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 específica, 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.

2.4.2. Modalidad Colocation Compartido

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.

Mantener en custodia los medios y dar cumplimiento a los procedimientos de borrado seguro o destrucción de medios en desuso.

Se debe garantizar que el backup se realice directamente al medio de almacenamiento externo.

2.4.3. Modalidad Infraestructura Propia

Con la finalidad de cumplir con lo dispuesto por la REGISTRADURÍA en las políticas de seguridad informática y garantizar la continuidad del servicio de autenticación biométrica en caso de presentarse fallas técnicas o siniestros no previstos en el plan de riegos del datacenter, se debe contemplar el respaldo de la información contenida en los LOGs y archivos de configuración de wallet.

El backup de los sistemas operativos, es responsabilidad del OAID.

Será responsabilidad del OAID el suministro de todos los recursos hardware, software y suministros tipo consumible, necesarios para la implementación y puesta en operación del servicio de backup, al igual que el recurso humano para la operación de este servicio.

Se debe garantizar que el backup se realice directamente a un medio de almacenamiento externo (disco, cinta) o en nuevas tecnologías garantizando en todo momento la disponibilidad, integridad y confidencialidad, para lo cual la REGISTRADURÍA deberá autorizar la implementación de dicha tecnología.

El OAID, debe cumplir estrictamente con los procedimientos para la custodia de los medios de backups y los procedimientos de borrado seguro o destrucción de los medios. Solo se permite el almacenamiento de los medios de backup dentro del DATACENTER autorizado por la REGISTRADURÍA.

2.5. Nivel de Soporte

El nivel de soporte debe ser 7x24x365

3. BALANCEADORES DE CARGA

La infraestructura tecnológica para este proyecto solo permite equipos físicos.

Los anchos de banda y tráfico de balanceadores de carga deberán crecer o decrecer simultáneamente con el crecimiento de los cotejos.

3.1. Servicio de balanceo de carga de servidores de acceso

Con la finalidad de garantizar la estabilidad de la plataforma, el operador del DATACENTER deberá suministrar el servicio de balanceo de carga en el acceso perimetral.

El operador del DATACENTER administrará los balanceadores de carga, pero toda regla de balanceo de carga será autorizada expresamente por la REGISTRADURIA.

3.2. Ancho de Banda

Las características mínimas que el operador del DATA CENTER y/o proveedor de comunicaciones deberá garantizar son:

- Ancho de banda dedicado mínimo disponible de 10 Mbps.
- Disponibilidad mínima del 99.982%
- Aplicación de protocolos de cifrado fuerte de datos a través de hardware dedicado para ello.

3.3. Nivel de Servicio

El nivel de soporte debe ser 7x24x365

4. FIREWALL ACCESO

La conectividad entre el datacenter del OAID y el datacenter de la REGISTRADURÍA, deberá realizarse mediante canales privados cifrados, en concordancia con las normas de seguridad previamente establecidas.

La conectividad entre el CLIENTE y el datacenter del OAID deberá realizarse mediante canales cifrados.

4.1. Servicio de firewall perimetral (Alta disponibilidad)

- Con la finalidad de cumplir con lo dispuesto por la REGISTRADURÍA, en relación a las políticas de seguridad de la información y garantizar el acceso seguro y controlado a la plataforma de identificación biométrica, el operador del DATACENTER suministrará el servicio de firewall perimetral.
- El operador del Data Center instalará, configurará y administrará el FIREWALL, bajo su cuenta y riesgo, pero toda regla de acceso y/o política de seguridad será autorizada expresamente por la REGISTRADURÍA.

- 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	Registraduría	Registraduría	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 replicación 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 licenciamiento 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 traves 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 RÉPLICA 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 Área 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 BIOMÉTRICA	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 (minimo) 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
Categoría 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 auditoria 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 disposicion del licenciamiento, software 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:

Item	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.	Sí
2	NUT	Cadena	12	NUT generado por el OAID.	Si
3	RequestId	Numérico	8	ID del LOG asociado a la búsqueda.	Sí
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