ACUERDO TÉCNICO DE ENTENDIMIENTO

Entre los suscritos a saber: EDUARDO JOSÉ TOUS DE LA OSSA identificado con cédula de ciudadanía No. 73.167.207 nombrado por resolución ORD-81117-00468 de 2024 y acta de posesión de fecha del 01 de febrero de 2024 en calidad de Jefe de la Unidad de Información de la Dirección de Información, Análisis y Reacción Inmediata – DIARI.- actuando en nombre y representación de la Dirección de Información Análisis y Reacción Inmediata de La CONTRALORÍA GENERAL DE LA REPÚBLICA quien en adelante se denominará "LA CONTRALORÍA" con NIT 899999067-2. De otra FÉLIX LEÓN MARTÍNEZ MARTÍN en calidad de Director General y Representante Legal de la Administradora de los Recursos del Sistema General de Seguridad Social en Salud ADRES con NIT. 901037916-1 quien en adelante se denominará "ADRES" o "la entidad" nombrado(a) mediante Decreto 1995 del 10 de octubre de 2025, posesionado el 12 de Octubre de 2022, mediante Acta emitida por el Ministerio de Salud y Protección Social, legalmente facultado por el numeral 2 del artículo 9 del Decreto No. 1429 de 2016, quien para efectos se denominara la ADRES, y quienes en conjunto se denominarán "las partes" suscriben el presente acuerdo mediante el cual se definen y desarrollan los procedimientos y requisitos necesarios para establecer y garantizar las condiciones de entrega de información a la Contraloría General de la República en el marco de sus facultades en ejercicio del control y vigilancia fiscal, cumpliendo con las formalidades, condiciones, requisitos, reserva, manejo, uso, salvaguarda y disposición final de la información.

I. FUNDAMENTOS DE DERECHO

1.1. El artículo 267 de la Constitución Política de Colombia establece que: *"La vigilancia y el control fiscal son una función pública que ejercerá la Contraloría General de la República, la cual vigila la gestión fiscal de la administración y de los particulares o entidades que manejen fondos o bienes públicos, en todos los niveles administrativos y respecto de todo tipo de recursos públicos. (…) El control fiscal se ejercerá en forma posterior y selectiva, y además podrá ser preventivo y concomitante, según sea necesario para garantizar la defensa y protección del patrimonio público. El control preventivo y concomitante no implicará coadministración y se realizará en tiempo real a través del seguimiento permanente de los ciclos, uso, ejecución, contratación e impacto de los recursos públicos, mediante el uso de tecnologías de la información, con la participación activa del control social y con la articulación del control interno. La ley regulará su ejercicio y los sistemas y principios aplicables para cada tipo de control. (…) La vigilancia de la gestión fiscal del Estado incluye el seguimiento permanente al recurso público, sin oponibilidad de reserva legal para el acceso a la información por parte de los órganos de control fiscal, y el control financiero, de gestión y de resultados, fundado en la eficiencia, la economía, la equidad, el desarrollo sostenible y el cumplimiento del principio de valoración de costos ambientales. La Contraloría General de la República tendrá competencia prevalente para ejercer control sobre la gestión de cualquier entidad territorial, de conformidad con lo que reglamente la ley (...)*

1.2. El artículo 268 de la Constitución Política de Colombia establece respecto de las funciones del Contralor General de la República: *1. Prescribir los métodos y la forma de rendir cuentas los responsables del manejo de fondos o bienes de la nación e indicar los criterios de evaluación financiera, operativa y de resultados que deberán seguirse.(…) 4. Exigir informes sobre su gestión fiscal a los empleados oficiales de cualquier orden y a toda persona o entidad pública o privada que administre fondos o bienes públicos.*

1.3. El artículo 136 de la ley 1955 de 2019 dispone que: "*La Contraloría General de la República para el cumplimiento de sus funciones, **tendrá acceso sin restricciones a los sistemas de información o bases de datos de las entidades públicas y privadas** que dispongan o administren recursos y/o ejerzan funciones públicas.*
***La reserva legal de información o documentos no le será oponible a la Contraloría General de la República** y se entenderá extendida exclusivamente para su uso en el marco de sus funciones constitucionales y legales".*
***PARÁGRAFO PRIMERO**. Cada entidad deberá disponer de lo necesario para garantizar **el suministro oportuno y en tiempo real de la información** requerida por la Contraloría General de la República.*

***PARÁGRAFO SEGUNDO**. Además de las sanciones ya previstas en la ley, la Contraloría General de la República **podrá suspender en el ejercicio del cargo**, hasta por el término de 180 días y con el fin de impulsar el correcto ejercicio del control fiscal, **a los servidores públicos que impidan o entorpezcan el acceso a la información**, previo agotamiento del procedimiento legal administrativo correspondiente, en el cual se garantizará el derecho al debido proceso. El Contralor General de la República reglamentará la materia".*

1.4. Que, el Decreto 2037 de 2019 mediante el cual se modifica el Decreto 267 del 2000: por el cual se establece la estructura orgánica de la Contraloría General de la República; dispone la creación de la Dirección de Información, Análisis y Reacción Inmediata – DIARI. Compuesta a su vez por la Unidad de Información, Unidad de Análisis y Unidad de Reacción Inmediata - las cuales, tendrán como funciones, entre otras *"1. Dirigir la formulación de políticas, planes, programas, proyectos y procedimientos relacionados con el acceso, acopio, custodia, seguridad, uso, análisis y aprovechamiento de datos e información, que contribuyan a incrementar la eficiencia, eficacia y resultados con valor agregado de las acciones de vigilancia y control fiscal (…) son funciones de la Unidad de Información: 2.Orientar, gestionar y controlar la adquisición, acceso, almacenamiento, seguridad, uso y generación de información y datos en la Contraloría General de la República, de conformidad con las políticas y protocolos que se adopten para el efecto. 3.Administrar y actualizar las bases de datos e información para el ejercicio de la función de vigilancia y control fiscal, de conformidad con las directrices y protocolos adoptados por la Dirección de Información, Análisis y Reacción Inmediata. 4. Proponer y participar en la formulación de las políticas de acceso, custodia, almacenamiento, aseguramiento, intercambio y uso de la información adquirida, obtenida o administrada por la Entidad, en coordinación con las dependencias competentes."*

1.5. Que el artículo 128 de la Ley 1474 de 2011 crea la Unidad de Cooperación Nacional e Internacional de Prevención, Investigación e Incautación de Bienes – UNCOPI, la cual tiene como función:
"implementación de tratados, acuerdos o convenios con entidades internacionales o nacionales para obtener el intercambio de información, pruebas y conocimientos por parte de personal experto o especializado que permita detectar bienes, cuentas, inversiones y otros activos de personas naturales o jurídicas investigadas o responsabilizadas por la causación de daños al patrimonio público para solicitar el decreto de medidas cautelares en el trámite de los procesos de responsabilidad fiscal y de cobro coactivo o en las acciones de repetición."

Que el artículo 103 de la ley 1474 de 2011 establece que, en las investigaciones, procesos de responsabilidad fiscal o de cobro coactivo, deberá ordenarse la investigación de bienes de las personas que aparezcan como posibles responsables fiscales.

1.6. Que, en cumplimiento de sus funciones legales, la UNCOPI ha desarrollado el Sistema de Búsqueda de Bienes – SBB como una herramienta tecnológica que permite agilizar la búsqueda patrimonial través de la integración y conexión de múltiples fuentes de información.

1.7. El Decreto 403 de 2020 introduce el control concomitante y preventivo en cabeza de la Dirección de Información, Análisis y Reacción Inmediata. En virtud del seguimiento permanente al recurso público, el acceso a la información es un mecanismo clave para el desarrollo de esta función. Particularmente el artículo 59 del Decreto determina la potestad de la Contraloría de requerir, conocer y examinar todos los datos e información sobre hechos, operaciones, actos, contratos, programas, proyectos o procesos en ejecución en los que se involucren recursos públicos.

