviene de fuentes fidedignas tomadas del Registro Único Empresarial y Social de la Superintendencia de sociedades RUES, así:

*"Dentro de los requisitos habilitantes se destaca la «capacidad financiera» y la «capacidad organizacional». **La entidad, como responsable de la estructuración de su procedimiento de selección, es autónoma para requerir la capacidad financiera y la capacidad organizacional necesarias, de acuerdo con la naturaleza del contrato que se pretende suscribir y a su valor.***

- Es de anotar que de acuerdo a lo indicado en la introducción de la guía para la elaboración de Estudios del Sector versión G-EES-03, se indica en la parte introductoria que ***"El resultado del análisis debe plasmarse en los estudios y documentos previos del Proceso de Contratación."*** (resaltado y subrayado fuera de texto).

2. **Metodología y Resultado del Análisis de los Indicadores de Orden Financiero (Índice de liquidez, Razón de Endeudamiento, Cobertura de Intereses) y de Orden Organizacional (Rentabilidad del Patrimonio, Rentabilidad del activo).**

La metodología utilizada está sustentada en los manuales y guías elaborados por la Agencia Nacional de Contratación Pública, Colombia Compra Eficiente; partiendo de la obligatoriedad de tener en cuenta los 5 indicadores de orden financiero y organizacional, se tomó información financiera de diecisiete (17) empresas del sector, ubicadas trece (13) en la ciudad de Bogotá, una (01) en la ciudad de Cucuta, una (01) en la ciudad de Ibagué, una (01) en la ciudad de Armenia y una (01) en el municipio de Cajicá, las cuales pertenecen al sector de los bienes y/o servicios requeridos, mediante la aplicación de seis medidas o promedios estadísticos así:

FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE LA SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL				
Cantidad de Proponentes	Indices Capacidad Organizacional		Indices Capacidad Financiera	
	Rentabilidad del patrimonio	Rentabilidad del activo	Indice liquidez	Cobertura de Intereses
1	0,88	0,75	3,57	810,59
2	0,11	0,10	17,47	INDETERMINADO
3	0,01	0,01	135,67	35,13
4	0,08	0,06	2,94	1,80
5	0,65	0,27	2,23	694,97
6	0,15	0,11	6,31	13,34
7	0,13	0,10	10,71	INDETERMINADO
8	1,86	1,08	2,73	114,19
9	0,06	0,04	4,14	INDETERMINADO
10	0,12	0,04	1,42	5,15
11	0,07	0,04	1,56	INDETERMINADO
12	0,41	0,25	2,23	35,02
13	1,09	0,59	2,13	27,15
14	0,08	0,07	1,63	450,95
15	0,07	0,03	2,06	INDETERMINADO
16	0,82	0,28	2,03	17,80
17	0,78	0,39	1,99	2.355,47
a. Media Aritmética	0,43	0,25	11,81	268,33
b. Media Podada	0,37	0,21	4,25	200,39
c. Mediana	0,13	0,10	2,23	35,08
d. Mínimo	0,01	0,01	1,42	1,80
e. Máximo	1,86	1,08	135,67	2.355,47
f. Promedio Ponderado	0,56	0,33	31,08	572,21

Para los resultados obtenidos de los instrumentos estadísticos aplicados, se contemplan los siguientes criterios:

a. **Media Aritmética**: para la cual se tuvieron en cuenta las diecisiete (17) empresas y se aplicó el promedio ponderado en forma directa.
b. **Media podada**: para la aplicación de esta medida no se tuvieron en cuenta los datos atípicos de cada extremo, es decir el más bajo y el más alto, tampoco los resultados en cero (0,00), negativos e indeterminados, razón por la cual se tuvieron en cuenta desde quince (15) y diez (10) empresas por cada indicador, con el fin de obtener un resultado objetivo, equilibrado y lineal.

c. **Mediana** se aplica en forma directa y corresponde a la posición central dentro de las diecisiete (17) empresas de la muestra.
d. **Mínimo:** promedia el valor del indicador de las diecisiete (17) empresas asignando el límite inferior, excluyendo los valores en cero (0,00), negativos e indeterminados.
e. **Máximo:** promedia el valor del indicador de las diecisiete (17) empresas asignando el límite superior.
f. **Promedio Ponderado:** este se aplica ponderando las anteriores medidas estadísticas por cada uno de los indicadores.

