Manual de
Protección de Datos Personales

Proceso Información, Innovación y Tecnología
Subproceso Seguridad de la Información
Versión 03
Código MN-IIT-0062
Año 2024

El contenido de este documento corresponde a Información Pública

TABLA DE CONTENIDO

1. OBJETIVO

Establecer las políticas y procedimientos internos que adopta la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales – UAE DIAN, (en adelante DIAN), para desarrollar el cumplimiento de lo establecido en la Ley Estatutaria 1581 de 2012 – Por la cual se dictan disposiciones generales para la Protección de datos Personales, especialmente lo consagrado en los literales k y f de los artículos 17 y 18, respectivamente.

2. ALCANCE

El presente manual es de obligatorio y estricto cumplimiento por parte de los funcionarios, contratistas y terceros que obran en nombre de la DIAN.

En ese sentido, se debe observar y respetar la regulación en materia de protección de datos, la Política de Tratamiento de Datos Personales establecida por la DIAN, las disposiciones previstas en el presente manual en lo que corresponda y/o las instrucciones dadas por la entidad relacionadas con estos aspectos.

El presente manual establece las condiciones, los lineamientos, los principios, derechos y obligaciones de los responsables o encargados del tratamiento de datos personales, así como los procedimientos aplicables al tratamiento de los datos personales que la DIAN solicite, recopile, procese, almacene o utilice, en desarrollo de las funciones objeto de su misión como entidad pública para todas las bases de datos físicas o automatizadas.
La DIAN realiza directamente el tratamiento de los datos personales; sin embargo, se reserva el derecho a delegar en un tercero tal tratamiento, exigiendo al encargado, la atención e implementación de los lineamientos y procedimientos idóneos para la protección de los datos personales y la estricta confidencialidad de estos, de acuerdo con la normatividad vigente y lo establecido en este manual.

3. DEFINICIONES Y SIGLAS

- **Activo:** cualquier bien que tiene valor para la entidad. También se entiende por cualquier información o sistema relacionado con el tratamiento de datos personales, que tenga valor para la entidad. *Fuente: ISO/IEC 13335-12004.*

- **Autorización**: consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales. *Fuente: Ley 1581 de 2012.*

- **Aviso de privacidad**: comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales. *Fuente: Artículo 2.2.2.25.1.3. del Decreto Único Reglamentario 1074 de 2015.*

- **Base de Datos**: conjunto organizado de datos de personas naturales, bien sea que se encuentren de forma física o electrónica y que sea objeto de Tratamiento. *Fuente: Ley 1581 de 2012, artículo 3: Definiciones, Literal b) Bases de Datos.*

- **Bases de Datos de procesos misionales**: son bases de datos físicas o electrónicas que contienen datos obtenidos o recopilados en cumplimiento de las funciones y objetivos misionales de la DIAN, ligados a los procesos Tributarios, Aduaneros y Cambiarios – TAC, su tratamiento no requiere de autorización previa del Titular o de su representante legal. El hecho de que no requieran autorización no exime al Responsable del cumplimiento de las demás obligaciones relacionadas con la protección de los datos. *Fuente: Oficina de Seguridad de la Información. DIAN - 2023.*

- **Bases de Datos de procesos no misionales**: son bases de datos físicas o electrónicas que contienen datos públicos, privados, sensibles y de niños, niñas y adolescentes, obtenidos o recopilados en cumplimiento de alguna actividad laboral, contractual o específica, necesaria para el desarrollo administrativo de los recursos humanos, físicos, tecnológicos o financieros de la entidad. El Tratamiento de estos datos requiere de la autorización previa del Titular o de su Representante Legal. *Fuente: Oficina de Seguridad de la Información. DIAN - 2023.*

- **Canal de acceso electrónico**: se entenderá como canal de acceso electrónico aquellas formas mediante las cuales se recolecta y/o almacena información personal tales como, web, dispositivos móviles y atención telefónica. *Fuente: Oficina de Seguridad de la Información. DIAN - 2023.*

- **Captura de la Información Personal**: toda recolección de información personal de una persona natural (Titular). *Fuente: Oficina de Seguridad de la Información. DIAN - 2023.*

- **Cláusula de transmisión y/o transferencia de datos personales**: es la disposición establecida en un contrato en el cual una o varias obligaciones derivadas de su cumplimiento requieren el envío de bases de datos con datos personales a terceros en modalidad de Transmisión o Transferencia y el establecimiento de la obligación de tratar la información con medidas de seguridad y confidencialidad. *Fuente: Oficina de Seguridad de la Información. DIAN - 2023.*

- **Cláusula contractual**: una cláusula es una disposición inserta en un contrato por medio de la cual las partes acuerdan unas condiciones especiales relativas a la naturaleza de la obligación, el lugar, el precio, el modo de ejecución, entre otras.

  En ese sentido, las partes pactan y manifiestan su voluntad estableciendo parámetros y características del vínculo que se va a suscribir. El Código Civil colombiano las clasifica como esenciales, accidentales y naturales. Las primeras son fijadas por el legislador o por la costumbre, necesarias para la existencia jurídica del contrato. Las segundas representan la plena autonomía de las partes y solo se consideran si están presentes en el cuerpo del contrato. Las últimas son aquellas que se consideran inherentes al contrato sin que las partes las señalen expresamente, ya que suplen la voluntad de las partes cuando se guarda silencio. Fuente: *Oficina de Seguridad de la Información. DIAN - 2023.*

- **Confidencialidad:** propiedad de la información que determina que esté disponible a personas autorizadas. Fuente: *Ministerio de Tecnologías de la Información y las Comunicaciones - Glosario. Hipervínculo: https://www.mintic.gov.co/portal/inicio/Glosario/*

- **Consulta en materia de Protección de Datos Personales**: los Titulares o sus causahabientes pueden tener acceso, conocer o “consultar” la información personal del Titular que repose en cualquier base de datos de la Entidad, la DIAN debe suministrar al Titular toda la información

contenida en el registro individual o que esté vinculada con la identificación del titular (art. 14 Ley 1581 de 2012). *Fuente: Oficina de Seguridad de la Información. DIAN - 2023.*

- **Contrato**: *contrato o convención es un acto por el cual una parte se obliga para con otra a dar, hacer o no hacer alguna cosa. Cada parte puede ser de una o de muchas personas.*
  Fuente: Artículo 1495 del Código Civil

- **Contrato de Transmisión y/o Transferencia de datos personales**: es el contrato cuyo objeto radica en el envío de bases de datos que contienen datos personales. A través de estos contratos, el Responsable -el cual almacena y trata bases de datos con datos personales- acuerda las condiciones macro, establece responsabilidades y obligaciones respecto de un tercero, que ejercerá el rol de Encargado (en contratos de Transmisión) o como Responsable (en contratos de Transferencia); acerca del Tratamiento de las bases de datos objeto del envío, define medidas de seguridad y confidencialidad de la información enviada. *Fuente: Oficina de Seguridad de la Información. DIAN - 2023.*

- **Datos personales de niñas, niños y adolescentes**: son los datos que puedan hacer identificables a niños, niñas y adolescentes y su Tratamiento es permitido siempre y cuando el fin que se persiga responda al interés superior y asegure respeto a sus derechos prevalentes. *Fuente: Oficina de Seguridad de la Información. DIAN - 2023.*

- **Dato personal**: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. *Fuente: Ley 1581 de 2012.*

- **Dato público**: es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva" (Decreto Único Reglamentario 1074 de 2015). Así mismo, se entiende como dato público, aquel dato que por mandato legal o decisión del Titular se encuentre en redes de libre acceso. *Fuente:* Artículo *2.2.2.25.1.3 del Decreto Único Reglamentario 1074 de 2015.*

- **Dato privado**: es el dato que por su naturaleza íntima o reservada solo es relevante para el Titular. *Fuente: Ley 1266 de 2008.*

- **Dato semiprivado**: es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero o crediticio de actividad comercial o de servicios a que se refiere el Titulo IV" de la Ley 1266. *Fuente: Ley 1266 de 2008.*

- **Datos sensibles**: se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos". *Fuente: Artículo 2.2.2.25.1.3 del Decreto Único Reglamentario 1074 de 2015.*

- **Derecho Constitucional a la intimidad personal y familiar**: todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. *Fuente: Artículo 15 de la Constitución Política de Colombia.*

- **Derecho de Habeas Data**: derecho de los Titulares de información personal a conocer, actualizar y rectificar la información recogida en Bases de Datos. *Fuente: Artículos 15 y 20 de la Constitución Política de Colombia.*

- **Encargado del Tratamiento**: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012). *Fuente: Artículo 2.2.2.25.1.3 del Decreto Único Reglamentario 1074 de 2015.*

- **Gestión de Eventos:** es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles.
  Fuente: Función Pública - Gestión del Riesgo DAFP. https://www.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf/50bff85a-70c6-dd15-68f5-6cd2ea2a8707?t=1677003002032

- **Finalidad del Tratamiento**: la recolección de los datos personales debe tener una finalidad legítima y cierta, es decir, una razón de ser de esa recolección. Además, los datos recolectados deben ser pertinentes y adecuados para alcanzar dicho fin, estos deben corresponder a objetivos misionales, estratégicos, de control o apoyo de la DIAN. *Oficina de Seguridad de la Información. DIAN - 2023.*

- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
  Fuente: Función Pública - Gestión del Riesgo DAFP. https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Versi%C3%B3n+5+-+Diciembre+de+2020.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=1611247032238

- **Incidente de seguridad:** cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de una empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información
  Fuente: Instituto Nacional de Ciberseguridad (INCIBE) - España. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

  Un incidente de seguridad asociado al tratamiento de datos personales puede enunciarse como un evento o serie de eventos de seguridad asociados a la violación de la confidencialidad, integridad o disponibilidad de los datos personales respecto de los cuales la DIAN actúa como responsable o encargado del tratamiento y que, en consecuencia, afecte los derechos y libertades de los interesados. La violación o brecha de seguridad debe representar una afectación, real amenaza y perjuicio para el Titular, la Información o la Entidad. Fuente: ISO 27035:2011.

- **Integridad**: propiedad de salvaguardar la exactitud y estado completo de los activos. Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. *https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf*

- **Marco de Interoperabilidad:** 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 ciudadanos, empresas y a otras entidades, mediante el intercambio de datos entre sus sistemas TIC. Fuente: *Ministerio de Tecnologías de la Información y las Comunicaciones https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8117.html*

- **Oficial de Protección de Datos**: persona o dependencia encargada al interior de la DIAN que será Responsable de articular el Programa Integral de Protección de Datos Personales al interior de la Entidad, en adelante OPD. *Fuente: Oficina de Seguridad de la Información – DIAN 2023.*

- **Principio de responsabilidad demostrada (*Accountability*)**: los responsables que recogen y hacen Tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012. Los responsables del tratamiento deben contar con un programa integral de gestión de datos personales y estar preparados para demostrarle a la autoridad la implementación efectiva de esas medidas en la organización. *Fuente: Artículo 2.2.2.25.6.1 del Decreto Único Reglamentario 1074 de 2015*.

- **Principio de seguridad, privacidad y circulación restringida de la información**: toda la información de los usuarios que se genere, almacene o transmita en el marco de los servicios ciudadanos digitales, debe ser protegida y custodiada bajo los más estrictos esquemas de seguridad y privacidad con miras a garantizar la confidencialidad, el acceso y circulación restringida de la información, de conformidad con lo estipulado en el componente de seguridad y privacidad de la Estrategia de Gobierno en Línea. *Fuente: Artículo 2.2.17.1.5 del Decreto 1413 de 2017.*

- **Principio de privacidad por diseño y por defecto**: desde antes que se recolecte información y durante todo el ciclo de vida de esta, se deben adoptar medidas preventivas de diversa naturaleza (tecnológica, organizacional, humana, procedimental) para evitar vulneraciones al derecho a la privacidad o a la confidencialidad de la información, así como fallas de seguridad o indebidos tratamientos de datos personales. La privacidad y la seguridad deben hacer parte del diseño, arquitectura y configuración predeterminada del proceso de gestión de información y de las infraestructuras que lo soportan. (Decreto 1413 de 2017). *Fuente: Artículo 2.2.17.1.5 del Decreto 1413 de 2017.*

- **Protección de datos personales en la DIAN**: conjunto de normas, procesos, políticas, procedimientos, controles, medidas y demás actividades adoptadas y/o definidas al interior de la entidad, para asegurar el adecuado cumplimiento del Régimen de Protección de Datos Personales, en adelante PDP. *Fuente: Oficina de Seguridad de la Información. DIAN - 2023.*

- **Reclamo en materia de protección de datos personales**: solicitud del Titular del dato o las personas autorizadas por este o por la ley para corregir, actualizar o suprimir sus datos personales o cuando adviertan que existe un presunto incumplimiento del régimen de protección de datos. *Fuente: Ley 1581 de 2012.*

- **Requisito de procedibilidad**: el Titular o causahabiente solo podrá elevar queja ante la Superintendencia de Industria y Comercio o Procuraduría General de la Nación una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento. *Fuente: Artículo 16 de la Ley 1581 de 2012.*

- **Responsable del tratamiento**: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. *Fuente: Ley 1581 de 2012.*

- **Riesgo:** efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Fuente: *Función pública - Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. https://www.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf/50bff85a-70c6-dd15-68f5-6cd2ea2a8707?t=1677003002032*

- **Seguridad de la información en la Política de Gobierno Digital**: es un elemento que apoya a las entidades de manera trasversal, habilitando el desarrollo de los componentes de la política de Gobierno Digital. Este componente se desarrolla, a través de lineamientos en materia de seguridad y privacidad de la información, así como de gestión de riesgos de seguridad digital, lo cuales soportan las acciones establecidas por cada entidad para proteger los activos de información, preservando la confidencialidad, integridad, disponibilidad y privacidad de los datos. *Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones – Gobierno Digital* https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/

- **SIC:** Superintendencia de Industria y Comercio.

- **Sistema de videovigilancia**: controles realizados mediante la instalación y manejo de cámaras de seguridad o videovigilancia implementadas para garantizar la seguridad de bienes o personas. *Fuente: Oficina de Seguridad de la Información. DIAN - 2023.*

- **Supresión**: derecho que tienen los titulares a solicitar la eliminación o retiro de sus datos personales cuando ha cesado la finalidad para la cual fueron recolectados.
Fuente: Oficina de Seguridad de la Información. DIAN - 2023.

- **Titular**: persona natural cuyos datos personales son objeto de tratamiento. *Fuente: Ley 1581 de 2012.*

- **Transferencia**: la 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. *Fuente: Artículo 2.2.2.25.1.3. del Decreto Único Reglamentario 1074 de 2015.*

- **Transmisión:** tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento

por el encargado por cuenta del responsable. *Fuente: Artículo 2.2.2.25.1.3. del Decreto Único Reglamentario 1074 de 2015.*

- **Tratamiento:** cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. *Fuente: Artículo 2.2.2.25.1.3. del Decreto Único Reglamentario 1074 de 2015.*

- **Usuario:** persona natural que tiene algún vínculo legal, contractual o por servicio consentimiento expreso otorgado a la entidad *Fuente: Oficina de Seguridad de la Información. DIAN - 2023.*

- **Servidores Públicos o funcionarios:** son servidores públicos de la contribución, las personas naturales que prestan sus servicios en la Dirección de Impuestos y Aduanas Nacionales, vinculados a ella por una relación legal y reglamentaria sea ésta en calidad de servidores de carrera, supernumerarios o de libre nombramiento o remoción. Fuente: https://www.dian.gov.co/dian/entidad/Paginas/NuestraGenteDian.aspx#:~:text=Son%20servidores%20p%C3%BAblicos%20de%20la,de%20libre%20nombramiento%20o%20remoci%C3%B3n.

4. MARCO LEGAL Y REGLAMENTARIO

Ver catálogo normativo del proceso opción “Marco Normativo” en el siguiente link: https://www.dian.gov.co/atencionciudadano/Seguridad-de-la-Informacion/Paginas/Proteccion-de-datos-personales.aspx

5. CONDICIONES GENERALES

La Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales” desarrolla el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en Bases de Datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la mencionada Carta.

El presente manual, sus políticas y procedimientos forman parte de las disposiciones normativas internas frente a Protección de datos personales, por lo que deben ser observadas por cualquier individuo o persona jurídica que tenga acceso o lleve a cabo el tratamiento de datos personales que formen parte de los archivos y bases de datos de la entidad.