1.8. El artículo 59 del Decreto 403 de 2020 determina que *"cada entidad deberá disponer lo necesario para garantizar el suministro oportuno y en tiempo real de la información requerida por la Contraloría General de la República, por conducto de la Dirección de Información, Análisis y Reacción Inmediata -DIARI-."*

1.9. El artículo 91 del Decreto 403 de 2020 establece que*: "El acceso a los sistemas de información o bases de datos será solicitado de manera formal a la entidad que los haya generado, los administre o por cualquier razón los detente, por parte del Auditor General de la República, el contralor territorial*

correspondiente, el Contralor General de la República, el Vicecontralor General o el Director de la Dirección de Información, Análisis y Reacción Inmediata -DIARI-, quienes serán los únicos facultados para ello. Dicha solicitud de acceso podrá efectuarse frente a una fracción o la totalidad de los sistemas de información o de las bases de datos, siempre que se pueda establecer una clara relación entre la información objeto de acceso y las funciones de vigilancia y control fiscal de la Contraloría General de la República, y la defensa y la protección del patrimonio público."

1.10. El artículo 92 del Decreto 403 de 2020 establece que: *"Los órganos de control fiscal acordarán con la entidad correspondiente los términos mediante los cuales se hará efectiva la interoperabilidad o el acceso a los sistemas de información o a las bases de datos solicitado, según las alternativas tecnológicas disponibles y con plena garantía de la seguridad y la integridad de la información, a través de la suscripción de protocolos técnicos o memorandos de entendimiento. Asimismo, dispone que: "una vez formalizada una solicitud de acceso a los sistemas de información o a las bases de datos, este deberá hacerse efectivo en los términos establecidos por los órganos de control fiscal o aquellos acordados con la entidad correspondiente que, en todo caso, deberá garantizar el acceso oportuno."*

1.11. El artículo 3 del Decreto 235 de 2010 dispone que, para formalizar el intercambio de información, las entidades públicas podrán emplear el mecanismo que consideren idóneo, tales como cronograma de entrega, planes de trabajo, protocolo o convenio, entre otros.

1.12. El artículo 93 del Decreto 403 de 2020 establece que: "Los órganos de control fiscal realizarán actividades de control pertinentes ante la evidencia de deficiencias importantes en la generación y disposición de datos e información pública por parte de los sujetos de control, con el fin de evaluar los procesos y productos relativos a los activos de información, determinar el grado de calidad de los mismos, emitir un concepto sobre la gestión de dichos activos y requerir un plan de remediación cuando sea el caso"

1.13. El artículo 94 del Decreto 403 de 2020 establece que: "La Dirección de Información, Análisis y Reacción Inmediata -DIARI- de la Contraloría General de la República será la responsable de custodiar y administrar los sistemas de información y las bases de datos a los que tenga acceso la Contraloría General de la República.

***PARÁGRAFO**. Los servidores públicos de la Dirección de Información, Análisis y Reacción Inmediata -DIARI- y en general todos los funcionarios y contratistas de la Contraloría General de la República, **tienen el deber de preservar la confidencialidad y reserva de toda la información a la que accedan en el ejercicio de sus funciones, so pena de las sanciones disciplinarias a las que haya lugar**.*

Sin perjuicio de lo anterior, los servidores públicos y contratistas que desempeñen sus funciones en la Dirección de Información, Análisis y Reacción Inmediata - DIARI- deberán suscribir actas o acuerdos de confidencialidad en las materias que determine la Contraloría General de la República".

1.14.** Que, la ley 2195 de 2022 establece en el parágrafo primero de su artículo 36 que **Las entidades públicas y privadas que generen, obtengan, adquieran, controlen, administren manejen o analicen información patrimonial o financiera sobre investigados o responsabilizados fiscales, deberán brindar de manera oportuna a la Contraloría General de la Republica la información que esta solicite en ejercicio de sus funciones, atribuciones y competencia, sin que sea oponible reserva alguna.

1.15. El artículo 2 del Decreto 235 de 2010 establece que: *"las entidades (...) deberán establecer mecanismos magnéticos, electrónicos o telemáticos para integrar, compartir y/o suministrar la información que por mandato legal se requiere, o permitir el acceso total dentro del marco de la Constitución y el derecho fundamental a la intimidad, a las bases de datos completas que requieran otras entidades para el ejercicio de sus funciones".*

1.16. Que la circular 09 del 01 de abril de 2020, expedida por el Contralor General de la República establece un "*plan de transición de acceso a fuentes de información de forma periódica a acceso en tiempo real".*

1.17. Que las Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI, establecen que *"La Dirección de Información, Análisis y Reacción Inmediata DIARI establece como compromiso preservar la confidencialidad, integridad y disponibilidad de los datos e información gestionados dentro de su operación, mediante un enfoque basado en riesgos, la adopción de estándares y mejores prácticas de la industria, la adopción de la estrategia de defensa en profundidad, el establecimiento de una cultura de seguridad de la información y el mantenimiento del proceso de mejora continua del Sistema de Gestión de Seguridad en materia de información."*

1.18. De otra parte, se define la naturaleza jurídica de la Administradora de los Recursos del Sistema General de Seguridad Social en Salud - ADRES así:

La Administradora de Recursos del Sistema General de Seguridad Social en Salud -ADRES, fue creada por la Ley 1753 de 2015 como una entidad adscrita al Ministerio de Salud y Protección Social; es un organismo de naturaleza especial del nivel descentralizado de la Rama Ejecutiva del orden nacional, con personería jurídica, autonomía administrativa y financiera, patrimonio independiente, asimilada a una Empresa Industrial y Comercial del Estado. La cual tiene como fin gestionar el flujo de recursos del Sistema General de Seguridad Social en Salud -SGSSS.

Siendo sus funciones principales:

1. Administrar los recursos del Sistema, de conformidad con lo previsto en los artículos 66 y 67 de la Ley 1753 de 2015 y las demás disposiciones que la reglamenten, modifiquen, adicionen o sustituyan.

2. Efectuar el reconocimiento y pago de las Unidades de Pago por Capitación y demás recursos del aseguramiento obligatorio en salud, de acuerdo con la reglamentación que expida el Gobierno Nacional o el Ministerio de Salud y Protección Social, en el marco de sus competencias.

3. Realizar los pagos, efectuar giros directos a los prestadores de servicios de salud y proveedores de tecnologías en salud, de acuerdo con lo autorizado por el beneficiario de los recursos, y adelantar las transferencias que correspondan a los diferentes agentes del Sistema.

4. Adelantar las verificaciones para el reconocimiento y pago por los distintos conceptos, que aseguren el buen uso y control de los recursos.

5. Administrar la información propia de sus operaciones* de acuerdo con la reglamentación expedida para el efecto por el Ministerio de Salud y Protección Social, en los términos señalados en las Leyes 100 de 1993 y 1438 de 201 1 y en el Decreto Ley 4107 de 2011 y tas demás disposiciones que la reglamenten, modifiquen, adicionen o sustituyan.

De acuerdo con lo expresado por Colombia Compra Eficiente, los memorandos o acuerdos de entendimiento son instrumentos simplificados en los cuales se incluyen intenciones, compromisos, aspiraciones, propósitos o se desarrollan instrumentos preexistentes. En los mismos no se contemplan obligaciones de comportamiento reales, ni términos imperativos u obligacionales, sino más bien clausulas programáticas que suelen contener simples exhortaciones o declaraciones de intención. Las normas que regulan los memorandos de entendimiento o cartas de intención corresponden a aquellas que de manera general le asignan las funciones a las Entidades Estatales. En este orden de ideas, este tipo de acuerdos no tienen el alcance de contrato estatal, en la medida en que no generan obligaciones para quienes lo suscriben, en consecuencia, no están sujetos a la normativa del Sistema de Compra Pública.

Que, de acuerdo con lo señalado anteriormente y en virtud del principio de coordinación y colaboración, las autoridades administrativas deben garantizar la armonía en el ejercicio de sus respectivas funciones con el fin de lograr los fines y cometidos estatales.