Para la asignación de los límites de cada requisito habilitante de orden financiero y organizacional se adopta la medida estadística del Mínimo, cuando el indicador sea cero y/o indeterminado procederá al siguiente ascendentemente a fin de dar libertad en la participación de las empresas que permita mayor pluralidad sin que ponga en riesgo el objeto del proceso y su cuantía para la ejecución fiscal del mismo.

3. Metodología y Resultado del Análisis del Indicador de orden Financiero Razón de endeudamiento

Partiendo del resultado obtenido del valor absoluto para cada empresa según metodología anterior, se procede a realizar un análisis individual por empresa mediante la aplicación del gráfico de **TALLOS Y HOJAS.** Para posteriormente aplicar las medidas estadísticas como lo son el promedio ponderado, la mediana, la desviación estándar, la media podada.

GRAFICO TALLO Y HOJAS

Muestra	Tallo	Hojas	Bajo, medio y alto nivel de endeudamiento	Mayoria de oferentes estan en este rango	Promedio de los 17 muestra poblacional	Mediana	Desviacion estandar	Media podada 15 items de 17	Desviacion estandar de la media podada	Razon de endeudamiento por encima o debajo de la media podada frente a la desviacion estandar	Valor local o Limite fijado adjudicador
10	0										
11	1	0150	10								
15	2	0458		20% a 26%	35	35	15	34	16	entre (34-16)=18 y (34+16+16)=66	66%
18	3	56	35								
20	4	258									
24	5	06									
25	6	25	65								
26	7										
35	8										
38	9										
42											
45											
48											
50											
58											
62											
65											

El gráfico anterior permite observar la concentración de los datos delimitando los valores más y menos frecuentes. Los menos frecuentes son los ubicados en los extremos del gráfico y corresponden a aquellos proveedores que tienen un bajo o alto índice de endeudamiento (10% y 65%); los más frecuentes corresponden a los proveedores que tienen un índice medio de endeudamiento entre el 20% y 26%, donde se encuentra la mayoría de los datos.

Basados en el análisis estadístico se define un índice de endeudamiento máximo de 66% o 0,66, teniendo en cuenta que es la media podada más dos veces la desviación estándar, siendo acorde con el sector económico y la naturaleza del proceso de contratación incluyendo los riesgos. la complejidad y valor del contrato.

4. Consolidado de los 5 indicadores de orden financiero y organizacional

Rentabilidad del patrimonio	Rentabilidad del activo	Indice liquidez	Razon de endeudamiento	Cobertura de Intereses
>=0,01	>=0,01	>=1,42	<=0,66	>=1,80

Conclusiones y Notas

De todo lo anterior, se concluye que los límites fijados a cada indicador son el resultado no solo de la aplicación de fórmulas financieras y estadísticas, sino que también respaldan los dos objetivos principales del Decreto 1082 de 2015, garantizar la pluralidad de oferentes y minimizar el riesgo para la Entidad.

Finalmente, es preciso indicar que se debe realizar la respectiva evaluación económica, basados en el concepto C – 028 de 2024 emitido por Colombia Compra Eficiente, *razón por la cual se procederá a evaluar con el último año fiscal actualizado.*

Atentamente,

Yenny Lorena Barragán Páez

Intendente **YENNY LORENA BARRAGÁN PÁEZ**
Analista de tesorería

Patrullero **DELFINA INES JARABA RODRÍGUEZ**
Auxiliar de presupuesto

ELABORÓ: PT. Delfina Jaraba Rodriguez
DILOF – GUPEG

REVISÓ: IT. Yenny Lorena Barragan Páez
DILOF – GITEG

Fecha elaboración: 24/03/2026
Ubicación, Y:\03. PRESUPUESTO2026\INDICADORES

Carrera 59 No. 26-21 CAN. Bogotá
Teléfonos 5159000 Ext 9811
dilof.gupeg1@policia.gov.co
www.policia.gov.co

INFORMACIÓN PÚBLICA

OFTIC GUDES

De:	OFTIC GUDES
Enviado el:	jueves, 27 de agosto de 2026 10:11 a.m.
Para:	'john.mantilla1515@correo.policia.gov.co'
Asunto:	solicitud certificado comercio exterior proceso FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE LA SOLUCIÓN SHAREPLEX

POLICÍA NACIONAL
Dirección General
Oficina de Tecnologías de la Información y las Comunicaciones
OFTIC

CORREO No. 0909 / OFTIC – GUDES 27/018/2026

Dios y Patria cordial saludo.