El incumplimiento de las políticas y procedimientos de datos personales establecidos en el presente manual acarreará para los servidores públicos, contratistas y terceros de la DIAN, el inicio de las acciones disciplinarias, administrativas, penales y/o fiscales a que haya lugar, así como las sanciones previstas en la Ley. La observancia de estas disposiciones está cubierta por los vínculos legales o contractuales y la suscripción del compromiso de confidencialidad de cada uno de ellos.

Para el cumplimiento del principio de privacidad por diseño desde antes de que se recolecte información y durante todo el ciclo de vida de esta, se deben adoptar medidas preventivas y/o correctivas de diversa naturaleza (tecnológica, organizacional, humana, procedimental) para evitar vulneraciones al derecho a la privacidad o a la confidencialidad de la información, así como posibles fallas de seguridad o indebidos tratamientos de datos personales. La privacidad y la seguridad hacen parte del diseño,

arquitectura y configuración predeterminada del proceso de gestión de información y de las infraestructuras que lo soportan. En ese orden de ideas el diseño de procesos, procedimientos, formatos, aplicativos, sistemas informáticos, software adquirido o desarrollo de productos y servicios que se realice o adquiera la entidad que, implique el tratamiento de datos personales, debe contemplar medidas de privacidad y protección de datos.

La DIAN reconoce que los datos personales son propiedad de los titulares y que solo ellos pueden decidir sobre los mismos. En este sentido, hará uso de los datos solo para aquellas finalidades relacionadas con el cumplimiento de su objeto misional, obligaciones legales o contractuales y para las que se encuentra facultada, respetando en todo caso la normatividad vigente sobre protección de datos personales.

La DIAN cumplirá en los mismos términos de la normativa vigente, con las políticas de protección y tratamiento de datos personales de funcionarios, exfuncionarios, contratistas y demás terceros que en desarrollo de actividades no misionales tengan relación con la entidad.

Para vincular jurídicamente a los usuarios de los datos, se deberán celebrar contratos que establezcan la adhesión a las políticas internas de la DIAN y, en caso de ser necesario (en particular para la tercerización de servicios), se especifican las obligaciones de confidencialidad, seguridad de la información, recolección y tratamiento de datos personales de empleados , usuarios o terceros, restricciones a la circulación de los datos personales y mandatos de supresión o cancelación de la información al término de las relaciones contractuales.

Quien ejerza la supervisión de los contratos, debe asegurar que el contratista cumple y aplica todas las disposiciones legales para el tratamiento de datos personales. Para esto debe verificar la suscripción de compromisos de confidencialidad, la implementación de instrumentos de recolección y circulación de la información (autorizaciones, avisos de privacidad, compromisos, riesgos), entre otros mecanismos.

Además, los lineamientos relativos al tratamiento de datos personales exceptuando la etapa de recolección, deben ejecutarse cuando se trate de cualquier dato personal sin discriminar el origen de los datos, siendo así obligatorio proteger los derechos de los titulares de la información personal que haya sido proporcionada con autorización y de aquellos datos que se hayan obtenido en ejercicio de las funciones de la DIAN.

La DIAN establece medidas o estándares de seguridad en el cumplimiento de la ley, de la Política de Tratamiento de Datos Personales y del presente manual cuando la información sobre la cual se va a realizar el tratamiento sea de carácter sensible o de niños, niñas y adolescentes.

El tratamiento de datos personales en sistemas de información interoperables está regulado por el Gobierno Nacional. En este orden de ideas los principios y directrices establecidas por la Ley 1581 de 2012 y sus decretos reglamentarios, son aplicables a este tipo de prácticas de intercambio de información. Las acciones de interoperabilidad de la información, independientemente del medio (tecnológico o físico) en que lo realicen las dependencias, deben asegurar la implementación de medidas de protección de datos personales. Toda acción de intercambio, transferencia, transmisión o entrega de información debe estar soportada en documentos que contengan la responsabilidad del tratamiento de datos por las partes y la suscripción de actas, compromisos, acuerdos, convenios, protocolos, contratos y demás acciones que protejan la privacidad de los titulares.

En la adopción de inteligencia artificial o utilización de sistemas de inteligencia de datos o de analítica de datos que desarrolle o contrate la DIAN, deben contemplarse medidas de seguridad y privacidad que garanticen los derechos de los titulares de datos personales.

De acuerdo con lo establecido en el artículo 7 de la Ley 1581 de 2012, la DIAN asegura el respeto a los derechos prevalentes de los niños, niñas y adolescentes. Así mismo se acoge a la regla general, según la cual queda proscrito el tratamiento de datos personales de esta población protegida, salvo aquellos datos que sean de naturaleza pública.

En todos los procesos antes señalados, la DIAN pondrá a disposición de los titulares el Aviso de Privacidad y la Política de Tratamiento de Datos Personales según sea el caso.

La dependencia competente dará respuesta a las consultas y reclamos de titulares a través de la plataforma PQSRD dentro de los plazos señalados en la Ley 1581 de 2012 y en la Política de Tratamiento de Datos Personales de la entidad.

Los datos personales a los que haga tratamiento la DIAN deberán provenir de fuentes públicas, o recolectadas del titular o por terceros, y siempre de fuentes confiables. No podrán obtenerse datos personales mediante instrumentos engañosos o fraudulentos o para fines contrarios a los correspondientes a la naturaleza de la entidad conforme a su gestión y su misión institucional.

No se requerirá autorización para el tratamiento de datos contenidos en fuentes públicas de información siempre que dichos datos sean de naturaleza pública.

Salvo la excepción del requisito de autorización, el carácter público de la DIAN no la faculta para no cumplir con los principios rectores para la protección de los datos personales ni valida el tratamiento de datos personales por sus servidores públicos, trabajadores y contratistas en perjuicio de sus titulares.

La Oficina de Seguridad de la Información o el Oficial de Protección de Datos, publicará en los medios dispuestos por la entidad, las modificaciones que se realicen a la Política de Tratamiento de Datos Personales establecida por la DIAN con apego a la normatividad legal vigente.

Para el desarrollo, estructuración, mejora o modificación de los servicios y procedimientos de la DIAN, adecuaciones tecnológicas, entre otros, en los cuales haya lugar a obtener, entregar, almacenar o realizar cualquier tipo de tratamiento o actividad sobre datos personales o Bases de Datos, la dependencia responsable es la encargada de velar por el cumplimiento de los lineamientos establecidos en el presente manual.

El Oficial de Protección de datos personales, o quien haga sus veces, será el responsable de diseñar, divulgar, actualizar y verificar el cumplimiento de los lineamientos aquí vertidos.

6. PRINCIPIOS PARA EL TRATAMIENTO DE LOS DATOS PERSONALES

De acuerdo con lo establecido en el artículo 4 de la Ley 1581 de 2012 y la Política de Tratamiento de Datos Personales expedida por la DIAN, los servidores de la entidad aplicarán integralmente los siguientes principios que se constituyen en los parámetros a seguir en la recolección, manejo, uso, tratamiento, almacenamiento e intercambio de datos personales.

- Principios relacionados con la **<u>recolección</u>** de datos personales:

Ilustración 1. Principios

- Principios relacionados con el **uso** de datos personales:

FINALIDAD

• La **DIAN** realiza el tratamiento de datos personales con la finalidad de dar cumplimiento a su misión institucional, al desarrollo de las demás funciones consagradas en el ordenamiento jurídico y a las obligaciones legales y contractuales. Asimismo, son finalidades las que propenden directa e indirectamente por el fortalecimiento y mejor función de sus obligaciones misionales y legales.

TEMPORALIDAD

• Los datos personales se conservarán únicamente por el tiempo razonable y necesario para cumplir la finalidad del tratamiento y las exigencias legales o instrucciones de las autoridades de vigilancia y control u otras autoridades competentes. Los datos serán conservados cuando ello sea necesario para el cumplimiento de una obligación legal o contractual. Para determinar el término del tratamiento se considerarán las normas aplicables a cada finalidad y los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

- Principios relacionados con la **calidad** de la información:

VERACIDAD O CALIDAD

•La información sujeta a tratamiento deberá ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error. Se deberán adoptar medidas razonables para asegurar que los datos sean precisos y suficientes y, cuando así lo solicite el titular o cuando la **DIAN** así lo determine, sean actualizados, rectificados o suprimidos cuando sea procedente.

- Principios relacionados con la **protección, acceso y Circulación** de datos personales:

SEGURIDAD

• La DIAN implementará todas las medidas de seguridad que estén a su alcance, de acuerdo con las normas técnicas y estándares internacionales, para garantizar que, a nivel técnico, tecnológico, administrativo, procedimental y humano se preserve la confidencialidad e integralidad de los datos personales a los que haga tratamiento o conserve, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

TRANSPARENCIA

• La DIAN garantiza el derecho del titular de conocer en cualquier momento, gratuitamente y sin restricciones, la información acerca de la existencia de datos que le conciernen.

ACCESO Y CIRCULACIÓN RESTRINGIDA

• Los datos obtenidos y procesados por la DIAN en cumplimiento de su misión y objetivo como entidad del Estado están protegidos, y por lo tanto, se garantiza su acceso de conformidad con lo establecido en la ley, con la naturaleza del dato y con las autorizaciones dadas por el titular, sin perjuicio de las excepciones contempladas en la ley o por mandato judicial.

CONFIDENCIALIDAD

•La DIAN promueve políticas, procedimientos y lineamientos para que todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos estén obligados a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento o culminada su relación contractual o vínculo jurídico con la DIAN, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley.

7. DEBERES DE LA DIAN COMO RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES

De acuerdo con lo consagrado en los artículos 17 y 18 de la Ley 1581 de 2012, o las normas que lo reglamenten o modifiquen, son deberes de la DIAN como responsable y encargado del tratamiento de datos personales, los siguientes:

- Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Solicitar y conservar, en las condiciones previstas en la citada ley, copia de la respectiva autorización otorgada por el titular.
- Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Recopilar y conservar los datos personales bajo las condiciones de calidad (veraz, completa, exacta, actualizada, comprobable y comprensible) de conformidad con los términos definidos por ley.
- Actualizar la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada.
- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.
- Suministrar al encargado del tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la citada ley.
- Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.
- Tramitar las consultas y reclamos formulados en los términos señalados en la citada ley.
- Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la citada ley y en especial, para la atención de consultas y reclamos.
- Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
- Informar a solicitud del titular sobre el uso dado a sus datos.
- Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
- Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- Cumplir las instrucciones y requerimientos que imparta la Procuraduría General de la Nación y autoridades públicas y privadas, dentro de la órbita de su competencia, protegiendo derechos constitucionales de terceros.

7.1 Responsabilidades y obligaciones frente a la protección de datos

La DIAN cuenta con disposiciones internas que definen las responsabilidades y obligaciones en materia de protección de datos personales para la Oficina de Seguridad de la Información, en su calidad de Oficial de Protección de Datos Personales y para las dependencias de la DIAN que realicen tratamiento y protección de datos personales. Las dependencias deben atender lo dispuesto en el acto administrativo que asigna las funciones de Oficial de Protección de Datos Personales y fija obligaciones a las dependencias frente a la protección de datos personales en la entidad, con el fin de prestar especial atención a aquellas actividades que, en ejercicio de sus funciones, conllevan a la protección de este tipo de información.

8. DEBERES DE LA DIAN COMO ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES

La DIAN actúa como encargado cuando recibe del responsable, información para su tratamiento en nombre de un tercero. Generalmente, actúa como encargado cuando existe un acuerdo o convenio que así lo establece. Cuando la DIAN gestione datos personales como encargado del tratamiento, debe cumplir con los siguientes deberes:

- Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio de hábeas data.

- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Realizar oportunamente la actualización, rectificación o supresión de los datos personales en los términos señalados por la ley.
- Actualizar la información reportada por los responsables del tratamiento dentro de los cinco (5) días hábiles contados a partir de la fecha de su recibo.
- Tramitar las consultas y los reclamos formulados por los titulares en los términos señalados en la Ley 1581 de 2012 y sus decretos reglamentarios.
- Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los titulares.
- Registrar en la base de datos la leyenda “reclamo en trámite” en la forma regulada por la Ley.
- Insertar en la base de datos la leyenda “información en discusión judicial” una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
- Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
- Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
- Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.
- En el momento en que la DIAN sea responsable y encargado del tratamiento, le será exigible el cumplimiento de los deberes previstos para cada uno de ellos.

9. DERECHOS DE LOS TITULARES

La dependencia encargada de canalizar las solicitudes de los titulares referentes a la protección de datos personales es la Coordinación de Administración del Sistema de PQSRD - Peticiones, Quejas, Sugerencias, Reclamos y Denuncias o quien haga sus veces frente a la gestión de PQSRD en la DIAN, la cual dará trámite a las mismas para garantizar a los titulares el ejercicio de los derechos establecidos en la normatividad vigente y en el presente manual.

La DIAN se compromete a adelantar todas las acciones requeridas para preservar el derecho de los titulares de datos personales, de acuerdo con lo establecido en la Ley 1581 de 2012, el Decreto 1074 de 2015 y la Política de Tratamiento de Datos Personales de la entidad, así como aquellas normas que los modifiquen o actualicen. En particular se resaltan los siguientes derechos:

Derechos de los Titulares	
Derecho de acceso	La DIAN garantiza el derecho de acceso a los titulares de datos personales que correspondan a personas naturales, previa acreditación de la identidad del titular, legitimidad, o personalidad de su representante, poniéndolos a su disposición sin costo alguno.

Derechos de los Titulares	
Derecho a actualización, rectificación y supresión	Los titulares de datos personales tienen derecho a solicitar a la DIAN la actualización, rectificación o supresión de sus datos personales que resulte incompleta o inexacta, de acuerdo con los procedimientos adoptados en el presente manual. La DIAN como responsable del tratamiento de datos personales puede negar o limitar el ejercicio del derecho de supresión de datos, cuando su eliminación obstaculice actuaciones vinculadas al cumplimiento de obligaciones fiscales, a la investigación o persecución de delitos, o a la actualización de sanciones administrativas.
Derecho a revocar la autorización	Todo titular de datos personales puede revocar en cualquier momento, el consentimiento al tratamiento de estos, siempre y cuando, no lo impida una disposición legal o contractual. La DIAN como responsable del tratamiento de datos personales se puede negar o limitar el ejercicio del derecho a revocar la autorización, cuando su revocatoria obstaculice actuaciones vinculadas al cumplimiento de obligaciones fiscales, a la investigación o persecución de delitos, o a la actualización de sanciones administrativas.

Tabla 1. Derechos de los titulares

10. CATEGORIZACIÓN DE DATOS PERSONALES

10.1 Tipos de datos

La normativa define la clasificación de los datos personales en dato público, dato semiprivado, dato privado y datos sensibles.

Tipos De Datos	
Dato Personal	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Lit. c. Art. 2 Ley 1581 de 2012)
Dato Público	Es el dato que no es semiprivado, privado o sensible. Son considerados datos públicos, entre otros los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, cédula, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no están sometidas a reserva. (Art. 4 Ley 1581 de 2012).

Tipos De Datos	
Dato Semiprivado	Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el título IV de la ley. (Lit. g. Art. 3 Ley 1266 de 2008).
Dato Privado	Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Religión, política, hobbies, asociación, entre otros). (Lit. h. Art 3 Ley 1266 de 2008). Como consecuencia, aquella información que no es pública y que no tiene efectos sobre terceros, requerirá de la autorización para su recolección y tratamiento de conformidad con las disposiciones generales para la protección de datos personales.
Datos Sensibles	Aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Art 5 Ley 1581 de 2012).

Tabla 2. Tipos de datos

Las dependencias de la entidad deben cumplir los siguientes lineamientos:

- Inventariar y clasificar las bases de datos personales (físicas o automatizadas) que producen y gestionan.

- Identificar si hace tratamiento de bases de datos en calidad de responsable (la DIAN es dueña de esta información) o de encargado (la información de la base de datos es suministrada por un tercero).

- Revisar o replantear la pertinencia de esta recolección, es decir si obedece a lo funcional de la dependencia o proceso, si son temporales o permanentes, si tienen una finalidad clara de recolección o si se pueden fusionar o incorporar a otras bases de datos o tomar los datos de un sistema de información diferente.

- De cada base de datos o sistema de información con datos personales (físico o electrónico) identificar qué tipos de datos contiene (dato público, dato semiprivado, dato privado, dato sensible o datos de niños, niñas y adolescentes), si se gestionan como parte de un proceso financiero, de servicio al cliente, misional o de apoyo (ver mapa de procesos), para considerar el tipo de tratamiento al que será sujeto, qué tipo de tratamiento realiza (consulta, uso, almacenamiento, circulación, entre otros.), las medidas de seguridad y de gestión de riesgos teniendo en cuenta la metodología desarrollada por la DIAN, que tendrá que adoptar para proteger la privacidad de los titulares.