Por otra parte, de acuerdo con la Guía para Caracterización de Usuarios de las Entidades Públicas del Ministerio de Tecnologías de la Información y las Comunicaciones, el enunciado proceso para la caracterización de usuarios. El citado documento determina la necesidad de caracterizar usuarios en tanto que "una constante de las entidades del Estado es la diversidad de usuarios. Cuando una entidad reconoce esta diversidad, e identifica las características, actitudes y preferencias que diferencian a sus usuarios, tiene la oportunidad de ajustar sus

actividades, decisiones y servicios, para responder satisfactoriamente el mayor número de requerimientos, obtener su retroalimentación y/o lograr participación en el logro de los objetivos de la entidad.

II. OBJETIVO

Establecer el tipo de información, canal de comunicación, mecanismos de control de seguridad y demás aspectos técnicos que deben adoptarse para la transferencia y entrega de información a la CGR en el marco del presente documento técnico de entendimiento.

III. DEFINICIONES

Con el fin de facilitar la interpretación del presente anexo técnico, a continuación, se definen algunos conceptos básicos:

3.1 Acuerdo de confidencialidad: acuerdo en el cual se adquieren compromisos de no divulgación respecto de información de carácter confidencial o de reserva de conformidad con lo dispuesto en el acuerdo y en las leyes que regulan la materia de protección de datos personales.

3.2 Amenazas: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

3.3 Amenaza cibernética: la aparición de una situación potencial donde un agente tiene la capacidad de generar un ataque realizado por actores maliciosos contra la Entidad, población, el territorio y la organización política del estado.

3.4 Autenticación: es el mecanismo de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

3.5 Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

3.6 Canal de comunicación: se refiere a un medio de transmisión físico, como un cable o a una conexión lógica a través de un medio multiplexado, por ejemplo, un canal de redes informáticas que se utiliza para transmitir datos desde un emisor (quien transfiere) a un receptor (quien recibe).

3.7 Ciberseguridad: capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

3.8 Ciberespacio: se refiere a un entorno no físico creado por equipos de cómputo unidos mediante una red para interoperar entre sí.

3.9 Cifrado: proceso por el que la información se convierte en un código secreto o ilegible, conocido como "texto cifrado", para protegerla de accesos no autorizados. Este proceso de transformación se basa en un algoritmo matemático y una clave que se utiliza para realizar la codificación y, posteriormente, la decodificación de los datos.

3.10 Confidencialidad: asegurar que la información solo sea accedida, conocida y/o divulgada por los usuarios autorizados.

3.11 Custodio de la información: responsable de resguardar y proteger la información, datos o activos digitales confiados a su cuidado.

3.12 Disponibilidad: esta propiedad está destinada a garantizar el uso de los activos de información en el momento requerido, según [ISO/IEC 13335-1: 2004): Característica/ propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

3.13 Evento de seguridad de la información: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

3.14 Evento tecnológico: hace referencia a un suceso inesperado o un problema que ocurre en el ámbito de la tecnología, la informática o la ciberseguridad. Estos eventos pueden medirse por su nivel de gravedad y alcance o impacto, desde problemas menores como la caída de un servidor que ocasionan indisponibilidad en los servicios hasta eventos graves como el aprovechamiento de vulnerabilidades derivadas en ataques cibernéticos.

3.15 Gestión de claves: son controles implementados mediante definición de políticas para su generación, uso, protección, renovación o destrucción de claves criptográficas.

3.16 Hash: un valor hash (llamado suma de comprobación) es un valor de cadena fruto del cálculo de un algoritmo matemático que transforma cualquier bloque de datos en una nueva serie de datos compuesto por un código alfanumérico hexadecimal con una longitud fija y especifica. Es una huella digital que identifica el contenido de un fichero en una secuencia de caracteres, permitiendo reproducir el proceso de generación de hash para comparar el resultado y garantizar la integridad del archivo transferido.

3.17 Impacto: el costo o consecuencia de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros - p.ej., pérdida de reputación, implicaciones legales, etc.

3.18 Incidente de seguridad: es cualquier evento de origen interno o externo que pueda comprometer la integridad, confidencialidad o disponibilidad de sistemas, redes, activos o datos de la organización. Se considera que un incidente es la materialización de una amenaza que pone en peligro la seguridad de la información.

3.19 Información: la información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, impresa o escrita en papel, almacenada electrónicamente (digital), transmitida por correo o por medios electrónicos, se puede mostrar en videos o exponer oralmente en conversaciones.

3.20 Infraestructura tecnológica: conjunto de equipos, programas y comunicaciones mediante los cuales se realiza el registro, consulta y acceso a la información de los datos que se encuentran almacenados en una base de datos o repositorio. Teniendo en cuenta las consideraciones de disponibilidad y seguridad, se realizará el acceso a la información mediante el uso de los servicios proporcionados por la red gubernamental autorizada, la cual provee a las entidades del Estado enlaces de comunicación con niveles apropiados de calidad de servicio, para que los sistemas de información puedan interactuar de manera óptima.

3.21 Información pública: es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal de conformidad con lo dispuesto por la ley 1712 del 2014 o demás normas que modifiquen o complementen la materia.

3.22 Información pública clasificada: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014 o demás normas posteriores que modifiquen o complementen la materia.

3.23 Información pública reservada: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014 o demás normas posteriores que modifiquen o complementen la materia.

3.24 Información privada: es aquella que se encuentra en el ámbito propio del sujeto a quien le incumbe y sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones.

3.25 Información semiprivada: se refiere a los datos que versan sobre información personal o impersonal que no está comprendida como información pública, reservada o íntima pero que para su acceso y conocimiento presenta un grado mínimo de limitación, de tal forma que sólo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Es el caso de los datos relativos a las relaciones con las entidades de la seguridad social y al comportamiento financiero de las personas. Administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Es el caso de los datos relativos a las relaciones con las entidades de la seguridad social y al comportamiento financiero de las personas.

3.26 Información sensible: información que afecta la intimidad de las personas o cuyo uso indebido puede generar discriminación.

3.27 Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

3.28 Interoperabilidad: forma de intercambiar información entre plataformas tecnológicas, sistemas de información o aplicaciones, eficiente y continua, para lo que se utilizan estándares para enviar y recibir datos mediante protocolos de seguridad, sin importar las tecnologías existentes de quienes participen. Según el marco de interoperabilidad definida por MINTIC, es “la capacidad de las organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio para interactuar hacia objetivos mutuamente beneficiosos, con el propósito de facilitar la entrega de servicios digitales a ciudadanos, empresas y a otras entidades, mediante el intercambio de datos entre sus sistemas TIC”.

3.29 ISP: proveedor de servicios de internet.

3.30 Logs: registros son archivos de texto plano donde se almacenan cronológicamente las actividades realizadas en un sistema informático, aplicación y/o dispositivo que permite realizar procesos de monitoreo, seguimiento y análisis de las actividades realizadas por un usuario.

3.31 Mecanismo de control de seguridad: conjunto de elementos, procesos o herramientas que se utilizan para fortalecer la confidencialidad, la integridad y la disponibilidad de un sistema informático, redes, activos o datos

3.32 No repudio: se refiere a la capacidad de demostrar de manera inequívoca que una persona o entidad no puede negar la autenticidad de su participación en una transacción, comunicación electrónica o recepción de información.

3.33 Perfil de acceso: mecanismo de control de seguridad mediante el cual se definen los permisos de acceso de usuario o grupo de usuarios a un recurso o sistema de información.

3.34 Plataforma tecnológica: conjunto de elementos tecnológicos de hardware, software y comunicaciones que se utilizan como base y están destinados al procesamiento de información con características específicas.

3.35 Privilegio mínimo: es una estrategia para proteger sistemas, redes, datos y activos al limitar los permisos de acceso otorgados a usuarios, sistemas y programas a los necesarios para realizar actividades y funciones específicas, para reducir el riesgo de exposición a amenazas y mantener un entorno seguro con mayor nivel.