Respetuosamente me permito solicitar la posibilidad, se emita la certificación comercio exterior para la estructuración del estudio previo cuyo objeto es el" FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE LA SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL por un valor de ($2.029.125.000,00) INCLUIDO IVA y bajo la modalidad de SELECCIÓN ABREVIADA.

Agradezco su colaboración a la presente solicitud.

Atentamente,

Mayor
Luis Fernando Romero Roa
Jefe Grupo de Desarrollo y Operaciones TIC
3176467824

POLICÍA NACIONAL DE COLOMBIA
Oficina de Tecnologías de la Información y las Comunicaciones

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DIRECCIÓN LOGÍSTICA Y FINANCIERA
ÁREA DE CONTRATACIÓN

Bogotá D. C., 27 de agosto de 2026

CERTIFICACIÓN

En cumplimiento al numeral 8 del Artículo 2.2.1.1.2.1.1 del Decreto 1082 del 26 de mayo de 2015, modificado por el artículo 1 del Decreto 399 del 13 de abril de 2021, se certifica que una vez verificados en la página web de Colombia Compra Eficiente y en la del Ministerio de Comercio, Industria y Turismo, los Acuerdos Comerciales y Tratados de Libre Comercio (TLC), negociados por Colombia en los capítulos de contratación pública, se estableció que el proceso de **"FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL",** por un valor de **$2.029.125.000,00.**, **SI** está cubierto bajo las obligaciones de carácter internacional derivadas de los Acuerdos: ALIANZA DEL PACIFICO, CHILE, CANADÁ, COREA, COSTA RICA, ESTADOS AELC, ISRAEL, ESTADOS UNIDOS, MÉXICO, REINO UNIDO DE GRAN BRETAÑA, UNIÓN EUROPEA, E IRLANDA DEL NORTE, TRIANGULO NORTE, CAN; toda vez que:

a. La cuantía del proceso excede los umbrales establecidos en los acuerdos publicados.
b. La Policía Nacional se encuentra incluida en los listados de entidades cubiertas por los acuerdos.
c. Los bienes y/o servicios a contratar no se encuentran cubiertos bajo alguna exclusión de aplicabilidad o excepción.

De acuerdo a lo anterior, se deben tener en cuenta los principios y obligaciones en cuanto a la protección de los principios de derecho internacional, la publicidad de las contrataciones, el uso de medios electrónicos, las modalidades de contratación y la revisión de impugnaciones en la configuración de los documentos del proceso contractual.

Atentamente,

PRO03 **JOHN ALEXANDER MANTILLA**
Analista Contractual Dilof

** Excepción: Las convocatorias limitadas a Mipyme: Esta excepción sólo es aplicable en los casos en que la Entidad Estatal verifica las condiciones previstas en el artículo 2.2.1.2.4.2.2. del Decreto 1082 de 2015 para que una convocatoria sea limitada a Mipyme. Así, esta excepción no puede ser utilizada para excluir la cobertura del Acuerdo Comercial en el aviso de Convocatoria; los estudios y documentos previos; o, el borrador del pliego de condiciones.* (Colombia Compra Eficiente M-MACPC-14).