- Conforme con el tratamiento realizado (físico o electrónico), implementar los mecanismos necesarios desde la recolección del dato (autorización, aviso de privacidad, Disclaimer, entre otros), gestión (medidas de seguridad, registro, almacenamiento, riesgos, entre otros.) y disposición final del dato

(en este caso debe ser consecuente con la tabla de retención documental de la dependencia y las políticas y lineamientos en materia de gestión documental.

- Identificar los posibles usuarios internos y externos de esta base de datos y en qué medios y qué tipo de información puede compartir o intercambiar con estos usuarios.

10.2 Tipos de datos en la DIAN

Para el inventario de bases de datos se identifica como titulares, a los contribuyentes, los usuarios aduaneros, los servidores públicos de la entidad con sus familiares, y contratistas. La información que se encuentra en esas bases de datos contiene la clasificación y tipos de datos relacionados:

10.2.1 **Contribuyentes y usuarios aduaneros**

En estas bases de datos es frecuente encontrar datos personales tales como:

No.	Clasificación	Tipos
1	Datos Generales	• Datos de personas menores de 18 años. • Datos de personas mayores de 18 años.
2	Datos de Identificación	• Datos generales de identificación de la persona, familiares, beneficiarios o terceros. Entre otros como nombres, apellidos, tipo de identificación, número de identificación, fecha y lugar de expedición, estado civil. • Datos específicos de identificación de la persona. Ej: firma, nacionalidad, datos de familia, firma electrónica, firma digital, otros documentos de identificación, lugar y fecha de identificación o muerte, edad, entre otros. • Datos biométricos de la persona. Huella digital, firma digital, entre otros.
3	Datos de Ubicación	• Datos de ubicación relacionados con actividad comercial o profesional de las personas. Ej: dirección, teléfono, correo electrónico, entre otros.
4	Datos Sensibles	• Población en condición vulnerable. • Datos sobre personas en condición de discapacidad. Caracterización de condiciones sociales y/o económicas. Investigaciones fiscales o aduaneras.
5	Datos de Contenido Socio Económico	• Datos financieros, crediticios y/o derechos de carácter económico de las personas. • Datos socioeconómicos como estrato, propiedad de la vivienda o similares. • Datos de información tributaria de la persona, declaraciones, información del RUT, estados de cuenta, cobros, entre otros. • Datos patrimoniales de la persona. Ej: bienes muebles e inmuebles, ingresos, egresos, inversiones, entre otros. • Datos relacionados con la actividad económica de la persona.

10.2.2 Servidores públicos de la DIAN y sus familiares

No.	Clasificación	Tipos
1	Datos Generales	• Datos de personas menores de 18 años. • Datos de personas mayores de 18 años.
2	Datos de Identificación	• Datos generales de identificación de la persona, familiares, beneficiarios o terceros. Ejemplo Nombre, apellido, tipo de identificación, número de identificación, fecha y lugar de expedición, nombre, estado civil. • Datos específicos de identificación de la persona. Ej: firma, nacionalidad, datos de familia, otros documentos de identificación, lugar y fecha de identificación o muerte, edad, entre otros. • Datos biométricos de la persona. Ej: huella digital, ADN, geometría facial o corporal, firma digital, fotografías, videos. • Datos de la descripción morfológica de la persona. Ej: color de piel, color de iris, color y tipo de cabello, señales particulares, estatura, peso, complexión, entre otros.
3	Datos de Ubicación	• Datos de ubicación relacionados con actividad comercial o profesional de las personas. Ej: dirección, teléfono, correo electrónico, entre otros. • Datos de ubicación relacionados con la actividad privada de las personas. Ej. Domicilio, teléfono, correo electrónico, entre otros.
4	Datos Sensibles	• Datos relacionados con la salud de las personas, en cuanto a factor RH, órdenes y relación de pruebas complementarias como laboratorio, imagen, endoscópicas, patológicas, estudios, diagnósticos médicos, generales o especializados, psicológicos o psiquiátricos, medicamentos y/o tratamientos médicos o terapéuticos de cualquier tipo, entre otros. • Datos relacionados con la pertenencia a Sindicatos, organizaciones sociales, de derechos humanos, religiosas o políticas. • Población en condición vulnerable Ej. Personas de la tercera edad, personas víctimas de la violencia, personas en situación de desplazamiento forzado por violencia, madres gestantes o lactantes o cabeza de familia en situación de vulnerabilidad. • Datos relacionados con investigaciones disciplinarias.
5	Datos de Contenido Socio Económico	• Datos financieros, crediticios y/o derechos de carácter económico de las personas. • Datos socioeconómicos como estrato, propiedad de la vivienda, etc. • Datos de información tributaria de la persona. • Datos patrimoniales de la persona. Ej: bienes muebles e inmuebles, ingresos, egresos, inversiones, entre otros. • Datos relacionados con la actividad económica de la persona • Datos relacionados con la historia laboral de la persona, experiencia laboral, cargo, fechas de ingreso y retiro, anotaciones, llamados de atención, sanciones, entre otros. • Datos relacionados con el nivel educativo, capacitación y/o historial académico de la persona, etc.

No.	Clasificación	Tipos
		• Datos generales relacionados con afiliación y aportes al Sistema Integral de Seguridad Social. Ej: EPS, IPS, ARL, fechas de ingreso/retiro EPS, AFP, o entre otros. • Datos sobre gustos y/o intereses particulares. Ej: deportivos, ocio, turismo, hobbies. • Datos de antecedentes judiciales, fiscales, profesionales y/o disciplinarios de las personas.
6	Otros Datos	• Datos personales de acceso a sistemas de información. Ej: usuarios, IP, claves, perfiles.

Tabla 3. Clasificación de datos

10.2.3. Contratistas, prestadores de servicios, partes interesadas.

No.	Clasificación	Tipos
1	Datos Generales	• Datos de personas mayores de 18 años.
2	Datos de Identificación	• Datos generales de identificación de la persona, familiares, beneficiarios o terceros. Ejemplo Nombre, apellido, tipo de identificación, número de identificación, fecha y lugar de expedición, nombre, estado civil. • Datos específicos de identificación de la persona. Ej: firma, nacionalidad, datos de familia, otros documentos de identificación, lugar y fecha de identificación.
3	Datos de Ubicación	• Datos de ubicación relacionados con actividad comercial o profesional de las personas. Ej: dirección, teléfono, correo electrónico, entre otros. • Datos de ubicación relacionados con la actividad privada de las personas. Ej. Domicilio, teléfono, correo electrónico, entre otros.
4	Datos de Contenido Socio Económico	• Datos financieros, crediticios y/o derechos de carácter económico de las personas. • Datos de información tributaria de la persona. • Datos patrimoniales de la persona. Ej: bienes muebles e inmuebles, ingresos, egresos, inversiones, entre otros. • Datos relacionados con la actividad económica de la persona. • Datos relacionados con la historia laboral de la persona, experiencia laboral, cargo, fechas de ingreso y retiro, anotaciones, llamados de atención, sanciones, entre otros. • Datos relacionados con el nivel educativo, capacitación y/o historial académico de la persona, entre otros. • Datos generales relacionados con afiliación y aportes al Sistema Integral de Seguridad Social. Ej: EPS, IPS, ARL, fechas de ingreso/retiro EPS, AFP, entre otros. • Datos de antecedentes judiciales, fiscales, profesionales y/o disciplinarios de las personas.

Realizar la caracterización de los datos personales que gestiona cada dependencia o proceso, por tipos

de datos y por titulares, permite identificar los niveles de confidencialidad de los mismos, de seguridad y protección, la gestión de riesgos, el tipo de instrumentos que debe utilizar para hacer un adecuado tratamiento del dato, tales como: la autorización, el aviso de privacidad, la autorización por conducta inequívoca, la atención de consultas o requerimientos, el registro nacional de bases de datos, el tipo de almacenamiento, la supresión y/o disposición final.

11. LINEAMIENTOS FRENTE AL TRATAMIENTO DE DATOS PERSONALES

11.1 Generalidades

La DIAN realiza el tratamiento (recolección, almacenamiento, uso, circulación, suministro, transferencia, transmisión y demás actividades sobre los datos) de los datos personales de acuerdo con las finalidades y, la ley para cumplir con las actividades propias de su objeto misional. En este orden de ideas al hacer cualquier actividad que implique tratamiento, los responsables de los datos personales deben tener en cuenta los siguientes lineamientos generales:

- El tratamiento de los datos personales se podrá realizar a través de medios físicos, automatizados o digitales, de acuerdo con el tipo y forma de recolección de la información personal.

- La DIAN en cumplimiento de la Ley 1712 de 2014 “Ley de transparencia y de acceso a la información pública”, podrá publicar, en su página web o en el portal de datos abiertos, en medios públicos o masivos de comunicación, los datos personales de naturaleza pública, recabados y/o procesados en cumplimiento de su misión institucional y las notificaciones administrativas establecidas en la Ley.

- Si la DIAN debe recurrir a contratistas o terceros para realizar circulación de información que incluya datos personales, esto debe materializarse mediante la realización de acuerdos, convenios, contratos, memorandos de entendimiento o cualquier otro tipo de instrumento jurídico que respalde la transacción, evidencie adhesión a las políticas de seguridad y privacidad establecidas por la DIAN y que proteja la entrega de esta información, adicionalmente los competentes o nuevos responsables o encargados deben suscribir el compromiso de confidencialidad y no divulgación de la información reservada o clasificada para contratistas y/o terceras personas dispuesto por el Sistema de Gestión de calidad de la Entidad.

- En el caso de transferencia y/o transmisión nacional y/o internacional de datos personales, la DIAN debe asegurar los derechos y obligaciones que contiene la Ley 1581 de 2012 y su normativa complementaria. Debe suscribir un contrato, cláusula, acuerdo y/o convenio de transmisión y/o transferencia a que haya lugar en los términos de la Ley 1581 de 2012 y el Decreto 1074 de 2015 que incorporó el Decreto 1377 de 2013. Igualmente, la DIAN puede transferir o transmitir información (según corresponda), guardando las debidas medidas de seguridad, a otras entidades en Colombia o en el extranjero en ejercicio de sus funciones legales o por orden judicial, por obligación legal o contractual entre el titular y el responsable o salvaguardia de un interés público.

- Una vez cese la necesidad de tratamiento de los datos personales, los mismos podrán ser eliminados de las bases de datos de la DIAN, como medida de seguridad apropiada y conforme con los lineamientos y políticas en materia de gestión documental.

- En todos los procesos, procedimientos, formatos, sistemas de información, aplicaciones tecnológicas e informáticas, deben incorporarse los mecanismos necesarios para el adecuado

tratamiento de los datos personales que se recojan, circulen, almacenen, usen, así como para llevar a cabo las acciones correspondientes con el tratamiento, como las autorizaciones de tratamiento, los avisos de privacidad, los avisos en sistemas de videovigilancia, los avisos que adviertan la recolección de datos biométricos, entre diversos mecanismos que sean pertinentes al ciclo de vida del dato..

- Cada dependencia debe asegurar la aplicación de la política de impresión de la entidad y que en las prácticas de reciclaje de documentos físicos no se divulgue información pública clasificada (incluidos datos personales), información pública reservada. Por lo anterior no se podrán reciclar documentos que contengan datos personales semiprivados, privados, sensibles o de niñas, niños y adolescentes que correspondan a titulares de datos a cargo de la entidad.

- Se prohíbe fijar o compartir datos personales semiprivados, privados, sensibles o de niñas, niños y adolescentes en espacios físicos, carpetas públicas o sitios electrónicos de almacenamiento compartido que no cuenten con acceso restringido.

- Los nuevos desarrollos o diseños de tecnologías que requieran utilizar extractos de datos personales o que contengan información de carácter personal, se podrán llevar a cabo, previo aval de la dependencia responsable del activo de información, siempre que se cuente con la autorización del titular de la información. Además, será necesario suscribir los compromisos de confidencialidad y no divulgación de la información reservada o clasificada correspondientes y asegurar que se realice la destrucción o eliminación segura de la información, una vez finalizada la etapa de prueba o piloto.

- Cuando sea aplicada la política de “Dispositivos de punto final de usuario” consignada en el manual de políticas y lineamientos de seguridad de la Información de la DIAN, deberá contar con la autorización del titular para tratar sus datos personales al acceder a su dispositivo personal.

- La Subdirección Financiera deberá asegurar la aplicación de controles en la recolección, uso, circulación, supresión de datos personales en la administración, registro y seguimiento a las operaciones financieras.

11.2 Finalidades para el tratamiento de datos personales en la DIAN

La finalidad en el tratamiento consiste en que la entidad solo puede limitarse a tratar datos pertinentes y adecuados para los fines que son recolectados o requeridos, conforme con la misión institucional y la normativa legal vigente.

En cumplimiento del principio de finalidad y teniendo en cuenta la misión de la DIAN, las dependencias al involucrar en sus actividades el tratamiento de datos personales, deben observar que lo realizan en virtud de las siguientes finalidades generales:

- Ejercer las actividades propias de las funciones de la entidad para garantizar el cumplimiento de las obligaciones tributarias, aduaneras o cambiarias (en adelante TAC), que tienen los contribuyentes o usuarios.
- Ejercer su derecho de conocer de manera suficiente al usuario, que pretende contar con algún servicio ofrecido por la DIAN o realizar algún trámite a través de esta, prestar servicios y valorar el riesgo presente o futuro de las mismas relaciones y servicios.

- Realizar actividades estadísticas, o de atención al usuario, actividades de publicidad y convocatorias, directamente o a través de terceros derivados de cualquier vínculo jurídico o contractual cuyo objeto será ejercer funciones delegadas por la DIAN, conducentes al cumplimiento de la misión y visión institucional.
- Implementar estrategias de relacionamiento con usuarios, proveedores y otros terceros con los cuales la DIAN tenga relaciones contractuales o legales.
- Realizar invitaciones a eventos, capacitaciones, mejorar servicios y ofertar nuevos trámites y servicios, y todas aquellas actividades asociadas a la misión institucional de la entidad.
- Gestionar trámites, efectuar encuestas de satisfacción respecto de los trámites y servicios ofrecidos por la DIAN.
- Gestionar PQSRD (Peticiones, Quejas, sugerencias, Reclamos y Denuncias).
- Dar a conocer, transferir y/o transmitir datos personales dentro y fuera del país a terceros, a consecuencia de un convenio, tratado, contrato, ley o vínculo lícito que así lo requiera o para implementar servicios de computación en la nube.
- Cumplir con obligaciones laborales o contractuales frente a la calidad de servidor público de la DIAN o como contratista o proveedor de servicios en la Entidad. A esta finalidad van asociados los datos que se recolecten o almacenen sobre los servidores públicos, familiares, contratistas y personas que presten sus servicios mediante cualquier otra forma de vinculación.

En la DIAN pueden tratarse este tipo de datos mediante el diligenciamiento de contratos, formatos, acuerdos o cualquier solemnidad legal, vía telefónica, o con la entrega de documentos (hojas de vida, anexos), formatos o registros que serán tratados para todo lo relacionado con cuestiones laborales de orden legal o contractual.

En virtud de lo anterior, la DIAN utilizará los datos personales para:

1. Dar cumplimiento en lo que le aplique, a las leyes como, entre otras, de derecho laboral, seguridad social, pensiones, riesgos profesionales, cajas de compensación familiar (Sistema Integral de Seguridad Social) e impuestos, en los casos en los que aplique y corresponda.

2. Cumplir las instrucciones de las autoridades judiciales y administrativas competentes.

3. Implementar las políticas y estrategias laborales y organizacionales.

- Para propender por la seguridad de las personas, los bienes e instalaciones de la DIAN, podrán ser utilizados como prueba en cualquier tipo de proceso judicial o administrativo, respecto de los datos (i) recolectados directamente en los puntos de seguridad;(ii) tomados de los documentos que suministran las personas al personal de seguridad;(iii) y obtenidos de las videograbaciones que se realizan dentro o fuera de las instalaciones de la DIAN o sus sedes, estos se utilizarán para fines de seguridad de las personas, los bienes e instalaciones de la DIAN y podrán ser utilizados como prueba en cualquier tipo de proceso o en cumplimiento de deberes legales, contractuales o bajo requerimiento de una autoridad judicial o administrativa.
- Obtener, conservar y analizar toda la información proporcionada por los titulares de datos en uno o varios sistemas de bases de datos, en el formato que se considere más apropiado.
- Las demás relacionadas con el cumplimiento del objeto misional de la DIAN u obligaciones legales y contractuales.
- La DIAN puede llevar a cabo todas las actividades necesarias para cumplir con su objeto misional y también para cumplir con todas las obligaciones legales y contractuales que le corresponden.