3.36 Propietario del activo de información: es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso institucional se clasifican adecuadamente. Además, debe controlar la gestión de la información, incluyendo su seguridad; debe definir y revisar periódicamente las restricciones y clasificaciones del acceso, y gestionar los riesgos asociados a los activos de información, según su nivel de severidad.

3.37 Responsable de la información: funcionario o unidad organizacional que tiene responsabilidad aprobada por el propietario de la información, para el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información.

3.38 Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000). / efecto de la incertidumbre sobre los objetivos. (ISO 31000)

3.39 Responsable del tratamiento: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la información y su tratamiento. (Ley 1581 de 2012, art 3).

3.40 Secure File Transfer Protocol (SFTP): protocolo seguro de transferencia de archivos, el cual brinda seguridad al cifrar la sesión de conexión establecida para el intercambio de archivos entre un cliente y un servidor mediante una red como por ejemplo internet.

3.41 Seguridad de la Información: es la propiedad que asegura que los recursos de un sistema de información sean utilizados de la manera correcta y que su acceso sólo sea posible a las personas que se encuentren autorizadas, preservando la Integridad, Confidencialidad y Disponibilidad de los activos de información.

3.42 Transferencia de datos: tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

3.43 Usuario: será aquella persona que para ejercer una funcionalidad definida necesita acceder mediante un equipo de cómputo con un perfil y privilegios definidos a un sistema, un recurso o una plataforma para el normal desempeño de sus actividades y que le permita interactuar con los datos e información.

3.44 Vista materializada: el resultado de la consulta se almacena en una tabla caché real, que será actualizada de forma periódica a partir de las tablas originales. Esto proporciona un acceso mucho más eficiente, a costa de un incremento en el tamaño de la base de datos y a una posible falta de sincronía, es decir, que los datos de la vista pueden estar potencialmente desfasados con respecto a los datos reales. Es una solución muy utilizada en entornos de almacenes de datos (datawarehousing), donde el acceso frecuente a las tablas básicas resulta demasiado costoso.

3.45 VPN Site to Site: red virtual privada que permite conectar dos redes ubicadas geográficamente en diferentes sitios a través de una red pública como internet de forma segura utilizando el protocolo IPSec (Internet Protocol Security) el cual agrega mecanismos de cifrado y autenticación al canal de comunicación.

3.46 Vulnerabilidad: debilidad de un sistema, activo o control que pueda ser explotado por una o más amenazas.

3.47 Web Service: es un servicio a través de internet el cual mediante una interfaz permite la interoperabilidad entre maquinas o aplicaciones independientemente de su plataforma; generalmente, la interacción está basada en él envió de solicitudes y respuestas para el intercambio de datos entre un cliente y un servidor.

IV. CONDICIONES GENERALES DE PROTECCIÓN, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

La información suministrada será utilizada en el marco de sus competencias por la Dirección de Información, Análisis y Reacción Inmediata- DIARI y la Unidad de Cooperación Nacional, Internacional de Prevención, Investigación e Incautación de Bienes - UNCOPI.

De conformidad con lo dispuesto por el artículo 59 del Decreto 403 de 2020 la Contraloría General de la República podrá requerir, conocer y examinar todos los datos e información sobre hechos, operaciones, actos, contratos, programas y proyectos en ejecución que involucren recursos públicos sin oponibilidad de reserva legal. Para lo cual se apoya de la gestión inteligente de la información; entidad como el uso eficiente de todas las capacidades tecnológicas disponibles, inteligencia artificial, analítica y minería de datos, análisis predictivo y prospectivo, entre otros; para la determinación anticipada de eventos o malas prácticas con probabilidad significativa de ocurrencia, a través de la Dirección de Información, Análisis y Reacción Inmediata – DIARI.

Asimismo, el artículo 128 de la Ley 1474 de 2011 determinan que la Contraloría General de la República debe ordenar la investigación de bienes con el propósito de decretar medidas cautelares contra los presuntos responsables fiscales y en los procesos de cobro coactivo. De igual manera, se establece que la UNCOPI tendrá como funciones la detección de bienes, cuentas, inversiones y demás activos de personas naturales o jurídicas, que sean investigadas o responsabilizadas fiscalmente. Por lo anterior, se implementó el Sistema de Búsqueda Integrado de Bienes, el cual se nutre de diversas fuentes de información provenientes de los sujetos de control con el propósito de garantizar la eficacia del control fiscal.

4.1 El canal de comunicación por el que se realizará el acceso y/o transferencia de la información deberá ofrecer un uso adecuado y eficaz, así como los mecanismos de control de seguridad para proteger la confidencialidad, la autenticidad y la integridad de la información clasificada y/o reservada y/o de datos sensibles.

4.2 Las partes deberán ceñirse a las directrices internas de cada entidad y a la normatividad vigente en seguridad de la información.

4.3 Las partes garantizarán mediante mecanismos como *logs* de auditoría, la trazabilidad del consumo o notificación a correos electrónicos institucionales cuando el servicio así lo requiera.

4.4 Las partes deberán implementar los mecanismos de controles de seguridad necesarios para restringir el acceso a la información sólo a aquellos servidores con cargos o roles establecidos por aquellos servidores con cargos y roles autorizados como responsables de la custodia de la información para garantizar la confidencialidad de la misma.

4.5 La entidad deberá implementar los mecanismos de controles de seguridad necesarios para garantizar la integridad de la información en la infraestructura utilizada para transferir y entregar la información a LA CONTRALORIA.

4.6 LA CONTRALORIA debe implementar los mecanismos tecnológicos necesarios para garantizar la confidencialidad e integridad de la información una vez obtenida la información.

4.7 La ADRES establece las condiciones en conjunto con LA CONTRALORIA para configurar un usuario de consulta que le otorga a dicha entidad, acceso a la información registrada en este acuerdo.

4.8 LA CONTRALORIA se compromete a asegurar que la información que se accede, solo será utilizada para los fines y propósitos de la vigilancia y control fiscal y a la vez se compromete a no entregar, ni revelar esta información a terceros sin previo consentimiento por escrito de cada una de las partes

4.9 En lo respectivo a la protección de datos personales, la CONTRALORÍA contrae las obligaciones como responsable del tratamiento de la información que se determinan en el presente documento técnico de entendimiento.

4.10 LA CONTRALORIA como entidad usuaria de la información que contiene datos personales, se obliga a cumplir con las normas que conforman en su integridad el régimen general de protección de datos personales: Ley 1266 de 2008 modificada por la Ley 2157 de 2021, Ley estatutaria 1581 de 2012; así como aquellas normas relativas al derecho de habeas data, dentro de las que se incluyen la Ley 1712 de 2014, Ley 1755 de 2015 y demás disposiciones concordantes.

4.11 En observancia de los principios, deberes y obligaciones legales en el marco del uso de información que se llevará a cabo en virtud del documento técnico de entendimiento suscrito, la CONTRALORIA adquiere conjuntamente el rol de responsable del tratamiento de los datos personales de los sujetos de la base de datos de la ADRES. En mérito de lo expuesto, serán principios rectores en el tratamiento de la información, los siguientes:

- **Finalidad:** La utilización de la información de ADRES será tratada exclusivamente para el ejercicio de las competencias funcionales y legales de inspección, vigilancia y control fiscal de la CONTRALORIA orientadas particularmente a establecer la titularidad de presuntos responsables fiscales como propietarios de derechos patrimoniales susceptibles de ser objeto de medidas cautelares en el marco de los procesos de responsabilidad fiscal y cobro coactivo.

- **Autorización:** La ADRES declara que la información a consultar es de tipo público y autoriza a la CONTRALORIA para que haga tratamiento de los datos personales transferidos, para las finalidades propias de la ejecución del presente Protocolo Técnico. No obstante, si la petición registral establece una confidencialidad, la ADRES se compromete a mantenerla con la referencia contenida.

  Por su parte, LA CONTRALORIA declara, reconoce y garantiza que el tratamiento que lleve a cabo sobre los Datos Personales transferidos por la ADRES, lo convierte a su vez en responsable de tales datos.