Carrera 59 26-21 CAN, Bogotá
Teléfonos 515 9550 – 515 9837
arcon.diraf @policia.gov.co
www.policia.gov.co

INFORMACIÓN PUBLICA

OFTIC GUDES

De: OFTIC GUDES
Enviado el: viernes, 28 de agosto de 2026 7:08 p. m.
Para: OFTIC GUSAP-SEG. CONTRATOS
Asunto: Remisión de documentación proyecto SHAREPLEX - GUDES para revisión CITI
Datos adjuntos: 1. PRESENTACION CITI SHARE PLEX.pptx; TI.-F-026 FORMATO CASO DE NEGOCIOS PROYECTO SHAREPLEX.docx

POLICÍA NACIONAL
Dirección General
Oficina de Tecnologías de la Información y las Comunicaciones
OFTIC

CORREO No. 0921 / OFTIC – GUDES 28/08/2026

Dios y Patria cordial saludo

Respetuosamente me permito remitir el formato presentación CITI y formato de caso de negocios, correspondientes al proceso "FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL", para su conocimiento, revisión y fines pertinentes ante esa entidad.

Atentamente,

Grupo
Despliegue y Operaciones de TIC
IP:(1) 515 9000 extensión 9437

POLICÍA NACIONAL DE COLOMBIA
Oficina de Tecnologías de la Información y las Comunicaciones

El contenido de este mensaje y sus anexos es propiedad de la POLICIA NACIONAL DE COLOMBIA con carácter confidencial y de uso exclusivo de su destinatario. Si usted no es el destinatario autorizado de la misma por favor abstenerse de divulgar, copiar, distribuir, retener o usar cualquier información contenida en este mensaje, por favor informe inmediatamente al remitente y elimine el mensaje original y sus anexos de su sistema. Cualquier acción que tome al respecto de la información contenida, por personas o entidades diferentes al propósito original de la misma es ilegal.

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
GRUPO DESPLIEGUE Y OPERACIONES DE TIC

DECLARACIÓN EXPRESA DEL ESTRUCTURADOR Y DUEÑO DE LA NECESIDAD DEL ESTUDIO PREVIO

Los estructuradores del estudio previo y dueño de la necesidad del objeto **FORTALECIMIENTO DE LA INFRAESTRUCTURA DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE SOLUCIÓN SHAREPLEX, PARA LA OPTIMIZACIÓN Y MIGRACIÓN DE LAS BASES DE DATOS DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL**, con el fin de dar cumplimiento al numeral 2.1 del acta precontractual de la Resolución 0090 del 15 de enero del 2018, que establecen las instancias de apoyo a los delegatarios de contratación en la Policía Nacional, manifestando que conoce la finalidad y las funciones, y que en atención a la Ley 80 de 1993, Ley 1150 de 2007 y sus decretos reglamentarios, declaran lo siguiente:

1. Que no tengo ningún interés particular y directo en la regulación, gestión, control o decisión dentro del presente proceso contractual, como tampoco lo tiene mi cónyuge compañero(a) permanente o alguno de mis parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho.

2. Que no tengo vinculaciones comerciales, ni laborales, ni de contratista, ni comisionista, con las firmas que hicieron parte del estudio de mercado, ni con los posibles proponentes; ni con socios de las mismas, ni con sus familiares dentro del cuarto grado de consanguinidad o segundo de afinidad.

3. Que no he sido contactado por socio, ni por representantes, ni por gestores a ningún titulo, con el fin de obtener ventaja en futura contratación.

4. Que todas las actuaciones y recomendaciones están encaminadas a garantizar que el proceso de convocatoria se realice en un marco de cumplimiento de los principios de transparencia, economía, responsabilidad, selección objetiva e imparcialidad absoluta.

5. No tengo participación o interés económico directo o por interpuesta persona en empresas dedicadas directa o indirectamente con el objeto de la presente contratación.

6. No aceptaré ni recibiré beneficios particulares de personas naturales o jurídicas por la venta y/o la prestación del servicio objeto de la presente contratación, directamente o a través de terceros.

7. Que, con las condiciones jurídicas, técnicas y económicas, así como los criterios de evaluación dados para la elaboración de los pliegos de condiciones de la presente contratación, no se está direccionando, ni favoreciendo a ningún contratista, permitiendo con ello la pluralidad de oferentes y no corresponden a una marca en particular.

Karen Useche L

Patrullero de policía **KAREN SOFIA USECHE LEYVA**
Estructurador Estudio Previo

Intendente **WILSON ALEJANDRO HENAO ARIAS**
Estructurador Estudio Previo

Intendente Jefe **JOHN EDISON TRIANA LOPEZ**
Estructurador Estudio Previo