En la DIAN se encuentran identificadas las finalidades para realizar el tratamiento de datos personales, las cuales están relacionadas con el Registro Nacional de Bases de Datos dispuesto por la Superintendencia de Industria y Comercio y se han definido como documento de consulta en el *Anexo 7* MN0062 *Matriz de finalidades para el tratamiento de datos personales*, para el registro de la base de datos, o para tomar la decisión sobre la pertinencia de solicitar la autorización por parte del titular del dato personal.

11.3 Tratamiento de datos personales de niñas, niños y adolescentes

La normativa en materia de datos personales establece condiciones adicionales para dotar de mayor protección a aquella información que pueda afectar los aspectos más vulnerables del individuo y de la sociedad, toda vez que la facilidad para compartir la información puede provocar consecuencias irreversibles para los titulares de los datos.

De acuerdo con lo dispuesto en el artículo 2.2.2.25.2.9. del Decreto 1074 de 2015, el tratamiento de datos personales de niños, niñas y adolescentes está prohibido, salvo que se trate de datos de naturaleza pública y cuando dicho tratamiento cumpla con los siguientes parámetros y requisitos:

- Responda y respete el interés superior de los niños, niñas y adolescentes.
- Se asegure el respeto de sus derechos fundamentales.

11.3.1 Lineamientos específicos para el tratamiento de datos de niñas, niños y adolescentes

- Cumplidos los anteriores requisitos, dentro del principio de la buena fe constitucional, quien afirme tener autorización, o afirme ser representante legal del niño, niña o adolescente, otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.
- El representante legal del menor podrá autorizar el tratamiento de los datos, siempre que este responda y respete el interés superior de los menores y que se asegure el respeto de sus derechos fundamentales.
- Respecto a la protección de los datos personales de los niños, niñas y adolescentes, serán los representantes legales, entendiéndose como quienes ejercen la patria potestad o son los tutores legales, quienes estarán legitimados para ejercer sus derechos incluyendo la presentación de solicitudes y reclamos ante la DIAN para el acceso, rectificación y supresión de los datos.
- Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, debe velar por el uso adecuado de los mismos y en este sentido debe aplicar los principios establecidos en la Ley 1581 de 2012.
- En la entidad solo se pueden recolectar datos personales de niños, niñas y adolescentes en casos que sean indispensables para el cumplimiento de las funciones misionales o no misionales, en las condiciones, principios y parámetros dados anteriormente.
- La recolección de datos personales de niños, niñas y adolescentes deberá ser validada de manera previa por la dependencia que va a tratar dichos datos. Esto se realiza para determinar si la información a recolectar es estrictamente indispensable para el propósito previsto.
- En la DIAN está prohibido circular, publicar, compartir, difundir, enviar o realizar cualquier otra acción que comprometa los datos personales de niños, niñas y adolescentes, sin la autorización de los responsables o representantes legales de acuerdo con la normativa vigente.

- Las autorizaciones de tratamiento de datos de niños, niñas y adolescentes deben señalar de manera clara la finalidad del tratamiento, así como la temporalidad de este, ser redactadas de manera clara y sencilla, para favorecer que los niños, niñas y adolescentes puedan eventualmente opinar respecto al tratamiento de sus datos.
- Solo se podrán recolectar datos personales de niños, niñas y adolescentes en expedientes laborales cuando sea necesario para que estos reciban beneficios de bienestar y seguridad social de sus representantes legales. Se solicitarán datos mínimos, con preferencia a datos que sean de naturaleza pública, en particular los contenidos en el registro civil de nacimiento.
- Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, debe velar por el uso adecuado de los mismos, por lo cual queda prohibido solicitar o divulgar datos de niños, niñas y adolescentes para soportar informes de realización de eventos, gestión de planes internos en las dependencias o aquellos que se generen en materia de transparencia y acceso a la información pública, excepto cuando se cuente con la autorización del representante legal del menor de edad.
- La divulgación de fotografías y videos que contengan imágenes de niños, niñas y adolescentes debe contar con autorización del representante legal del menor de edad. La Oficina de Comunicaciones Institucionales y la Subdirección de Desarrollo del Talento Humano o quien haga sus veces respectivamente y las demás dependencias que promuevan actividades y eventos con niños, niñas y adolescentes, deben validar que se cuente con la autorización respectiva de manera previa a la difusión de materiales que incluyan imágenes de estos.
- Los funcionarios con acceso a datos personales de niños, niñas y adolescentes deben recibir una capacitación especial previo a llevar a cabo su tratamiento. La Subdirección de Desarrollo del Talento Humano o quien haga sus veces, debe llevar un registro de estas capacitaciones.
- La Oficina de Comunicaciones Institucionales, la Subdirección de Desarrollo del Talento Humano o quien haga sus veces y las demás dependencias que hagan tratamiento de datos de niños, niñas y adolescentes, podrán solicitar la orientación por parte del Oficial de Protección de Datos Personales, o quien haga sus veces, para el adecuado tratamiento de los datos personales de los titulares mencionados.
- El registro de niños, niñas y adolescentes para el acceso a las oficinas e instalaciones de la DIAN utilizará únicamente el nombre como medio de identificación. No se deben conservar imágenes de los niños, niñas y adolescentes, salvo las contenidas en los sistemas de videovigilancia.
- Los encargados que reciban datos personales de niños, niñas y adolescentes en poder de la DIAN, previo al tratamiento, deben suscribir los acuerdos de confidencialidad y adhesión a la Política de Tratamiento de Datos Personales establecida por la DIAN.
- Los datos personales de niños, niñas y adolescentes no estarán vinculados a bases de datos que tengan interoperabilidad con otras entidades públicas. Cualquier entrega de este tipo de datos requerirá de los lineamientos y medidas que proponga el Oficial de Protección de Datos Personales, o quien haga sus veces. La dependencia responsable de la información debe verificar la pertinencia y viabilidad de la entrega o intercambio de esta información conforme con las finalidades y funciones de la entidad pública o privada que las requiera y adecuará todos los procedimientos, medidas de seguridad y protección necesarios para garantizar el interés superior de los niños, niñas y adolescentes y que se cumpla con el respeto a sus derechos fundamentales.
- En caso de que los encargados tengan acceso o realicen el tratamiento de datos de niños, niñas y adolescentes contenidos en bases de datos de la DIAN, estos deben firmar los documentos jurídicos vinculantes respectivos y la dependencia responsable de la información debe validar que cuenten con los procedimientos, capacitación y medidas de seguridad necesarios para garantizar el tratamiento de los datos personales de los niños, niñas y adolescentes de conformidad con la normativa.

11.3.2 Medidas de Seguridad para el tratamiento de datos personales de niñas, niños y adolescentes

- El acceso a bases de datos que contengan datos personales de niños, niñas y adolescentes es restringido y sólo podrá llevarse a cabo previa identificación del usuario.
- Las bases de datos con datos personales de niños, niñas y adolescentes deberán conservarse en sistemas informáticos centralizados que lleven un registro automatizado que identifique los accesos y modificaciones.
- Los archivos físicos que contengan datos personales de niños, niñas y adolescentes deberán ser resguardados en mobiliarios con cerraduras funcionales.
- Las bases de datos que contengan información de niños, niñas y adolescentes, no deben ser compartidas en repositorios de acceso público sin las debidas restricciones de acceso, tales como carpetas públicas, SharePoint, Microsoft OneDrive.
- El acceso por terceros a bases de datos personales de niños, niñas y adolescentes se realizará en casos extraordinarios previa autorización de la dependencia responsable de los datos personales.
- Previo a cualquier acceso, los terceros deberán suscribir compromisos de confidencialidad que restrinjan el tratamiento no autorizado de los datos.
- Las dependencias responsables, darán autorización cuando se requiera del envío, copiado o impresión de las bases de datos que contengan datos personales de niños, niñas y adolescentes, conforme con las condiciones técnicas del sistema de información que las gestione.
- Los encargados del tratamiento de datos de niños, niñas y adolescentes, si los hubiere (terceros externos a la DIAN), deberán acreditar que cuentan con las mismas medidas de naturaleza técnica, humana y administrativa que sean útiles, apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 e implementadas por la DIAN.

11.4 Tratamiento de datos sensibles

La Ley 1581 de 2012 define a los datos sensibles como aquellos que afecten la intimidad del titular o cuyo uso indebido pueda generar su discriminación, tales como aquellos que revelen el origen racial y étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promuevan intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos, entendiendo a estos últimos como “aquel que parte del reconocimiento de una característica física de una persona que resulta única en cada individuo y que permite así distinguirlo de cualquier otro”[1].

Cabe señalar que, a pesar de la definición de dato biométrico indicada en el párrafo anterior, el aspecto físico perceptible a través de fotografías y videos no se considera dato biométrico, salvo que se implemente alguna técnica para “la extracción de elementos particulares del rostro”[2]. Esta aclaración

[1] Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos, conceptos C-2014-273515 y C-2018- 299565

[2] Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos, Resolución N. 60460 de 2017, disponible en: http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/201706046resolucion.pdf

resulta relevante para excluir de los procedimientos y lineamientos señalados en este documento, a los sistemas de videovigilancia y fotografías contenidas en los archivos y bases de datos de la DIAN.

El tratamiento de datos sensibles en la DIAN está prohibido, a excepción de lo dispuesto en el artículo 6o. de la Ley 1581 de 2012 y a la Política de Tratamiento de Datos Personales de la DIAN. Bajo estas excepciones la entidad limita el uso y tratamiento de los datos sensibles en los siguientes casos:

- El titular haya dado su autorización explícita a dicho tratamiento, salvo excepción de la ley.
- El tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado.
- El tratamiento se refiera a actividades de asociación a ONG, Fundaciones, Sindicatos, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del titular.
- El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

En el tratamiento de datos personales sensibles, cuando dicho tratamiento sea posible, conforme a los casos anteriormente relacionados, debe cumplirse las siguientes obligaciones:

- Informar al titular que, por tratarse de datos sensibles, no está obligado a autorizar su tratamiento.
- Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de tratamiento son sensibles y la finalidad del tratamiento, así como obtener su consentimiento expreso.

11.4.1 Lineamientos específicos para el tratamiento de datos sensibles

- Las autorizaciones para el tratamiento de datos sensibles deben señalar de manera clara la finalidad del tratamiento, así como la temporalidad de este.
- Las autorizaciones de tratamiento de datos sensibles son por escrito o de manera verbal y deben conservarse de acuerdo con la Tabla de Retención Documental y las políticas y lineamientos en materia de gestión documental.
- No se podrán recolectar datos personales de carácter sensible con el fin de realizar procesos de reclutamiento y selección.
- En los expedientes laborales, solo se podrá incluir información sensible que tenga como finalidad acreditar las cualificaciones requeridas para el rol o vacante.
- No se podrán divulgar datos sensibles salvo que una orden judicial lo disponga.
- Las solicitudes de información en cumplimiento de la Ley de Transparencia no deberán incluir datos personales sensibles.
- Los funcionarios con acceso a datos personales sensibles deben recibir capacitación especial previo a llevar a cabo su tratamiento. La Subdirección Escuela de Impuestos y Aduanas o quien haga sus veces debe llevar registro de las capacitaciones.
- El uso de datos biométricos como instrumento de identificación para el acceso a las oficinas y sistemas informáticos de la DIAN, debe contar con autorización previa expresa del titular de los

datos. En el caso de servidores públicos de la DIAN, la autorización debe conservarse en su historia laboral o el repositorio definido por la entidad.

- Previo a determinada transmisión y transferencia de bases de datos personales sensibles, el Oficial de Protección de Datos Personales, o quien haga sus veces, debe validar que se hayan implementado los procedimientos y medidas de seguridad necesarias para asegurar el tratamiento adecuado de los datos personales sensibles.
- Los funcionarios que realicen recolección de datos personales sensibles de la DIAN, previo al tratamiento, deben suscribir los compromisos de confidencialidad y adhesión a las Políticas de Tratamiento de Datos Personales establecidas por la DIAN.
- La Subdirección de Gestión del Empleo Público o quien haga sus veces, como responsable del reclutamiento, selección y vinculación de personal, define los datos personales sensibles que se solicitarán a los aspirantes y servidores vinculados.
- A más tardar, al momento de la vinculación, se deberá obtener la autorización para integrarla a la historia laboral.
- En caso de ya existir vinculación al momento de entrar en vigencia los presentes lineamientos, deberá recolectarse la autorización a través del ingreso al sistema por parte de los funcionarios o por recolección masiva definida por la entidad.
- La Subdirección de Compras y Contratos o quien haga sus veces, recolectará la información en caso de tercerización de servicios, quienes proporcionarán los datos personales sensibles (si se necesitan recoger y se encuentran dentro de las excepciones) y suscribirán la autorización para el tratamiento.
- Así mismo suscribirán los documentos jurídicos vinculantes que garanticen la protección de los datos personales sensibles en los archivos y bases de datos de la DIAN a los que tengan acceso.
- Para los datos personales recolectados en el marco de seguridad y salud en el trabajo de la entidad, la Subdirección de Gestión del Empleo Público, deberá aplicar los controles necesarios para salvaguardar los datos personales clasificados como semiprivados, privados y sensibles. Adicional, revisar la pertinencia de conservar los datos personales recolectados según el principio de proporcionalidad y temporalidad. El cumplimiento de estos lineamientos se extiende a las empresas administradoras de riesgos laborales, empresas promotoras de salud, cajas de compensación y demás empresas relacionadas.
- Al realizar las investigaciones disciplinarias, así como, las investigaciones fiscales y aduaneras es imperativo preservar la confidencialidad de los datos personales y cumplir con la finalidad para la cual se realiza el tratamiento.

11.4.2 Medidas de Seguridad para datos sensibles

- El acceso a bases de datos que contengan datos personales sensibles es restringido y sólo podrá llevarse a cabo previa identificación del usuario.
- Las bases que contengan datos sensibles no deben ser compartidas en repositorios de acceso público, tales como carpetas públicas, SharePoint, Microsoft OneDrive o portal web.
- Las bases de datos con datos personales sensibles deberán conservarse en sistemas informáticos que cuenten con un registro automatizado que identifique los accesos y modificaciones.
- Los archivos físicos que contengan datos personales sensibles deberán ser resguardados en mobiliarios con cerraduras funcionales.
- El Oficial de Protección de Datos Personales, o quien haga sus veces, tiene la facultad de revisar periódica o esporádicamente los registros de acceso a bases de datos para detectar accesos no autorizados.

- El acceso por terceros a bases de datos personales sensibles sólo se realizará en casos extraordinarios, previa autorización de la dependencia responsable de los datos personales. Anterior a cualquier acceso, los terceros deberán suscribir compromisos de confidencialidad que restrinjan el tratamiento no autorizado de los datos.
- La Oficina de Seguridad de la Información dará instrucciones, conforme con las condiciones técnicas del sistema de información que las gestione, sobre la prohibición de envío, copiado o impresión de las bases de datos con datos personales sensibles. Por lo tanto, cualquier reproducción de estas bases de datos deberá ser viabilizada por el Oficial de Protección de Datos Personales o quien haga sus veces.
- Los encargados del tratamiento de datos sensibles (terceros externos a la DIAN) deben acreditar que al menos cuentan con las mismas medidas de seguridad y privacidad implementadas por la DIAN para el adecuado tratamiento de los datos.

11.5 Protección de datos personales en los Sistemas de Computación en la Nube (E-Clouding)

La DIAN dispone del MN-IIT-0072 Manual de Políticas y Lineamientos de Seguridad de la Información que detalla los lineamientos relacionados con computación en la nube, los cuales deben ser rigurosamente cumplidos en lo que respecta a la protección de datos personales.

11.6. Protección de datos en el monitoreo en red, correo electrónico y sistemas de información de la entidad

La DIAN debe proteger los datos personales de naturaleza no pública relacionados en el proceso de monitoreo de la red, correo electrónico y sistemas de información (incluidas las actividades sobre los datos personales como consultas, eliminación, actualización de columnas de bases de datos), según lo establecido en el del MN-IIT-0072 Manual de Políticas y Lineamientos de Seguridad de la Información en especial lo consignado en el numeral “5.4.16 Actividades de seguimiento”.