- **Seguridad:** La información sujeta de tratamiento, se manejará con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Para ello, LA CONTRALORIA da especial aplicación y cumplimiento de los principios de privacidad y protección de datos personales, adoptando un Programa Integral de Gestión de Datos Personales y un Sistema de Administración de Riesgos Asociados al Tratamiento de Datos, los cuales hacen parte integral del presente documento.
  En línea con lo anterior, en el presente Protocolo Técnico se encuentran detalladas las medidas y procedimientos que buscan garantizar la seguridad en la consulta y descarga de la información, siguiendo los protocolos de seguridad y protección de datos requeridos para tales efectos y bajo la orientación de la Guía para la Implementación del Principio de Responsabilidad Demostrada emitida por la Superintendencia de Industria y Comercio, autoridad encargada de la protección de datos personales en el país.

- **Confidencialidad:** En virtud de la inoponibilidad de la reserva, atendiendo los principios y disposiciones contenidas en la Ley 1581 de 2012, LA CONTRALORIA se compromete a garantizar la reserva de la información transferida, incluyendo aquella catalogada por datos personales de carácter público, semiprivado y privado de los ciudadanos que se consultará y utilizará de la base de datos de la ADRES, en virtud del Protocolo Técnico.

  Con motivo de lo anterior, LA CONTRALORIA suscribirá acuerdos de confidencialidad con los funcionarios y contratistas facultados para conocer la información objeto del presente acuerdo, en aras de salvaguardar la reserva de esta.

  Aunado a lo expuesto y en adición a los acuerdos de confidencialidad individuales que deberán ser celebrados por los funcionarios de LA CONTRALORIA, este último ente de control y la ADRES suscribirán un ACUERDO DE CONFIDENCIALIDAD el cual hará parte integral de este anexo en aras de garantizar la seguridad y confidencialidad en la consulta.

4.12 Debido a que la ADRES se responsabiliza únicamente por otorgar el acceso a la información solicitada por LA CONTRALORIA, LA CONTRALORIA será responsable del tratamiento de la información y deberá seguir los deberes que dicha posición conlleva de conformidad con lo establecido en la Ley 1581 de 2012. Al respecto, la jurisprudencia constitucional ha sostenido que, una vez asumido el rol de responsable, la entidad deberá

garantizar los derechos fundamentales del titular de la información los cuales tienen su origen en el derecho de *habeas data* contenido en el artículo 15 de la Constitución Política. De este modo, le corresponderá a LA CONTRALORIA informar a los titulares de manera clara y expresa el tratamiento al cual serán sometidos sus datos y la finalidad del mismo. Esto se hará en observancia de los procedimientos y protocolos definidos para tal fin por la entidad.

- **Legibilidad**: De conformidad con el formato existente en las fuentes de datos de Función Pública para los usuarios que deben acceder a los datos según condiciones de seguridad definidas entre las partes, en este mismo documento.

- **Completitud**: Respecto a lo que sea solicitado y existente en las fuentes de datos acordadas.

- **Precisión**: En cuanto los datos reflejan lo ingresado por el titular en los sistemas de información de Función Pública.

- **Validez**: Los datos se ajustan al formato, tipo y rango existente en las fuentes de información de Función Pública.

4.13 Las partes definirán la periodicidad en que se entregarán las fuentes de la información cuando aplique, según el medio de transferencia.

V. CONDICIONES TÉCNICAS

5.1 Canal de comunicación de la información

Para el acceso de LA CONTRALORIA a la información de las bases de datos de la ADRES del que trata el numeral anterior, LA ADRES y LA CONTRALORIA acuerdan lo siguiente:

El canal definido para la disposición de la información solicitada es:

Medio de intercambio	Periodicidad de consumo
VPN site to site	Canal habilitado para consulta de información en tiempo real de la base de datos de la entidad en los términos acordados en el documento de acuerdo técnico de entendimiento.
SFTP - CGR	El SFTP es el canal habilitado para transmisión de fuentes de información de forma ocasional diferentes a las contempladas en el documento técnico de entendimiento.

5.1.2. Canal y protocolos de seguridad en la comunicación

De conformidad con lo acordado en el presente documento, el acceso a la información deberá realizarse cumpliendo con las políticas, protocolos y procedimientos de seguridad tecnológica y normativa vigente aplicable a cada entidad.

Para establecer la comunicación segura entre las partes se utilizará los siguientes elementos:

VPN: Se utilizará una red virtual privada VPN Site to Site, por medio de la cual se accederá a la vista de las consultas y tablas dispuesta por la ADRES, asociada a la fuente o fuentes de información solicitadas.

Para establecer y mantener la configuración de la VPN Site to Site entre la CONTRALORIA y la ADRES, se agendarán reuniones técnicas requeridas.

II. INFORMACION PARA REQUISITOS DE VPN Ipsec		
Parametros del VPN Device)	**INFORMACION CONTRALORIA**	**INFORMACION ADRES**
VPN Device IP Address	182.116.129.10	201.234.182.164
VPN Device Version	Fortigate 1500D	Fortinet Fortigate-600E V6.2.3 build1066 (GA)
VPN – Fase 1 (IKE)	**INFORMACION CONTRALORIA**	**INFORMACION SEDE Tercero**
Encryption Algorithm	AES-256	AES-256
Hashing Algorithm	SHA256 SHA512	SHA256 SHA512
Authentication Method	Preshared-key	Preshared-key
Diffie-Hellman group	2	2
Key Lifetime	28800	28800
Encryption Method	IKE	IKE
VPN – Fase 2 (IPSec)	**INFORMACION CONTRALORIA**	**INFORMACION SEDE Tercero**
Encryption Algorithm	AES-256	AES-256
Authentication Algorithm	SHA256 SHA512	SHA256 SHA512
Lifetime	3600	3600
Use perfect Forward Secrecy	No	No
Autokey Keep Alive	Si	Si
Dominio de la VPN	**INFORMACION CONTRALORIA**	**INFORMACION SEDE Tercero**
Source/Destination Servers		172.21.242.243
Ports	especificar los puerto de conexión a la base de datos o aplicativo	1441 (SQL) ICMP
LA VPN ES BIDIRECIONAL:	SI	NO

SFTP: El servicio SFTP dispuesto por la CGR será el medio alternativo para disposición de información cuando la CGR realice requerimientos esporádicos o diferentes a lo contemplado en el presente documento técnico de entendimiento. A la fecha de la suscripción del presente documento técnico de entendimiento, ADRES cuenta con credenciales de acceso al SFTP y se identifica con el nemotécnico "AdReS".

Al momento de disponer la información en el SFTP de la CGR (de acuerdo con los requerimientos), se debe incluir el archivo resultante del proceso de generación de los valores hash el cual dispone en la carpeta definida en los lineamientos los cuales se detallan en el enlace https://www.cas.contraloria.gov.co/lineamientos. Es importante recordar que los algoritmos acordados para su generación deberán corresponder a las funciones hash MD5, SHA1, SHA 256 y SHA 512.

5.1.3. Datos o información que se suministra.

La información suministrada por parte de la entidad se encuentra documentada, consolidada y detallada en el título *Descripción de las fuentes de información (Diccionarios de datos)*" del presente documento.

Clasificación de la información (seleccione los tipos que aplican)

Tipo de información	
Información Pública	X
Información pública clasificada	X
Información pública reservada	
Información Semiprivada	X
Información Privada	X
Información sensible	X

Nota: Las fuentes de información indicadas en la presente sección, pueden ser modificadas o ampliadas lo que implicará la actualización del documento técnico de entendimiento entre las partes (según sea el caso). Este dependerá del análisis e información que requiera realizar en sus funciones LA CONTRALORIA.

5.1.4 Periodicidad y fecha de disposición de las fuentes de información

La información suministrada por parte de la entidad se dispondrá en la periodicidad detallada a continuación:

Fuente de Información	Nombre Tabla	Nombre de la Vista	Descripción	Periodicidad / Fecha de Disposición	Medio
Información Circular 09	BDUA Régimen Contributivo	BDUA_RC_AAAAMMDD	Base de Datos Única de Afiliados al Régimen Contributivo	La periodicidad es mensual, los primeros diez (10) días mes vencido.	VPN
	BDUA Régimen Subsidiado	BDUA_RS_AAAAMMDD	Base de Datos Única de Afiliados al Régimen Subsidiado		
	BDEX	BDEX_AAAAMMDD	Base de Datos Única de Afiliados pertenecientes al Régimen de Excepción y Especial		
	HAC_4023	HAC_4023_AAAAMMDD	Datos Proceso de Compensación		
	HAPS	HAPS_AAAAMMDD	Datos Proceso Liquidación Mensual de Afiliados (LMA) – Régimen Subsidiado		
	HAPS_RESTITUCIONES	HAPS_RESTITUCIONES_AAAAMMDD	Datos Proceso de Restituciones - Régimen Subsidiado		
	Recobros	Recobros_MYT01_AAAAMMDD	Datos Proceso Recobros que corresponde al anexo técnico a través del cual se reportan los servicios y tecnologías no financiados por la UPC, que fueron prescritos por un profesional de la salud a través de MIPRES o autorizados por un Comité Técnico Científico, si aplica.		
	Recobros	Recobros_MYT02_AAAAMMDD	Datos Proceso Recobros que corresponde al anexo técnico a través del cual se reportan los servicios y tecnologías no financiados por la UPC, que fueron ordenados por un fallo de tutela.		
	Reporte de cuentas maestras de recaudo	CuentamaestraAAAAMM	Estructuras de datos con la cual la ADRES desagrega el detalle de los registros compensados y no compensados para el periodo objeto de reporte.		
	Descuentos Nueva Estructura	CGR_Descuentos_MM_AAAA_Nueva_Estructura	Información Complemento de la Circular 09 – Descuentos del proceso LMA		
	información Adicional	CGR_InformacionAdicional_MM_AAA	Información Complemento de la Circular 09 – Información adicional proceso LMA		
Información Reclamación No SOAT, Reclamaciones FURIPS, FURIPS2, FURTRAN y FURPEN	ECAT_FURIPS1	ECAT_FURIPS1_AAAAMMDD	Formulario único de certificación del censo de víctimas y eventos catastróficos		
	ECAT_FURIPS2	ECAT_FURIPS2_AAAAMMDD	Datos formulario único de reclamación de las instituciones prestadoras de servicios de salud por servicios prestados a víctimas de eventos catastróficos y accidentes de tránsito		
	ECAT_FURPEN	ECAT_FURPEN_AAAAMMDD	Datos formulario único de reclamación de indemnizaciones por accidentes de tránsito y eventos catastróficos		
	ECAT_FURTRAN	ECAT_FURTRAN_AAAAMMDD	Datos formulario único de reclamación de gastos de transporte y movilización de víctimas		
Información Pólizas y Siniestros	CGR_SINIESTROS_2018_2025	2025EE0091463_Siniestros	Información de pólizas y sinestros viales	La periodicidad es mensual,	VPN

Fuente de Información	Nombre Tabla	Nombre de la Vista	Descripción	Periodicidad / Fecha de Disposición	Medio
	CGR_POLIZAS_2018_2025	2025EE0091463_Polizas		los primeros veinte (20) días mes vencido.	
Información reintegro RC y RS	REINTEGRO Régimen Contributivo	REINTEGRO_RC_AAAAMMDD_AAAAMMDD	Datos Procedimiento de Reintegro de Recursos relacionados con los valores reintegrados por las EPS del régimen contributivo y subsidiado, en las etapas del procedimiento de reintegro de recursos de UPC apropiados y/o reconocidos sin justa causa - Régimen Contributivo	La periodicidad es Semestral, los primeros diez (10) días mes vencido.	VPN
	REINTEGRO Régimen Subsidiado	REINTEGRO_RS_AAAAMMDD_AAAAMMDD	Datos Procedimiento de Reintegro de Recursos relacionados con los valores reintegrados por las EPS del régimen contributivo y subsidiado, en las etapas del procedimiento de reintegro de recursos de UPC apropiados y/o reconocidos sin justa causa - Régimen Subsidiado		
Información Cuentas Financieras	INFORMACION_ADRES - CUENTAS FINANCIERAS	2023ee0151990_cuentas_financieras	Datos de reporte de giro realizado por la ADRES a las EPS del régimen subsidiado. Contiene la liquidación de los Presupuestos Máximos establecidos por la Ley 1955 de 2019, que denota el presupuesto anual con el se garantiza la prestación de los servicios y tecnologías en salud no financiados con la UPC a sus afiliados.	La periodicidad es Semestral, los primeros diez (10) días mes vencido.	VPN
Información Procesos de repetición	PROCESOS DE REPETICIÓN	PRE1_AAAAMMDD	Datos de los Procesos de repetición en contra de los conductores y/o propietarios por transitar sin SOAT (identificación del deudor) hasta mayo 25 2022	La periodicidad es Semestral, los primeros veinte (20) días hábiles del siguiente mes de finalizado el semestre (p.e. Febrero 27 2026- Agosto 27 2026)	VPN
	PROCESOS DE REPETICIÓN	PRE2_AAAAMMDD	Datos de los Procesos de repetición en contra de los conductores y/o propietarios por transitar sin SOAT (Actos administrativos realizados) desde mayo 26 2022		
	PROCESOS DE REPETICIÓN	Resumen_PRE1_AAAAMMDD	Resumen gestión hasta mayo 25 2022		
	PROCESOS DE REPETICIÓN	Resumen_PRE2_AAAAMMDD	Resumen gestión desde mayo 26 2022		
Giro Directo	Contributivo	GDCONTRIBUTIVO_AAAAMM	Información giro directo régimen contrbutivo	La periodicidad es mensual, los primeros diez (10) días mes vencido.	VPN
	Subsidiado	GDSUBSIDIADO_AAAAMM	Información giro directo régimen subsidiado		
	Presupuestos Máximos	GDPRESUPUESTOMAXIMO_AAAAMM	Información giro directo mecanismo de presupuestos máximos		

* AAAAMMDD Corresponde a la fecha de corte de la información. Para los Reintegros y las Reclamaciones se define la fecha inicial y fecha final de la información entregada.

Se recomienda a las entidades permanecer atentos y consultar regularmente la vigencia de los accesos otorgados entre las partes.

ADRES habilitó un servicio de base de datos para permitir el acceso a la CGR a las vistas materializadas asociadas a las fuentes de datos definidos en el alcance de este documento. Para tal efecto, ADRES entregó un usuario y contraseña a la CGR.

Debido a la sensibilidad de la información, los usuarios y contraseñas de acceso son manejados por el oficial de seguridad de la Contraloría General de la República y son enviados únicamente al correo de él o al correo del funcionario encargado de las Entidades del Sector Salud de la Unidad de Información de la Dirección de Información, Análisis y Reacción Inmediata – DIARI.

Una vez dispuesta la información por parte de la ADRES deberá informar al correo institucional cgr@contraloria.gov.co con copia al correo del enlace técnico designado por la CGR.

5.2 Descripción de las fuentes de información (Diccionarios de datos)

La información para consumir por la CGR y suministrada por parte de ADRES, se puede consultar en el diccionario de datos correspondientes al archivo anexo denominado "*"Anexo Técnico CGR – ADRES.pdf*"".