11.7. Anonimización de datos personales

La anonimización de datos se refiere al proceso de ocultar o eliminar los datos de manera que no sea posible identificar a las personas o entidades individuales a las que pertenecen esos datos. El objetivo principal de la anonimización es preservar la privacidad y la confidencialidad de la información que no sea de naturaleza pública, por tal motivo es necesario que la DIAN tenga en cuenta lo siguiente:

- Cuando prevalezca la necesidad de publicar, divulgar, circular o entregar información por cumplimiento de ley y existan datos personales que no sean de naturaleza pública, a estos se les debe aplicar un proceso de anonimización.

12. GESTIÓN Y MODELAMIENTO DEL FLUJO DE DATOS PERSONALES

La Ley 1581 de 2012 define el tratamiento de datos personales como cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. En este orden de ideas se enunciarán los lineamientos necesarios para tener en cuenta en la recolección, uso, circulación, supresión o disposición final de los datos personales en la DIAN.

En la DIAN para el tratamiento de datos personales debe cumplirse con los principios establecidos en la Ley 1581 de 2012 y mencionados en el presente manual: legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

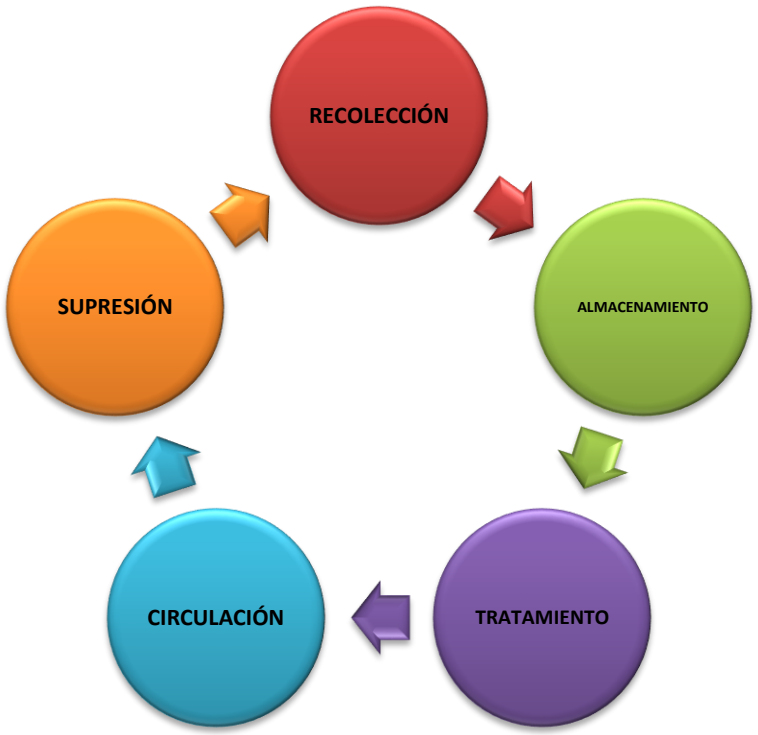
Las dependencias de la DIAN solo pueden solicitar datos personales en cumplimiento de las funciones asignadas. Ningún funcionario de la entidad podrá solicitar o tratar información personal que no tenga relación con la misión y funciones de la DIAN y con las finalidades de la recolección previstas en el presente manual.

Cuando se desarrollen actividades directamente o a nombre de la entidad, que involucren la recolección o recopilación de datos personales, la dependencia responsable deberá tener en cuenta:

- La finalidad para la cual solicita el (los) dato(s) personal (es) (para qué).
- La pertinencia de recopilar el dato personal (qué clase de dato se va a solicitar, es decir, dato público, dato semiprivado, dato privado, dato sensible o datos de niños, niñas y adolescentes).
- El medio por el cual se va a obtener la información (manual, automatizada, video, llamada, audio, página web, evento entre otros).
- El medio de conservación y custodia de esta información (físico o electrónico).
- La supresión o disposición final del (os) dato (s) recolectado (s).

12.1. Etapas del ciclo de vida del dato

Para entender y asociar las distintas acciones que implican el tratamiento de datos personales, es importante diferenciar las etapas del ciclo de vida del dato, las cuales se explican con posterioridad en este documento:



12.2. Recolección o recopilación de datos personales

Hace referencia al momento en que la DIAN tiene acceso al dato personal para integrarlo en sus archivos y bases de datos:

- La recolección de datos debe limitarse a aquellos que sean pertinentes y adecuados para la finalidad por la cual son obtenidos y no podrán recopilarse por medios engañosos o fraudulentos.
- De acuerdo con los principios jurídicos que rigen la actuación administrativa, la recolección de datos por parte de la DIAN, solo podrá realizarse en el ámbito de las facultades que le confiera la ley.
- Previo a cualquier tratamiento y, a más tardar al momento de recolectar los datos personales, se debe obtener la autorización de los titulares. Sin embargo, la Ley 1581 de 2012 exceptúa a las entidades públicas que requieran la información en ejercicio de su objeto misional o funciones legales o por orden judicial, por lo que la DIAN no necesitará autorización para recolectar y tratar datos cuando se trate de dichas actividades.
- En caso de hacer la recolección a través de medios físicos, deberá considerar la serie o tipo de activo de información al que pertenecen estos datos y determinar los usuarios que tienen acceso y los medios seguros en los que se almacenarán estos datos.
- Independientemente de que la recolección de los datos requiera o no autorización, el aviso de privacidad debe implementarse conforme con el medio en que se está recolectando la información. En el capítulo de instrumentos necesarios para el adecuado tratamiento de datos, se menciona el tipo de aviso de privacidad que se requiere por cada medio utilizado. (Ver capítulo 17. Instrumentos para el tratamiento de datos personales).

La dependencia responsable de recolectar o recopilar datos personales, debe tener presente los siguientes aspectos:

- Comunicar al titular sobre las políticas y procedimientos que tiene la entidad para el tratamiento de sus datos (aviso de privacidad).
- Siempre que se trate de la recolección o recopilación de datos personales, el responsable de la dependencia debe garantizar que el titular de los datos conozca los derechos, la finalidad y las medidas que adopta la entidad para preservar la seguridad y confidencialidad de la información suministrada, esta información se conoce como aviso de privacidad.
- Los derechos que le asisten de acuerdo con la Ley 1581 de 2012 y la Política de Tratamiento de Datos Personales adoptada por la DIAN.

La DIAN recolecta datos que le son suministrados por contribuyentes, usuarios aduaneros, servidores públicos, contratistas y encargados, para lo cual se debe tener en cuenta lo siguiente:

Contribuyentes y usuarios aduaneros

- Los contribuyentes y usuarios aduaneros suministran datos de manera presencial o virtual en los canales u oficinas de la DIAN aportando datos personales de identificación, ubicación, información patrimonial y actividades económicas, entre otros, dependiendo el tipo de servicio o trámite que demande de la entidad.
- Dependiendo el tipo de trámite a realizar, la DIAN recolectará la autorización para el tratamiento de datos personales (casos no misionales).
- La DIAN asociará los datos personales recolectados del contribuyente o usuario aduanero a las

bases de datos de la entidad, para proporcionar los servicios y trámites al público, así como la vigilancia y control de la recaudación fiscal y el control aduanero.
- Dependiendo de la operación a realizar, la DIAN establecerá los accesos a la información y los plazos de conservación de conformidad con la normativa y lineamientos establecidos en materia de gestión documental.

Servidores públicos

- La Subdirección de Gestión del Empleo Público o quien haga sus veces, lleva a cabo la vinculación, el reclutamiento y selección del personal y la provisión mediante sistema de carrera administrativa, el proceso de vinculación de personal; de estos dos procesos solicita información de carácter personal a los aspirantes que cubrirán las vacantes incluyendo información de antecedentes, hoja de vida con datos como la identificación, domicilio, estudios, experiencia laboral, datos de familiares, afiliaciones al sistema de seguridad social, datos biométricos Durante el tiempo de vinculación igualmente recolecta y trata datos de los servidores públicos de la entidad, familiares y de niños, niñas y adolescentes, hasta su retiro definitivo o hasta el cumplimiento de las obligaciones legales, de control o administrativas.
- A más tardar, al momento de la vinculación, se deberá recolectar la autorización e integrarla al expediente laboral.
- Así mismo, generará los registros físicos (fotografías y/o huella digital, entre otros) necesarios para fines de identificación y acceso a las instalaciones de la DIAN.
- El Oficial de Protección de datos personales, o quien haga sus veces, validará la viabilidad de recolectar para el proceso de Talento Humano, algunos datos sensibles o de niños, niñas y adolescentes.
- La Subdirección de Gestión del Empleo Público o quien haga sus veces, integrará la historia laboral y restringirá el acceso a la información del servidor público para permitir la consulta y actualización.

Contratistas y partes interesadas

- La Subdirección de Compras y Contratos o la dependencia que haga sus veces recolectará la información en caso de tercerización de servicios. Los contratistas proporcionarán su información incluyendo la información de antecedentes y suscribirán la autorización para el tratamiento de sus datos personales, así como los documentos jurídicos vinculantes para asegurar la protección de los datos personales en los archivos y bases de datos de la DIAN a los que tengan acceso.
- La Subdirección de Compras y Contratos o la dependencia que cumpla sus funciones correspondientes, publicará exclusivamente la información proporcionada por los contratistas de acuerdo con las disposiciones aplicables en materia de transparencia y acceso a la información pública. Esta divulgación se limitará estrictamente a datos personales que sean de carácter público y estén permitidos para su difusión según las regulaciones vigentes.

12.2.1. Consideraciones de seguridad para la recolección de datos en sistemas de información

En caso de realizar la recolección a través de medios digitales, se debe considerar lo siguiente:

- Toda aplicación, desarrollo o formato electrónico destinado a la recolección de datos personales debe contar con las medidas de privacidad y seguridad de la información. Esto incluye la autorización para el tratamiento de datos (cuando aplique) y el aviso de privacidad.

- Toda plataforma de recolección de datos personales debe usar la versión vigente del protocolo de seguridad TLS (Transport Layer Security).
- Los procesos de registro y recolección de información en las aplicaciones digitales deben implementar manejo de sesión de usuario.
- Todos los sistemas de recolección de información deben considerar la autenticación como proceso para recolectar la información.
- De preferencia el proceso de registro y recolección debe contemplar el doble factor de autenticación.
- Todo sistema que registre/recolecte información de datos personales debe considerar tener un sistema de logs y auditoría.
- La comunicación entre la aplicación y las personas deben usar canales seguros de comunicación.
- El desarrollo de sistemas de información que considere recolección de datos personales debe considerar la seguridad y privacidad por diseño y por defecto.
- El sistema de información que se considere para la recolección de datos personales debe basarse en el principio del menor privilegio para la recolección de la información.

12.2.2. Recolección de datos personales que requieren autorización del titular

Para determinar si la dependencia debido a sus funciones y respecto a los datos personales que recolecta requiere autorización del tratamiento por parte del titular, es imprescindible que se tenga el conocimiento si la recolección de los datos es de naturaleza pública o corresponde a un tema misional (en cuyos casos no requerirá de la misma) o la recopilación de los datos obedece al cumplimiento de las funciones de los procesos no misionales en la DIAN.

Una vez identificada la necesidad de recoger la autorización y dependiendo del medio de recolección de la información, la dependencia responsable debe obtener la autorización para el tratamiento de los datos personales recolectados, a través de los siguientes medios:

- Por escrito, cuando el dato personal se obtenga por este medio.
- De forma oral, cuando se comunique y acepte expresamente el consentimiento de las personas (en este caso se deberá dejar evidencia de esta comunicación).
- De manera inequívoca, cuando se indique, comunique o avise de manera expresa que la realización de una acción realizada por el titular de los datos frente a la entidad implica la aceptación de la finalidad de la actividad. y da su autorización para este fin.

La forma de comunicar estas acciones, dependen del medio que se esté empleando de acuerdo con lo que se establece en el Capítulo 17. Instrumentos para el tratamiento de datos personales.

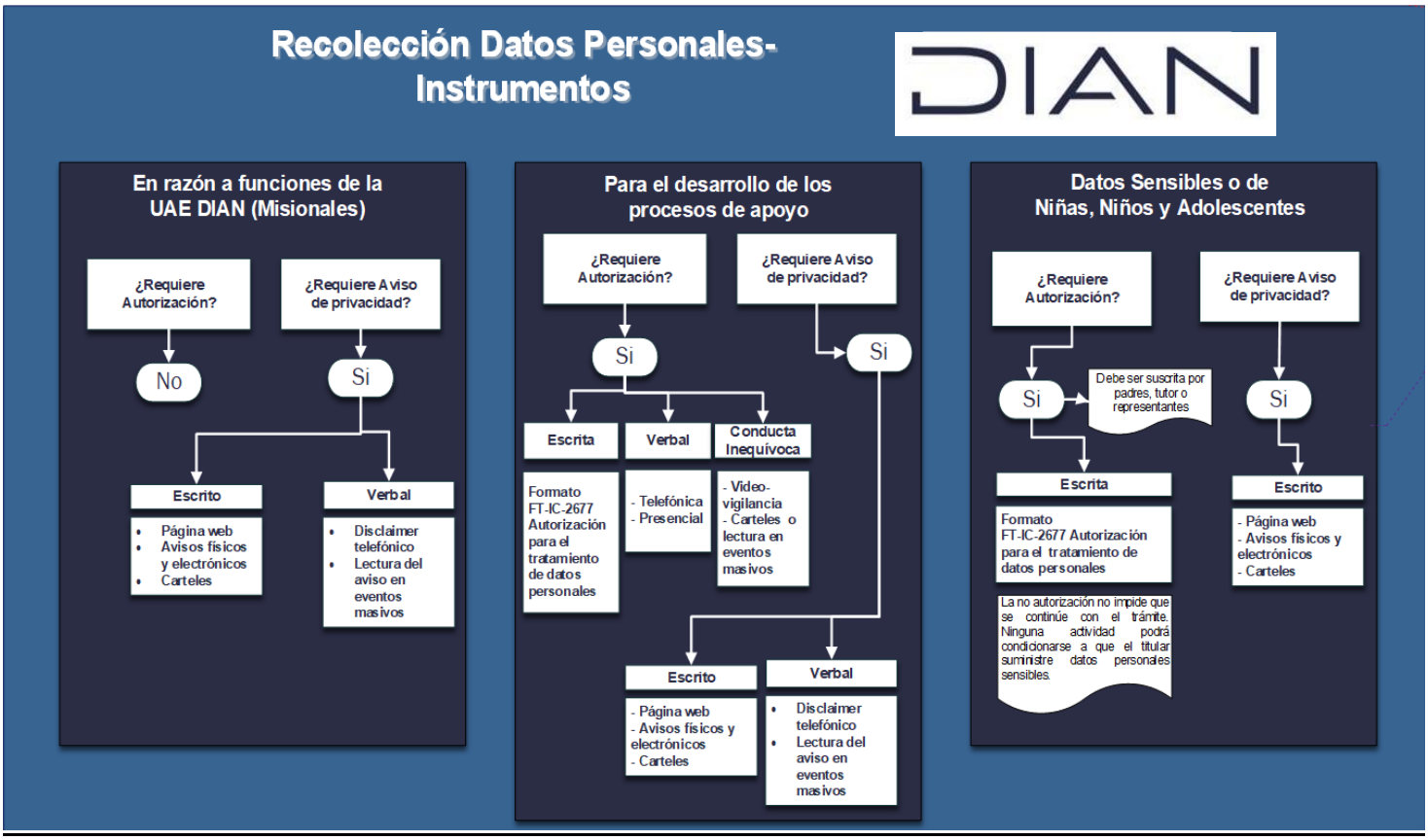


Ilustración 2. Recolección de datos personales

12.2.3. Recolección de datos que no requieren autorización

Para decidir sobre la pertinencia o no de solicitar la autorización, debe revisarse el mapa de procesos de la entidad y clasificar el tipo de recolección dependiendo del proceso al que corresponde esta información. Ahora bien, si las dependencias pertenecen a un proceso no misional, pero recolecta información para apoyar temas misionales es viable omitir la autorización, caso en el cual debe darse únicamente el aviso de privacidad. Si por el contrario la recolección se realiza por el desarrollo de actividades de un proceso no misional, debe implementarse la autorización, recolectarse y dejar un repositorio de las evidencias de esa recolección, en caso de ser requeridas por el titular o por un ente de control.

Si los datos personales los obtiene la DIAN mediante cumplimiento de convenios o acuerdos nacionales o internacionales, su captura o recolección no requieren autorización porque existe una relación directa entre la información solicitada y el cumplimiento de su misión.