De manera complementaria a este documento, y para dar cumplimiento a los requerimientos de la UNCOPI en lo referente a búsqueda de información patrimonial de presuntos responsables fiscales y responsabilizados fiscales se consumirá la por la CGR a través de la VPN la siguiente información:

Tabla Afiliados

Base de Datos Única de Afiliados		Descripción
58,920,757		Tamaño (a julio 31 2025)
ADRES		Fabricante de la Bases de datos
Descripción		Nombre de la tabla
Información de los afiliados al SGSSS		AFILIADOS
Descripción	Tipo	nombre del campo
Fecha de nacimiento del afiliado.	DATETIME	AFILIADOS
Identificador único de los registros de la tabla AFILIADOS.	INT	AFL_ID
Primer apellido del afiliado.	VARCHAR	AFL_PRIMER_APELLIDO
Primer nombre del afiliado.	VARCHAR	AFL_PRIMER_APELLIDO
Segundo apellido del afiliado.	VARCHAR	AFL_SEGUNDO_APELLIDO
Segundo nombre del afiliado.	VARCHAR	AFL_SEGUNDO_NOMBRE
Identificador único de los registros de la tabla TIPOS_GENEROS.	VARCHAR	TPS_GNR_ID

Tabla Aportantes

Base de Datos Única de Afiliados		Descripción
12,186,784		Tamaño (a julio 31 2025)
ADRES		Fabricante de la Bases de datos
Descripción		Nombre de la tabla
Información de los empleadores aportantes		APORTANTES
Descripción	Tipo	nombre del campo
Digito de verificación del número del documento de un aportante	INT	APR_DIGITO_VERIFICACION
Fecha de finalización de la vigencia valida de un aportante en BDUA.	DATETIME	APR_FECHA_FIN
Fecha de inicio de la vigencia valida de un aportante en BDUA.	DATETIME	APR_FECHA_INICIO
Identificador único de los registros de la tabla APORTANTES.	INT	APR_ID
Número del documento de identificación de un aportante	VARCHAR	APR_NUMERO_IDENTIFICACION
Identificador único de los registros de la tabla TIPOS_APORTANTES.	VARCHAR	TPS_APR_ID
Identificador único de los registros de la tabla TIPOS_CIIUS.	VARCHAR	T TPS_CS_ID
Identificador único de los registros de la tabla TIPOS_IDENTIFICACIONES.	VARCHAR	TPS_IDN_ID
Identificador único de los registros de la tabla TIPOS_SECTORES.	VARCHAR	TPS_SCT_ID

Dentro de cada uno de estos archivos, se encuentra nombre del campo y tipo de dato, que ofrece la información de contexto (metadatos) de cada uno de los campos que se entregan a la CGR.

Lo anterior, debido al alto número de campos que posee cada una de las fuentes de información, se anexan al documento el archivo en mención.

5.2.1 Actualización y vigencia de la Información

Las vistas materializadas y los diccionarios descritos en este documento podrán ser modificados previo acuerdo mutuo entre las partes, con el propósito de mantener su relevancia y actualidad. En lugar de redactar un documento completamente nuevo, se ajustará el diccionario de datos denominado "Anexo técnico CGR – ADRES.pdf". Es importante mencionar que la información requerida por la CGR en las vistas materializadas y los diccionarios no tiene una restricción de temporalidad. Por lo tanto, la CGR podrá solicitar datos de periodos previos a la fecha de firma de este documento.

5.2.2 Características de seguridad para el acceso a la información

5.2.2.1 Cumplimiento

a. Las partes deben ceñirse a las directrices internas de cada una de las partes y a la normatividad vigente en seguridad de la información. Asimismo, para el tratamiento de datos personales deberán aplicar lo establecido en la Ley de Protección de Datos Personales (Ley 1581 de 2012 y decretos reglamentarios) y Ley de Transparencia (Ley 1712 de 2014) y demás disposiciones concordantes que modifiquen o complementen la materia.

b. Las partes deben aplicar los lineamientos para garantizar la interoperabilidad e implementar los mecanismos de control de seguridad necesarios que permitan salvaguardar la consulta de información.

c. LA CONTRALORIA debe velar por el buen uso del servicio dispuesto por la consulta de información. Así mismo, la entidad debe garantizar que dicho servicio se utilizará únicamente para la consulta y descarga de información solicitada y en ningún caso será utilizado para realizar copias de respaldo temporales o como repositorio de información personal.

d. Las partes deben implementar los mecanismos de control de seguridad necesarios para detectar y eliminar software o código malicioso previniendo la infección por malware a través de comunicaciones electrónicas o por labores como consulta y descarga de información.

e. Las partes deben asegurar la trazabilidad de la conexión, las actividades efectuadas y la consulta y descarga de información para la data estructurada y no estructurada, a través de mecanismos de control de seguridad, como registros de logs de auditoría garantizando adicionalmente el principio de no repudio.

f. Las partes deben implementar los mecanismos de control de seguridad necesarios para limitar el acceso a la información, siguiendo el principio de mínimo privilegio. Estos privilegios solo serán otorgados a los funcionarios con roles y perfiles de usuario claramente definidos y que serán responsables de la custodia de la información, asegurando así la confidencialidad de los datos.

g. Las partes notificarán a través de comunicados escritos enviados por correo electrónico a los canales institucionales previamente definidos en el acuerdo, cualquier evento tecnológico que genere interrupción por tiempo prolongado en la consulta y descarga de información afectando la disponibilidad de la información. El propósito de esta notificación es tomar de manera inmediata las acciones necesarias para reestablecer el servicio.

h. Las partes notificarán, a través de comunicados escritos enviados por correo electrónico a los canales institucionales previamente definidos en el acuerdo, cualquier incidente de seguridad que amenace y ponga en riesgo la confidencialidad e integridad de la información. El propósito de esta notificación es tomar de manera inmediata las acciones necesarias para minimizar el impacto que dicho incidente pueda ocasionar en la contraparte, así mismo, respaldar, contribuir y fortalecer las medidas de ciberseguridad del Estado.

5.2.2.2 Controles de seguridad aplicados a la Contraloría General de la República por parte de la entidad dentro del acceso establecido:

a. Se gestionan el acceso a los recursos informáticos (aplicaciones, recursos compartidos, equipos de cómputo, bases de datos) y demás sistemas de información, mediante la asignación de usuarios autorizados por la Entidad aplicando el principio de mínimo privilegio. Igualmente, se implementa una restricción efectiva para prevenir el acceso de usuarios no autorizados.

b. Se controla el acceso a recursos informáticos (aplicaciones, recursos compartidos, equipos de cómputo, bases de datos) y demás sistemas de información, empleando mecanismos de control de seguridad para autenticación mediante inicio de sesión seguro que minimiza las posibilidades de acceso no autorizado. Estos mecanismos incluyen la gestión de claves, el uso de contraseñas robustas y complejas, cambios periódicos y registro de intentos fallidos de autenticación.

c. Se realiza cifrado del canal de comunicaciones implementando el estándar AES o 3DES que permite establecer una conexión segura para la información en tránsito desde el origen de la conexión hasta el punto final de recepción. En la configuración del usuario de consulta de información estructurada se implementa VPN Site to Site utilizando protocolos de seguridad como IPsec, para la consulta y descarga de información no estructurada se utiliza una extensión del protocolo SSH (Secure Shell) para garantizar la confidencialidad e integridad de los datos.

d. Se restringen conexiones establecidas entre las Entidades mediante la aplicación de políticas de firewall que limitan su acceso a la ubicación geográfica de Colombia.

e. Se realiza monitoreo constante de las herramientas de seguridad perimetral y de la plataforma tecnológica con el objetivo de hacer seguimiento a las actividades realizadas en el ciberespacio para identificar tráfico anómalo que pueda derivar en posibles amenazas cibernéticas.