No se requerirá autorización de los titulares cuando los datos personales se obtengan a través de los sistemas interoperables de la administración pública y cuando sean necesarios para garantizar el cumplimiento de las funciones de la DIAN, adicionalmente porque se ha corroborado que la entidad u organización que proporciona la información cuenta con las políticas y medidas necesarias para asegurar una adecuada protección de los datos personales.

Cabe señalar que las excepciones se refieren únicamente al requisito de autorización del tratamiento y no exime a la DIAN de cumplir con las demás obligaciones para el uso, almacenamiento, conservación y supresión de los datos personales de los que la entidad sea responsable.

12.3. Almacenamiento y conservación de los datos personales obtenidos

Es una de las acciones que la Ley señala como tratamiento e implica que el responsable que almacene los datos (ya sea en medios digitales o físicos) adopte las medidas adecuadas para asegurar la integridad del dato personal y la confidencialidad de la información.

La DIAN dispondrá de los medios físicos y técnicos adecuados para el almacenamiento de la información y para el control del cumplimiento del Régimen General de Protección de datos personales.

La DIAN contará por sí misma o a través de un tercero, con espacios e instalaciones necesarias para el correcto funcionamiento de sus archivos (incluyendo servidores para resguardar las bases de datos).

Independiente de la forma o medio en que fueron recopilados los datos personales, las diferentes dependencias de la DIAN deben adoptar todas las medidas necesarias para preservar la seguridad y privacidad de la información obtenida, de tal manera que se minimice el riesgo de pérdida, adulteración, o difusión no autorizada.

Las dependencias o procesos que recopilan datos personales de los usuarios, a nivel central, las direcciones seccionales, los canales de atención y los puntos de contacto, deben informar a la dependencia responsable del tratamiento de estos datos. Lo cual, permitirá que dicha dependencia ejerza el control sobre las autorizaciones otorgadas por los titulares de los datos. La información recopilada se almacenará y archivará en el repositorio de información de la dependencia que la recolecta, o en las series documentales que se creen u organicen específicamente para este fin.

Una vez cumplida la finalidad para la cual fueron recolectados los datos, estos deben conservarse de manera segura, según el medio de almacenamiento establecido (físico o digital) y con restricción de acceso a los mismos. Corresponde a cada jefe de dependencia designar de manera expresa, a un número limitado de funcionarios que podrán tener acceso de consulta a esta información.

Para la conservación y custodia de la información de datos personales obtenida de manera física o electrónica, cada dependencia debe cumplir con las siguientes disposiciones:

ALMACENAMIENTO FÍSICO	ALMACENAMIENTO ELECTRÓNICO
Carpetas, archivadores, mobiliario, espacios específicos de archivo internos y externos	Servidor externo propio o a cargo de un tercero.
Las autorizaciones obtenidas a través de medios físicos serán registradas y controladas por las dependencias responsables de su recolección y almacenadas en la serie que le corresponda conforme con la TRD de la dependencia.	Toda información de datos personales que quede registrada directamente en una base de datos debe disponer de esquemas de seguridad que garanticen su conservación y recuperación ante posibles eventualidades (Backup), y el acceso restringido a la misma, para lo cual la dependencia responsable escalará las respectivas solicitudes a la Dirección de Gestión de Innovación y Tecnología o la dependencia que haga sus veces.

ALMACENAMIENTO FÍSICO	ALMACENAMIENTO ELECTRÓNICO
Se debe almacenar en la serie documental que le corresponda, la información suministrada por los titulares junto con la autorización o la evidencia de la autorización de tratamiento de los datos.	El desarrollo de sistemas de información que considere almacenamiento de datos personales debe considerar la seguridad y privacidad por diseño y por defecto.
Es necesario que una vez usado el medio físico (papel, entre otros) sea almacenado en el repositorio seguro al que corresponde.	En el evento de obtener las autorizaciones a través de centros de llamadas, las grabaciones serán custodiadas por el centro y monitoreadas por la dependencia designada.
La administración y conservación de las series que contienen "datos personales" debe realizarse conforme con los procedimientos vigentes en materia de gestión documental y archivo.	
La conservación de los datos personales solo podrá realizarse durante el tiempo que sea razonable y necesario de conformidad con las finalidades que justifican el tratamiento.	La conservación de los datos personales solo podrá realizarse durante el tiempo que sea razonable y necesario de conformidad con las finalidades que justifican el tratamiento.
	La información con datos personales de titulares, recolectados de manera electrónica, no puede estar archivada o almacenada en equipos personales asignados a los funcionarios.
	El sistema de información que se considere para el almacenamiento de datos personales debe basarse en el principio del menor privilegio para el almacenamiento de la información.
Implementar las medidas de seguridad físicas y electrónicas necesarias y disponibles para impedir la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de los datos personales. Se deberá crear un registro, que podrá ser automatizado, de todos aquellos que tengan acceso a los datos personales en los que la DIAN sea responsable.	Implementar las medidas de seguridad físicas y electrónicas necesarias y disponibles para impedir la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de los datos personales. Se deberá crear un registro, que podrá ser automatizado, de todos aquellos que tengan acceso a los datos personales en los que la DIAN sea responsable.
Conservar las autorizaciones de los titulares para el tratamiento de sus datos personales durante la vigencia del tratamiento y de manera posterior a este, de conformidad con los plazos señalados en el programa de gestión documental de la DIAN y las tablas de retención documental.	Conservar las autorizaciones de los titulares para el tratamiento de sus datos personales durante la vigencia del tratamiento y de manera posterior a este, de conformidad con los plazos señalados en el programa de gestión documental de la DIAN y las tablas de retención documental.
De acuerdo con el procedimiento de incidentes de la DIAN se establece que es necesario informar al Oficial de Protección de Datos cualquier violación de seguridad que afecte a los archivos y bases de datos que contengan datos personales procesados por la DIAN. Este reporte debe realizarse en caso de detectar cualquier vulneración a la seguridad de dichos archivos y bases de datos que puedan comprometer la integridad, confidencialidad o disponibilidad de	De acuerdo con el procedimiento de incidentes de la DIAN se establece que es necesario informar al Oficial de Protección de Datos cualquier violación de seguridad que afecte a los archivos y bases de datos que contengan datos personales procesados por la DIAN. Este reporte debe realizarse en caso de detectar cualquier vulneración a la seguridad de dichos archivos y bases de datos que puedan comprometer la integridad, confidencialidad o disponibilidad de

ALMACENAMIENTO FÍSICO	ALMACENAMIENTO ELECTRÓNICO
los datos personales manejados por la DIAN.	los datos personales manejados por la DIAN.
	Si la información no queda registrada de manera automática en una base de datos, esta debe conservarse de manera segura, de ser posible en directorios de red disponibles y en una subcarpeta creada de manera exclusiva para este fin. Corresponde a cada jefe de dependencia, realizar la solicitud a la Coordinación de Soporte Técnico al Usuario o quien haga sus veces, tanto para la creación de la carpeta como para la autorización de los usuarios que tengan acceso a la misma.
No pueden almacenarse bases de datos físicas con información personal obtenidas por medios distintos a los de las funciones de la DIAN, o de terceros que no estén debidamente respaldadas por un documento legítimo que autorice su almacenamiento en las dependencias de la entidad.	No pueden almacenarse bases de datos electrónicas con información personal, obtenidas por minería de datos, inteligencia artificial, agregadas, entre otras formas de conformación, que se procesen por temas distintos a los de las funciones de la DIAN, o bases de datos de terceros que no estén debidamente respaldadas por un documento legítimo que autorice su almacenamiento digital por parte de la DIAN.
Registrar en las bases de datos la leyenda “Reclamo en trámite” e “información en discusión judicial” cuando se actualicen los supuestos normativos señalados en la Ley 1581 de 2012.	Registrar en las bases de datos la leyenda “Reclamo en trámite” e “información en discusión judicial” cuando se actualicen los supuestos normativos señalados en la Ley 1581 de 2012.

Tabla 4. Conservación o custodia de información

12.4. Tratamiento de los datos personales

Se entenderá por tratamiento cualquier uso, acceso, disposición, reproducción y divulgación de los datos personales realizados por prestadores de servicios y encargados, tales como funcionarios (sin importar el tipo de vinculación), pasantes, practicantes, asesores, consultores, contratistas, prestadores de servicios de vigilancia, o almacenamiento en la nube. La aplicación de la normativa colombiana no está limitada al uso de los datos personales dentro del territorio nacional, por lo que DIAN está obligada a cumplir con las obligaciones de la Ley 1581 de 2012 y normas concordantes.

El tratamiento de los datos personales que realiza la DIAN se encuentra descrito en la Política de tratamiento de datos personales.

En caso de que alguna dependencia identifique un nuevo tratamiento diferente de los descritos en la Política de tratamiento de datos personales, debe informar a la dependencia correspondiente y determinar los documentos que deban ser actualizados.

En caso de que una dependencia diferente de la que recolectó inicialmente el dato personal requiera utilizarlos, se podrá hacer siempre y cuando en la autorización se haya informado sobre dicho uso, se encuentre en la Política de tratamiento de datos personales o sea un uso previsible dentro de las actividades legales, constitucionales o misionales.

Cada dependencia debe asegurar que en las prácticas de reciclaje de documentos físicos no se divulgue información confidencial ni datos personales. Por lo anterior no se podrán reciclar hojas de vida, ni certificados académicos o laborales, ni resultados de exámenes médicos ni ningún documento que contenga información que permita identificar a una persona.

12.4.1. Acceso y uso de los datos personales obtenidos

Teniendo en cuenta que sólo deben recolectarse los datos personales que sean estrictamente necesarios para el cumplimiento de las finalidades del tratamiento, cada dependencia debe limitar el procesamiento de datos personales al mínimo necesario y siempre asociado a la finalidad para la cual fueron obtenidos, de acuerdo con el aviso de privacidad dado a conocer a los titulares.
El acceso a los datos personales estará restringido, de conformidad con los roles asignados a cada servidor público de la DIAN.

12.4.2. Consideraciones de seguridad para el tratamiento de datos en sistemas de información

La DIAN como responsable del tratamiento de datos personales y en cumplimiento del régimen general de protección de datos personales, debe implementar en la fase de tratamiento de información de datos personales los siguientes controles de seguridad acordes con la Política de Seguridad y Privacidad de la Información y las regulaciones vigentes, entre ellos están:

- Todo tratamiento de datos personales, de preferencia las operaciones que involucren supresión, modificación, corrección, deben contar con sistemas de logs y auditoría que se puedan supervisar a través de herramientas tecnológicas como soportes del proceso.
- El tratamiento de datos personales debe usar los principios de control de acceso definido para los sistemas de información.
- El sistema de control de acceso debe tener sistemas de auditoría disponibles para revisiones.
- El Sistema de control de acceso debe usar la autenticación y autorización como funciones vitales del sistema.
- De preferencia utilizar el doble factor de autenticación en los sistemas de información, donde se hace algún tratamiento de datos personales.
- En caso de ser necesario hacer descargas de la información contenida en algún sistema de información, es preciso que esta sea descargada a repositorios centrales y no a estaciones de trabajo o computadores personales.
- La extracción parcial de datos personales de sistemas de información se debe realizar con accesos controlados y debe estar limitado al cumplimiento de los principios de finalidad y circulación restringida.
- Toda estación local que haga uso de archivos que contengan datos personales y que requieran un tratamiento debe tener las medidas de seguridad provistas por la Oficina de Seguridad de la Información o quien haga sus veces.
- Utilizar técnicas como cifrado de datos (para control de acceso en reposo y en tránsito), etiquetado de datos, anonimización de datos, accesos restringidos, control de versiones de información, control de privilegios, controles de seguridad y de disposición final para bases de datos personales que se hayan procesado en fases de desarrollo y su uso ya no sea necesario.

12.5. Circulación de la información personal

Implica compartir la información personal contenida en bases de datos, bien sea entre dependencias de las dependencias de la DIAN o a terceros.

La normativa exige que cualquier envío de información dentro o fuera del país se realice previa autorización del titular, a excepción de los casos establecidos en la Ley y los decretos que la reglamentan.

En caso de que la DIAN deba comunicar los datos personales contenidos en las bases de datos que administra a otras entidades públicas con la finalidad de hacer más eficiente el cumplimiento de los objetivos del estado, debe ceñirse a la Circular externa conjunta No.04 de 2019 (SIC-ANDJE) para el tratamiento de datos personales en sistemas de información interoperables por las entidades de la rama ejecutiva. En cuanto a servicios ciudadanos digitales, la DIAN debe observar lo dispuesto en el Decreto 620 de 2020.

En la DIAN se identifican varios mecanismos que las normas y disposiciones internas de la entidad, consagran viables para la circulación y entrega de datos personales:

- Entrega de información con datos personales
- transmisión nacional e internacional de datos personales
- Transferencia nacional e internacional de datos personales
- Intercambio con datos personales
- Interoperabilidad de datos personales

En la circulación de la información es necesario tener clara la identificación de tres roles importantes en el tratamiento de Datos Personales:

Titular	Responsable del tratamiento	Encargado del tratamiento
• Persona natural cuyos datos personales sean objeto de tratamiento.	• Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.	• Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

Fuente: https://normograma.dian.gov.co/dian/compilacion/docs/ley_1581_2012.htm

Cada vez que se haga circulación de datos bajo las figuras mencionadas es necesario tener suficientemente claro qué rol asumirá la entidad frente al tratamiento, el cual puede ser responsable o encargado del tratamiento, los deberes y responsabilidades frente a cada rol, están definidos en los art. 17 y 18 de la Ley 1581 de 2012.

12.5.1. Mecanismos de circulación de los datos personales

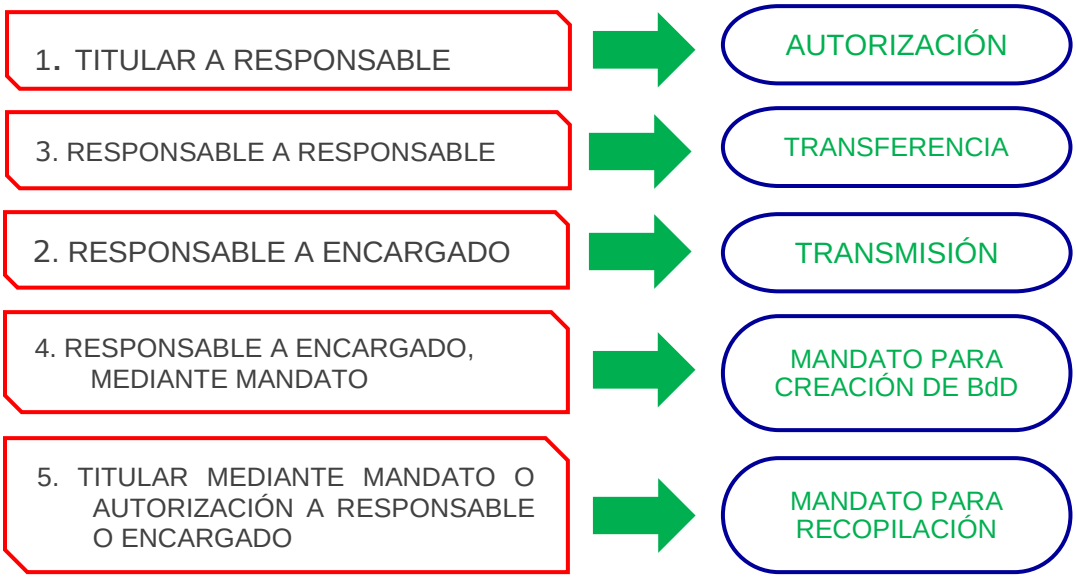


Ilustración 3. Mecanismos de circulación

12.5.2. Entrega de información con datos personales

12.5.2.1. Información interna

La entrega de información en la entidad está regulada por la circular interna No. 026 de 2020 y las normas que la modifiquen o complementen, sin embargo, en tratamiento de datos personales teniendo en cuenta los principios de finalidad y de acceso y circulación restringida, los datos o bases de datos constituidos, solo deben tratarse por las dependencias o procesos responsables de esa información personal. En razón a lo anterior, las demás dependencias de la DIAN que soliciten datos personales de los titulares de una base específica deberán revisar si debido a sus funciones o los procedimientos que desarrolla la dependencia o proceso, le permiten interoperar la información con dependencias internas.

12.5.2.2. Entrega de datos a autoridades administrativas, de control o judiciales

La entrega de información con datos personales a autoridades administrativas, de control o judiciales está considerada dentro de las excepciones de circulación, es por esta razón que la entidad mediante la Circular 026 de 2020 consideró en qué condiciones debe efectuarse esta transacción.

Entrega de información a autoridad administrativa: la DIAN remitirá la información en los términos y bajos las condiciones señaladas por la Circular 026 de 2020 y siempre y cuando medie disposición legal o acto administrativo que lo ordene y la entidad u organismo receptor garantice contar con las medidas de seguridad y privacidad para tratar esos datos.

En el documento de entrega de la información se debe incluir el modelo de clausula o de instrucción sobre la disposición final que se les dará a los datos una vez haya cesado el uso y finalidad por la cual fueron entregados. Ver *Anexo 5 MN0062. Cláusulas*.

12.5.2.3. Atención de solicitudes de información personal por parte de autoridades públicas.

La DIAN está comprometida con el principio de coordinación y colaboración armónica entre entidades del Estado. En este sentido, para la atención de solicitudes de información personal por parte de cualquier autoridad pública, se debe dar cumplimiento a lo contenido en la Ley 1581 de 2012 en consonancia con la Circular 004 de 2019 de la Agencia Nacional de Defensa Jurídica del Estado y la Superintendencia de Industria y Comercio.

Para atender estas solicitudes se debe tener en cuenta, como mínimo, lo siguiente:

- Verificar la naturaleza de la información solicitada.
- Verificar el tipo de entidad pública.
- Verificar la competencia del solicitante.
- Verificar la finalidad para la cual se requiere la información y si la entidad es competente para solicitarla.

Indicar a la entidad pública que al recibir esta información deberá garantizar los derechos fundamentales del titular de datos personales, de acuerdo con lo previsto en la sentencia C-748 de 2011 deberá "*(i) guardar reserva de la información que les sea suministrada por los operadores y utilizarla únicamente para los fines que justificaron la entrega, esto es, aquellos relacionados con la competencia funcional específica que motivó la solicitud de suministro del dato personal; (ii) informar a los Titulares del dato el uso que le esté dando al mismo; (iii) conservar con las debidas seguridades la información recibida para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento; y (iv) cumplir con las instrucciones que imparta la autoridad de control, en relación con el cumplimiento de la legislación estatutaria.*"

La información podrá suministrarse a las siguientes personas:

- A los titulares, sus causahabientes o sus representantes legales.
- A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
- A los terceros autorizados por el titular o por la ley.

En todo proceso de entrega de información a autoridad administrativa o de control debe suscribirse el compromiso de confidencialidad dispuesto por la DIAN mediante formato *FT-IIT-2635 Compromiso de confidencialidad y no divulgación de la información reservada o clasificada - Terceras Personas* y demás formatos o mecanismos que la entidad defina para la entrega.

12.5.3. Transferencia nacional e internacional de datos personales

La DIAN podrá realizar la transferencia de datos a otros responsables del tratamiento cuando así esté autorizado por el titular de la información o por la Ley o por un mandato administrativo o judicial conforme a lo establecido en la circular 001 de 2019 de la DIAN.

La DIAN hará transferencia nacional (dentro de Colombia) o transferencia internacional (fuera de Colombia) en el momento de enviar información personal a una persona natural o jurídica en el rol de responsable, quien decidirá autónomamente sobre las finalidades y el tratamiento de la información personal. Se entenderá como transferencia de datos personales en los siguientes casos, sin que los mismos correspondan a una lista taxativa:

El envío de información a una persona natural o jurídica, pública o privada, cuando esta última utiliza la información según sus propios parámetros.

Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la ley exige a los responsables.

No se aplicarán las prohibiciones cuando se trate de:

- Información respecto de la cual el titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del titular por razones de salud o higiene pública.
- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- Transferencias acordadas en el marco de tratados internacionales en los cuales la Republica de Colombia sea parte, con fundamento en el principio de reciprocidad.
- Transferencias necesarias para la ejecución de un contrato entre el titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del titular.
- Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

En la transferencia, la DIAN como responsable original, es decir quien recolectó o captó la información, le corresponde el deber de asegurar y garantizar que el responsable receptor cuente con medidas administrativas, técnicas y tecnológicas idóneas para asegurar la privacidad de la información, tales como políticas internas de seguridad y privacidad, un sistema de gestión de riesgos y manejo de incidentes asociados a la protección de información personal y en especial a que realice prácticas que evidencien la aplicación del principio de responsabilidad demostrada. Para tal actividad la DIAN cuenta con el formato FT-IIT-2748 *Responsabilidad Demostrada de Entidades Públicas en la protección de los Datos Personales*, el cual deberá ser diligenciado por la entidad solicitante y revisado por la DIAN.

El responsable receptor deberá contar con un esquema de protección de datos personales al interior de su organización (persona jurídica), por medio del cual cumpla los mínimos requeridos por la ley de protección de datos personales, sus decretos reglamentarios y en especial el principio de responsabilidad demostrada.

La transferencia internacional de datos personales podrá llevarse a cabo a países que cuenten con los niveles adecuados de protección de datos, según los estándares publicados por la SIC o cuando se cuente con autorización expresa de los titulares o se trate de transferencias en cumplimiento a tratados internacionales por el principio de reciprocidad, o se requieran para asegurar el cumplimiento de las funciones de la DIAN, en particular lo relativo a temas relacionados a la recaudación fiscal y la operación aduanera.

12.5.3.1. Estándares de un nivel adecuado de protección del país receptor de la información personal

El análisis para establecer si un país ofrece un nivel adecuado de protección de datos personales, a efectos de realizar una transferencia internacional de datos, estará orientado a determinar si dicho país garantiza la protección de estos, con base en los siguientes estándares:

- Existencia de normas aplicables al tratamiento de datos personales.
- Consagración normativa de principios aplicables al tratamiento de datos, entre otros: legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.
- Consagración normativa de derechos de los titulares.
- Consagración normativa de deberes de los responsables y encargados.
- Existencia de medios y vías judiciales y administrativas para garantizar la tutela efectiva de los derechos de los titulares y exigir el cumplimiento de la ley.
- Existencia de autoridad(es) pública(s) encargada(s) de la supervisión del tratamiento de datos personales, del cumplimiento de la legislación aplicable y de la protección de los derechos de los titulares, que ejerza(n) de manera efectiva sus funciones.

12.5.3.2. Países que cuentan con un nivel adecuado de protección de datos personales

La Superintendencia de Industria y Comercio en atención a los estándares de seguridad establece periódicamente una lista de países que garantizan un nivel adecuado de protección, la que en cualquier momento puede revisar, incluir o excluir a quien considere conveniente.

Sin limitarse a lo anterior y con el fin de dar cumplimiento tanto de la normatividad nacional como internacional, la DIAN realiza la transferencia de datos de manera adecuada, responsable y segura con los países con los que Colombia ha suscrito tratados internacionales dirigidos a evitar la doble imposición, tomando todas las medidas necesarias para una correcta práctica en esta materia.

12.5.4. Transmisión nacional e internacional de datos personales

La DIAN podrá enviar o transmitir datos a uno o varios encargados dentro o fuera del territorio de la República de Colombia en los siguientes casos:

- Cuando cuente con autorización del titular conforme con la Política de Tratamiento de Datos Personales de la DIAN.
- Cuando sin contar con la autorización exista entre el responsable y el encargado un contrato o acuerdo de transmisión de datos.

La DIAN realiza transmisión nacional (dentro de Colombia) en el momento de enviar información personal a una persona natural o jurídica en el rol de encargado, quien realizará el tratamiento de datos personales bajo las instrucciones de la DIAN quien será la responsable del tratamiento. Se entenderá como transmisión de datos personales en los siguientes casos, sin que los mismos correspondan a una lista taxativa:

- La contratación de servicios de tercerización (outsourcing) con entidades ubicadas dentro o fuera de Colombia, que implique el envío de bases de datos o información personal.
- La contratación de servicios en la nube, cuando el proveedor almacena información en un servidor dentro o fuera de Colombia.

Previo a suministrar información a los encargados, se deberá verificar que cumplen con los requisitos de seguridad y privacidad implementados al interior de la DIAN**,** los cuales deberán señalarse en las convocatorias de licitación y de adjudicación directa.

Los encargados deberán suscribir los documentos vinculantes por los cuales se obligan a cumplir con las políticas internas de la DIAN para el tratamiento de datos personales.

La dependencia responsable de los datos debe notificar a los encargados de cualquier actualización o supresión de la información suministrada.

Los encargados deberán informar a la DIAN de cualquier vulneración a la seguridad de los archivos y bases de datos entregadas por la DIAN.

El responsable será quien en todo momento decida respecto las bases de datos y su tratamiento.

El responsable proveerá datos personales que haya obtenido de manera lícita, ya sea a través de la autorización de los titulares o de las prerrogativas otorgadas por ley.

La información entregada deberá ser veraz, completa, exacta, actualizada, comprobable y comprensible, comunicando al encargado de la rectificación de la información suministrada, así como cualquier reclamación que afecte la información en poder del encargado.

El encargado deberá contar con un esquema de protección de datos personales al interior de su organización (persona jurídica), por medio del cual cumpla los mínimos requeridos por la ley de protección de datos personales, sus decretos reglamentarios y en especial el principio de responsabilidad demostrada.

El encargado asumirá las obligaciones de seguridad y mantenimiento de las bases de datos entregadas, para lo cual implementará manuales y políticas que garanticen el cumplimiento de la legislación para la protección de datos personales.

Aunque el responsable es quien tiene el contacto y responsabilidad con los titulares, el encargado también asume compromisos con los titulares al estar obligado a garantizar el ejercicio de sus derechos, mantener la confidencialidad, abstenerse de transferir los datos, sin la autorización de la DIAN, limitar el acceso sólo al personal autorizado y a informar a la DIAN y a la Superintendencia de Industria y Comercio de cualquier vulneración de seguridad y riesgos en la administración de los datos.

La remisión de datos personales al encargado puede llevarse a cabo mediante la inclusión de cláusulas de transmisión en el contrato que da origen a la relación entre el responsable y el encargado o a través de la celebración de un contrato de transmisión de datos personales.

La legislación no requiere que se autorice la transmisión de datos personales siempre que sea en cumplimiento de las finalidades por las cuales fueron recabados los datos y su tratamiento sea dentro del territorio nacional.

En los casos de las transmisiones internacionales de datos personales, se debe tener la autorización de los titulares, salvo que, entre el responsable y el encargado se suscriba un contrato de transmisión de datos personales o medie un tratado internacional que cumpla con los siguientes requisitos:

- Señalar los alcances del tratamiento, las actividades que el encargado realizará por cuenta del responsable y las obligaciones del encargado para con el titular y el responsable.
- Compromiso a dar aplicación a las obligaciones del responsable bajo la Política de Tratamiento de la Información fijada por este.
- Realizar el tratamiento de datos de acuerdo con la finalidad que los titulares hayan autorizado y con las leyes aplicables.
- Obligación del encargado a dar tratamiento, a nombre del responsable, a los datos personales conforme a los principios que los tutelan.
- Obligación de salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
- Guardar confidencialidad, respecto de la información personal tratada, incluso con posterioridad a la terminación de la relación legal o contractual que dio origen a la transmisión.

12.5.4.1. Gestión de encargados del tratamiento por transmisión de datos

La DIAN debe asegurar que los encargados del tratamiento cumplan con los estándares adecuados de seguridad y protección de datos personales de acuerdo con la regulación vigente en la materia. Los encargados de tratamiento son aquellos terceros a los cuales la entidad proporciona información con bases de datos personales para que actúen en nombre de la DIAN. Un ejemplo de esto es la información que se entrega a los centros de llamadas, los centros de cobro, los centros de correspondencia, las mesas de ayuda, entre otros. Es fundamental solicitar a los encargados del tratamiento que establezcan acuerdos contractuales sólidos con sus subcontratistas y terceros, asegurando que se comprometan a utilizar los datos de manera segura y solo para los fines autorizados por la DIAN, y asumiendo las responsabilidades pertinentes en caso de algún incumplimiento. La entidad encabeza de las dependencias responsables de estos convenios, contratos o cualquier forma de acuerdo de entrega de información, debe prever realizar las siguientes acciones a efectos de revisar y verificar que los encargados, están realizando adecuado tratamiento de los datos conforme con los fines que dieron origen a la entrega de la información, en los contratos y en las autorizaciones:

- Cumplimiento de los deberes consagrados en el artículo 18 de la Ley 1581 de 2012.
- Verificación de prácticas de protección de datos conforme con las normas legales, es decir verificar que la entidad u organización que asumió como encargado cuente con políticas de tratamiento de datos personales, procesos y procedimientos encaminados a estandarizar prácticas de protección de datos, medidas de seguridad apropiadas, sistema de gestión de riesgos relacionados con protección de datos, entre otras.
- Suscripción de cláusulas y compromisos de confidencialidad.
- Contratación de auditorías externas.
- Realización de auditorías internas.
- Solicitud de informes o certificaciones de eliminación de información entregada o producto del contrato
- Verificación de los estándares de seguridad por parte de funcionarios de la DIAN o de terceros contratados para el efecto.
- Aplicación de medidas contempladas para la disposición final o supresión de los datos entregados.

- Otras actividades tendientes a verificar la gestión de los encargados.

Las acciones por seguir y la periodicidad con la cual se realizan, son determinadas por la dependencia responsable de la información, teniendo en cuenta el tipo de información remitida a los encargados y el tipo de tratamiento que se haya establecido. Estas acciones y su periodicidad se deben registrar detalladamente en el instrumento jurídico que se utilice como soporte para realizar la transmisión de datos personales. Este plan contempla las actividades a llevar a cabo para garantizar la correcta recepción, procesamiento, almacenamiento y transmisión de la información, así como para asegurar la confidencialidad, integridad y disponibilidad de los datos en todo momento. Además, se establecen mecanismos de monitoreo y supervisión que permiten evaluar el cumplimiento de los objetivos y metas establecidos, así como la eficacia de los procedimientos implementados. De esta manera, se asegura una gestión adecuada de datos personales en la DIAN y se promueve la transparencia y confiabilidad en los procesos de tratamiento de datos.

12.5.5. Intercambio de información con datos personales

El intercambio de información se asemeja a la figura de transferencia de información, en lo que concierne a datos personales. Está regulado, en la mayoría de los casos por tratados internacionales y leyes que adoptan los mismos para el manejo de información fiscal.

12.5.5.1. Intercambio de información en sistemas interoperables o por mecanismos electrónicos

Respecto a la interoperabilidad de la información personal, por medio de la Circular Externa Conjunta No. 04 de 2019 expedida por la Superintendencia de Industria (SIC) y Comercio y la Agencia Nacional para la Defensa Jurídica del Estado (ANDJE), se reguló el tratamiento de datos personales en sistemas de información interoperables. Así las cosas, los principios y directrices establecidas por la Ley 1581 de 2012 respecto a la protección al derecho de habeas data, son plenamente aplicables a cualquier actividad, sin importar la novedad de las operaciones o de las tecnologías utilizadas para dicho efecto.

Así mismo, el artículo 10 del Decreto 2106 de 2019 señala que la circulación de la información que repose en sistemas de información interoperables que se encuentren integrados en el servicio ciudadano digital de interoperabilidad, deberá realizarse de conformidad con los principios y reglas de la protección de datos personales y conforme a los protocolos de clasificación, reserva y protección de datos. En ese sentido, no se requerirá para ello la suscripción de acuerdos, convenios o contratos interadministrativos.

Para los medios electrónicos que se habiliten para compartir información con datos personales con otras entidades públicas, en ejercicio de sus funciones, tales como Webservice, Sharepoint, Nube, Servidores, entre otros, una vez avalada la solicitud por la dependencia competente dueña de la información, deberán estar respaldados por la suscripción del *formato FT-IIT-2642 Compromiso de Uso del Servicio, de Confidencialidad y No Divulgación de la Información Reservada o Clasificada*.

De acuerdo con lo establecido en las políticas públicas para el uso de servicios ciudadanos digitales (carpeta ciudadana, autenticación electrónica e interoperabilidad de los sistemas del Estado), se incorpora como objetivo para la transformación digital del país, la promoción de la digitalización y automatización masiva de trámites. Para esto las entidades deberán definir proyectos estratégicos de transformación digital orientados por los principios de interoperabilidad, vinculación de las interacciones

entre el ciudadano y el estado a través del portal único del estado colombiano y el empleo de políticas de seguridad y confianza digital.

12.5.5.2. Tratamiento de datos personales, seguridad y privacidad de la información en relación con la prestación de servicios ciudadanos digitales, proyectos e iniciativas

Responsable y encargado del Tratamiento.

La DIAN como prestadora de servicios ciudadanos digitales, será responsable del tratamiento de los datos personales que los ciudadanos le suministren directamente. Así mismo será el encargado del tratamiento de los datos que otras entidades le proporcione.