5.2.2.3 Controles de seguridad generales aplicados por la entidad:

a. Garantizar la clasificación y el etiquetado de la información por parte del propietario del activo de información.

b. Supervisar el acceso a las credenciales de conexión proporcionadas a LA CONTRALORIA, asegurando su autenticidad y limitando su conocimiento exclusivamente a los funcionarios responsables del manejo de la información.

c. Garantizar la ejecución de tareas de análisis de la solución de antivirus institucional previa configuración de VPN y usuario de consulta de información.

d. Garantizar el principio de no repudio con la implementación de mecanismos de controles de seguridad que permitan evidenciar la trazabilidad de la consulta y descarga de la información y comunicados.

e. Supervisar la gestión de claves, limitando su acceso únicamente a los funcionarios responsables, con el propósito de reducir el riesgo de posibles fugas de información que podrían derivar en eventos o incidentes de seguridad.

f. Garantizar el uso de software licenciado instalado en las estaciones de trabajo para: sistema operativo, antivirus, herramientas ofimáticas, así mismo, garantizar la actualización de parches de seguridad y el uso de las versiones más recientes para minimizar las vulnerabilidades de los sistemas de información utilizados en la consulta y descarga de la información.

g. Informar a LA CONTRALORIA a través de comunicados escritos enviados por correo electrónico a los canales institucionales previamente definidos en el acuerdo, el nombre del proveedor de servicios (ISP) y el direccionamiento IP publico asignado para establecimiento del canal de información con el objetivo de mantener actualizadas las políticas de firewall, así mismo, se deben reportar inmediatamente surtan cambios en el proveedor de servicios y en el direccionamiento IP público.

h. Informar a LA CONTRALORIA a través de comunicados escritos enviados por correo electrónico a los canales institucionales previamente definidos en el acuerdo, sobre los nombres, cargos, datos de contacto y la dependencia de los funcionarios responsables de llevar a cabo las actividades de configuración y mantenimiento del canal establecido de información. Además, es fundamental comunicar a CONTRALORIA cualquier novedad relacionada con el personal que participa en dichas actividades.

5.2.2.4 Uso de herramientas utilitarias

Para la disposición de la información a través del VPN site to site configurada para LA CONTRALORIA, la ADRES recomienda utilizar las siguientes aplicaciones o similares

a. SQL DEVELOPER: es una herramienta de desarrollo integrada (IDE) para trabajar con bases de datos SQL. Es desarrollada por Oracle y se utiliza principalmente para gestionar y desarrollar bases de datos Oracle. https://www.oracle.com/database/sqldeveloper/

b. **Toad for SQL Server** es una herramienta de desarrollo y administración de bases de datos que ofrece funcionalidades avanzadas para trabajar con bases de datos. https://www.quest.com/products/toad-for-sql-server/

Recomendaciones:

a. Verificar en los sitios oficiales e instalar periódicamente las actualizaciones liberadas para las herramientas.

b. Las configuraciones deben acordadas previamente con la ADRES para asegurar el correcto funcionamiento.

5.2.2. Suscripción acuerdo de confidencialidad

Se realizará la suscripción de acuerdo de confidencialidad mediante el Anexo llamado "*ACUERDO DE CONFIDENCIALIDAD"* por el jefe de la Unidad de Información – DIARI de la Contraloría General de la República y los designados por parte de la entidad que hace parte integral del documento técnico de entendimiento.

VI MODIFICACIONES AL ACUERDO TÉCNICO DE ENTENDIMIENTO

Las propuestas de modificación de este anexo deberán limitarse a la actualización de información a consultar, así como de seguridad informática. Éstas deberán ser introducidas por la instancia de coordinación y seguimiento a la ejecución del presente acuerdo.

VII VERIFICACIÓN DE LA APLICACIÓN DEL ACUERDO TÉCNICO

La verificación de la correcta aplicación de las directrices, procedimientos y protocolos establecidos en este Anexo es responsabilidad de la instancia de coordinación y seguimiento a la ejecución del acuerdo técnico de entendimiento.

VIII FUNCIONARIOS DE CONTACTO

CONTRALORÍA GENERAL DE LA REPÚBLICA	ADMINISTRADORA DE LOS RECURSOS DEL SISTEMA GENERAL DE SEGURIDAD SOCIAL EN SALUD
Cargo: jefe Unidad de Cooperación Nacional e Internacional de Prevención Investigación e Incautación de Activos - UNCOPI	**Cargo**: Director General
Funcionario: Andrea Moreno Taleb	**Funcionario**: Félix León Martínez Martín
Correo: andrea.moreno@contraloria.govco	**Correo**: felix.martinez@adres.gov.co

CONTRALORÍA GENERAL DE LA REPÚBLICA	ADMINISTRADORA DE LOS RECURSOS DEL SISTEMA GENERAL DE SEGURIDAD SOCIAL EN SALUD
Cargo: Unidad de Cooperación Nacional e Internacional de Prevención Investigación e Incautación de Activos - UNCOPI	**Cargo**: Asesora de la Dirección General
Funcionario: Fanny Andrea Rodriguez Eslava	**Funcionario**: Ligia Andrea Flórez Cubillos
Correo: fanny.rodriguez@contraloria.gov.co	**Correo**: Ligia.Florez@adres.gov.co;
Cargo: jefe de la Unidad de Información – DIARI	**Cargo**: Asesor de la Dirección General
Funcionario: Eduardo Jose Tous de la Ossa	**Funcionario**: Saul Diaz Olivares
Correo: Eduardo.tous@contraloria.gov.co	**Correo**: saul.diaz@adres.gov.co
Cargo: Coordinador Unidad de Información – DIARI	**Cargo**: Coordinador de Gestión de Operaciones de Sistemas de información de la DGTIC
Funcionario: Lucio Fernando Díaz Soto	**Funcionario**: Jose Leonardo Herrera Quintero
Correo: lucio.diaz@contraloria.gov.co	**Correo**: Jose.herrera@adres.gov.co
Cargo: Profesional Universitario Grado 2	**Cargo**: Gestor de Operaciones encargado de Trasferencia de la Información
Funcionario: Julian R. Rodriguez Martinez	**Funcionario**: Luis Alejandro Garzon Ruiz
Correo: julian.rodriguezm@contraloria.gov.co	**Correo**: Luis.garzon@adres.gov.co

El día 22 del septiembre del año 2025 se elaboró el presente documento técnico de entendimiento entre las partes definiendo las condiciones técnicas y de seguridad para el manejo de la información.

Firma de las partes

Por parte de **ADMINISTRADORA DE LOS RECURSOS DEL SISTEMA GENERAL DE SEGURIDAD SOCIAL EN SALUD**

MARTINEZ MARTIN FELIX LEON

Firmado digitalmente por MARTINEZ MARTIN FELIX LEON

Nombre: **Félix León Martínez Martín**
Cargo: Director General

Por parte de LA **CONTRALORÍA GENERAL DE LA REPÚBLICA**,

Nombre: **Eduardo José Tous de la Ossa**
Cargo: Jefe de la Unidad de Información de la Dirección de Información, Análisis y Reacción Inmediata – DIARI.

Aprobó CONTRALORIA	Eduardo José Tous de la Ossa - Jefe Unidad de Información -DIARI ANDREA MORENO TALEB - Jefe Unidad de Cooperación Nacional e Internacional de Prevención Investigación e Incautación de Activos – UNCOPI
Revisó CONTRALORIA	Fanny Andrea Rodriguez Eslava – Profesional Especializado 04 Valeria Vergara Cruzado – Profesional Universitario Grado 2
Proyecto CONTRALORIA	María Paula Forero F – Profesional Universitario Grado 01 CONTRALORIA Carlos Daniel Roa O – Profesional Universitario Grado 01 CONTRALORIA Julian R. Rodriguez M – Profesional Universitario Grado 01 CONTRALORIA Freddy Alexander Jimenez - Profesional Universitario Grado 01 CONTRALORIA

Aprobó ADRES	Marcos Jaher Parra Oviedo Jefe de la Oficina Asesora Jurídica PARRA OVIEDO MARCOS JAHER Firmado digitalmente por PARRA OVIEDO MARCOS JAHER Fecha: 2025.09.25 20:52:19 -05'00'
Reviso ADRES	Grupo de Gestión de Contratación – Dirección Administrativa y Financiera
Revisión Inicial ADRES	Ligia Andrea Florez Cubillos – Asesora de la Dirección General Jose Leonardo Herrera Coordinador de Gestión de Operaciones de Sistemas de información de la DGTIC Luis Alejandro Garzon Ruiz Gestor de Operaciones de la DTIC