En cada caso, la DIAN deberá cumplir los deberes que le corresponde como responsable o encargados establecidos en la Ley 1581 de 2012 y en la Política de Tratamiento de Datos Personales de la entidad.

Evaluación del impacto de tratamiento de datos personales

Antes de iniciar la prestación de los servicios ciudadanos digitales o la implementación de un nuevo proyecto o iniciativa, la DIAN deberá evaluar el impacto de las operaciones de dichos servicios en el tratamiento de datos personales, incluyendo como mínimo lo siguiente:

1. Una descripción detallada de las operaciones de tratamiento de datos personales que involucran la prestación de los servicios y de los fines del tratamiento.
2. Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.
3. Una evaluación de los riesgos específicos para los derechos y libertades de los titulares de los datos personales.
4. Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad, tecnologías y mecanismos que garanticen la protección de datos personales, pudiendo realizar diseño de software, teniendo en cuenta los derechos e intereses legítimos de los titulares de los datos y de otras personas eventualmente afectadas.

Para lo anterior y con el fin de mantener la integración con el Sistema de Gestión de Seguridad y Privacidad de la información, se deben aplicar los lineamientos establecidos en el numeral “3.8 Gestión de riesgos de seguridad de la información en proyectos e iniciativas” de la cartilla CT-IIT-0132 Gestión de Riesgos de Seguridad de la Información.

Los resultados de esta evaluación, junto con las medidas para mitigar los riesgos, serán tenidas en cuenta e implementadas como parte de la aplicación del fundamento de privacidad por diseño y por defecto.

Privacidad por diseño y por defecto

La DIAN, como entidad del estado deberá atender las buenas prácticas y principios desarrollados en el ámbito internacional en relación con la protección y tratamiento de datos personales, los cuales se refieren a la privacidad por diseño y a la evaluación del impacto de tratamiento de datos personales. Conforme a ello, la protección de la privacidad y de los datos además del cumplimiento de la normativa, exige un modo de operar de las organizaciones que involucra sistemas de información, modelos,

prácticas de negocio, diseño físico, infraestructura e interoperabilidad, el cual garantiza la privacidad al ciudadano y a las empresas en relación con la recolección, uso, almacenamiento, divulgación y disposición de los mensajes de datos para los servicios ciudadanos digitales, proyectos e iniciativas gestionados por la DIAN**.**

Para ello, la DIAN deberá tener en cuenta los siguientes lineamientos:

1. Incorporar prácticas y procesos de desarrollo necesarios, destinados a salvaguardar los datos personales de los individuos a lo largo del ciclo de vida de un sistema, programa o servicio.
2. Mantener las prácticas y procesos de gestión adecuados durante el ciclo de vida de los datos que son diseñados para asegurar que los sistemas de información cumplen con los requisitos, políticas y preferencias de privacidad de los titulares.
3. Usar los máximos medios posibles necesarios para garantizar la seguridad, confidencialidad e integridad de los datos personales durante el ciclo de vida de los datos, desde su recolección original, a través de su uso, almacenamiento, circulación y supresión al final del ciclo de vida.
4. Asegurar la infraestructura, sistemas de TI y prácticas de negocios que interactúan o implican el uso de cualquier información o dato personal, siendo sujeta a verificación independiente por cuenta de todas las partes interesadas.

Limitación al uso de la información

Los datos personales y los datos de los usuarios enviados a través del servicio ciudadano digital de interoperabilidad, de algún proyecto o iniciativa y en general la información generada, producida, almacenada, enviada o compartida, no podrán ser objeto de comercialización, ni de explotación económica de ningún tipo, salvo autorización expresa del titular de los datos.

12.5.6. Instrumentos jurídicos para la transmisión o transferencia o intercambio de datos personales

Cuando la DIAN deba efectuar algún tipo de acción de circulación de información a un tercero que se encargue del tratamiento o que asuma como responsable, deberá existir un contrato, acuerdo, convenio o cualquier otro instrumento jurídico correspondiente, que respalde esta transacción de información personal, el cual debe incluir de manera expresa:

- El alcance del tratamiento de los datos personales.
- Relación de las actividades que realizará el encargado que estén legitimadas por la DIAN. El uso debe corresponder a las finalidades otorgadas por el titular.
- Descripción de las obligaciones que asume el encargado frente al titular y a la DIAN.
- La responsabilidad que asumen los terceros como encargados del tratamiento frente a las medidas de seguridad y privacidad de la información y la obligación que tienen de suscribir compromisos de seguridad y confidencialidad sobre los datos entregados.
- Las obligaciones y responsabilidades asumidas por las partes, así como la adhesión a las políticas internas de la DIAN frente a seguridad de la información y tratamiento de datos personales, exceptuando las realizadas entre responsables en cumplimento de una disposición legal o en el ejercicio de sus atribuciones o labores misionales; así mismo en el ámbito internacional cuando se encuentren previstas en una ley o tratado suscrito y ratificado por Colombia, o sea solicitada por una autoridad u organismo internacional competente.

- La obligación expresa sobre la disposición final, devolución o eliminación de los datos entregados.

12.5.7. Disposición final de los datos personales obtenidos

La DIAN debe eliminar bases de datos (i) cuando sea ordenado por una autoridad, (ii) cuando en virtud de la información o tipo de datos ya no se requieran al interior de la DIAN y hayan perdido completamente su valor. La eliminación o supresión segura de la información se realizará conforme a las políticas y lineamientos emitidos en materia de Gestión Documental por la entidad.

La eliminación o supresión de información es un tema relevante para proteger la confidencialidad, integridad y disponibilidad de la información, y en particular de los datos personales, es por ello, que la DIAN deben analizar los medios más eficaces que conviene implementar para evitar que se pueda recuperar la información que ya no se requiera.

Las técnicas de eliminación o supresión segura buscan que no sea posible recuperar la información tanto física como electrónica y evitan que personas no autorizadas puedan tener acceso a esos datos. Algunos parámetros y características para este tipo de destrucción son:

- Para la información personal en bases de datos electrónicas y físicas se deberá hacer la solicitud a la dependencia correspondiente, cumpliendo con los procedimientos de gestión documental de la entidad.
- La disposición final de los datos personales debe observar los principios de finalidad y temporalidad de la información, teniendo en cuenta el fin para el cual fueron creadas y el tiempo de uso de la información.
- No se podrán destruir las autorizaciones para el tratamiento de datos personales, independientemente del formato en que se encuentre, si la información de dicho titular aún se encuentra en uso.
- Toda operación de disposición final de información de datos personales (física o electrónica) debe estar autorizada por la Subdirección Administrativa o quien haga sus veces, o por la instancia competente conforme con la política y el procedimiento de gestión documental de la entidad.
- Por seguridad se sugiere que toda operación de disposición final de información personal electrónica, de preferencia, debe tener un log de auditoría que registre la operación.
- Por seguridad se sugiere que toda operación de disposición final de datos personales en medio físico, de preferencia, debe contar con un acta, certificación o cualquier otro documento que registre la operación.
- El método utilizado debe impedir la reconstrucción y posterior uso de los datos eliminados, ser seguro y procurar ser amigable con el medio ambiente.
- Considerar los lineamientos consignados en el MN-IIT-0072 Manual de Políticas y Lineamientos de Seguridad de la Información y en el Procedimiento de Borrado Seguro.
- La información por eliminar deberá contar con medidas de seguridad que impidan su consulta o copia de personas no autorizadas. Por ejemplo, no estar almacenados en pasillos, espacios abiertos al público, etc.
- Registrar, si la base se encontraba incluida en el Registro Nacional de Bases de Datos de la SIC sobre la novedad: eliminación y dejar la evidencia de este reporte.
- En todas las operaciones internas o externas de entrega, intercambio, transferencia o transmisión de información con datos personales se debe adherir una obligación que asegure la eliminación de los datos una vez haya finalizado el objeto o la finalidad para el cual fueron entregados. *Ver anexo 5 MN0062. Cláusulas.*

12.5.7.1. Supresión

Es necesario aclarar que el término supresión en protección de datos, se da cuando el titular en ejercicio de sus derechos, solicita que sus datos sean suprimidos de la base de datos por haberse agotado su uso conforme con la finalidad con los que fueron creados o autorizados. En este orden de ideas, la supresión en términos de datos del titular será de responsabilidad de la dependencia responsable dependencia dueña de la base de datos, la cual dejará la trazabilidad del dato o datos suprimidos y se realizará conforme con el procedimiento descrito en la Política de Tratamiento de Datos Personales de la entidad y demás lineamientos que la entidad establezca para tal fin.

Los datos personales son propiedad de sus titulares, por lo que una vez agotada la finalidad que motivó su recolección, el responsable debe asegurarse que los ha eliminado de manera definitiva de sus archivos y bases de datos. La supresión es un derecho potestativo a favor del titular que no exime al responsable de eliminar de manera proactiva aquellos datos que ya no han de utilizarse.

13. PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA (ACCOUNTABILITY)

Las entidades que recogen y hacen tratamiento de datos personales deben ser responsables del cumplimiento efectivo de las medidas que implementen los principios de privacidad y protección de datos, los responsables del tratamiento deben contar con un Programa Integral de Gestión de Datos Personales y estar preparados para demostrarle a la autoridad la implementación efectiva de esas medidas en la organización.

En la DIAN se realizará la implementación del Programa Integral de Gestión de Datos Personales que será la guía de actividades, que desarrollará la entidad en períodos determinados, con el fin de implementar las medidas orientadas al cumplimiento de las normas, políticas y lineamientos sobre tratamiento y protección de datos personales.

La DIAN en cumplimiento del principio de responsabilidad demostrada y con el fin de ofrecer protección a la información que entregue a encargados y responsables, define medidas de seguridad como acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar los principios de protección, confidencialidad, disponibilidad e integridad de los datos personales.

La verificación de estas medidas debe llevarse a cabo por la dependencia que está efectuando o piensa realizar un convenio, contrato o cualquier otra figura jurídica para la entrega, intercambio o disposición de datos personales:

- **Medidas de seguridad administrativas:** contempla que la entidad u organismo a la que se le compartan los datos cuente con políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información y capacitación del personal en materia de protección de datos personales.

- **Medidas de seguridad físicas:** Incluye que la entidad u organismo a la que se le compartan los datos tenga o implemente un conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

- **Medidas de seguridad técnicas:** Involucra que la entidad u organismo a la que se le compartan los datos desarrolle un conjunto de acciones y mecanismos a través de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en el tratamiento.

14. GESTIÓN DE INCIDENTES ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES

La gestión de incidentes de seguridad asociada al tratamiento de datos personales se describe en el procedimiento para la gestión de incidentes de seguridad de la información definido por la entidad, conforme con las disposiciones de la Superintendencia de Industria y Comercio (SIC) y considerando las mejores prácticas para la gestión de incidentes.

Es fundamental que los funcionarios conozcan dicho documento para identificar quiénes son los responsables, cómo se atienden los incidentes, su clasificación y el ciclo de vida.

Existen varios supuestos o situaciones que deben tenerse en cuenta al elaborar un plan de gestión de riesgos específico para la seguridad de los datos personales en la DIAN. Estos supuestos se refieren a eventos que puedan afectar la seguridad de los datos personales, y su objetivo es prevenir y mitigar posibles incidentes, así como establecer medidas de respuesta adecuadas en caso de violaciones de seguridad. Dichas medidas incluyen la identificación del riesgo, evaluación del riesgo, tratamiento del riesgo, monitoreo y revisión, la información previamente enunciada se describe detalladamente en la Metodología de riesgos de seguridad de la información con la que cuenta la entidad, y que en caso de ser necesario deberá ser consultada en la CT-IIT-0132- Cartilla Gestión de Riesgos de Seguridad de la Información.

14.1. Incidentes de seguridad en el tratamiento de datos personales

Los incidentes de seguridad relacionados con datos personales, se atenderán conforme su naturaleza (bases de datos o activos de información físicos o digitales) por las dependencias responsables y se comunicará de su ocurrencia al Oficial de Protección de datos personales, o quien haga sus veces, para que estudie y determine las acciones que correspondan de conformidad con la normativa y disposiciones vigentes. Todo esto deberá estar alineado con el procedimiento de gestión de incidentes de seguridad de la información de la DIAN.

14.2. Otros reportes ante la Superintendencia de Industria y Comercio

Del mismo modo, surge el deber de hacer el reporte de las siguientes novedades respecto de las bases de datos personales, conforme con las fechas establecidas por la SIC (Anualmente, el 2 de enero y el 31 de marzo, a partir del año 2020:

- **Reclamos:** los responsables y/o encargados del tratamiento deberán reportar a la SIC un consolidado de los reclamos que hayan presentado los titulares de la información, conforme a los tipos de reclamos preestablecidos por la Superintendencia. Este reporte se realizará conforme a los semestres calendario de enero a junio y de julio a diciembre de cada año. El reporte de los reclamos presentados durante el semestre anterior deberá realizarse entonces: (i) Febrero -primeros 15 días hábiles- y (ii) Agosto -primeros 15 días hábiles respectivamente.

- **Eliminación de bases de datos personales:** las causales predeterminadas para eliminar la base de datos son (i) cesión de información, (ii) cumplimiento de las tablas de retención documental, (iii) depuración de información, (iv) desuso/inhabilitación de datos, (v) fusión de datos, (vi) liquidación de persona jurídica, (vii) orden judicial o administrativa, entre otras. Este reporte se llevará cabo a través del Registro Nacional de Bases de Datos -RNBD de la Superintendencia de Industria y Comercio - SIC que eliminará la consulta, pero no su registro.

15. IDENTIFICACIÓN Y TRATAMIENTO DE RIESGOS INHERENTES A LOS DATOS PERSONALES

Respecto de la gestión de riesgos en el tratamiento de los datos personales, ésta deberá realizarse de acuerdo con los lineamientos establecidos en la Metodología de riesgos de seguridad de la información de la DIAN, en la cual se consideran los riesgos asociados al tratamiento de datos personales.

Es obligación de las dependencias de la DIAN, conocer y aplicar la metodología de riesgos de seguridad de la información contenida en la CT-IIT-0132- Cartilla Gestión de Riesgos de Seguridad de la Información.

16. PROCEDIMIENTO PARA LA ATENCIÓN DE SOLICITUDES DE LOS TITULARES DE DATOS PERSONALES FRENTE A LOS DATOS OBTENIDOS POR LA DIAN

Conforme con lo dispuesto en el Título V de la Ley 1581 de 2012 y la Política de Tratamiento de Datos Personales de la entidad, a continuación, se indica el procedimiento y términos a cumplir frente a las consultas, reclamos y requisitos que deben surtirse para facilitar el ejercicio de los derechos de los titulares de datos en la DIAN.

Se debe tener en cuenta que el término “consulta” de que trata la Ley 1581 de 2012, tiene una connotación diferente a la establecida en el procedimiento “PR-CAC-0043 Peticiones, quejas, sugerencias, reclamos, felicitaciones y denuncias”. La consulta sobre el tratamiento de datos personales hace referencia a la posibilidad que tienen los titulares o sus causahabientes de tener acceso, conocer o “consultar” la información personal del titular que repose en cualquier base de datos (art 14 de la Ley 1581 de 2012).

16.1. Lineamientos Generales para la atención de Peticiones, Consultas o Reclamos de los Titulares

- Los derechos de acceso, actualización, rectificación, supresión y revocación de la autorización de datos personales podrán ser ejercidos únicamente por el titular. No obstante, el titular podrá actuar a través de representante legal o apoderado cuando aquel se encuentre en situación de incapacidad o minoría de edad, hechos que le imposibiliten el ejercicio personal de los mismos, en cuyo caso será necesario que el representante legal o apoderado acredite tal condición.
- En ningún caso la DIAN exigirá algún valor a los titulares de los datos personales o sus representantes por el ejercicio de los derechos de acceso, actualización, rectificación, supresión o revocación de la autorización.
- Como garantía adicional para que el titular de datos personales ejerza sus derechos, la DIAN cuenta con la “Defensoría del contribuyente y usuario aduanero”, órgano especial que “promueve el respeto

de los derechos, la adopción de mejores prácticas en la prestación del servicio fiscal y el fortalecimiento de una relación armónica entre la DIAN y los ciudadanos".

- Conforme con el requisito de procedibilidad establecido en el artículo 16 de la Ley 1581 de 2012, el titular o causahabiente sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento. En este orden de ideas es necesario que cada responsable de base de datos lleve un control sobre las peticiones, consultas o reclamos hechos por el titular, para saber cómo proceder si el titular agotó o no el trámite y evitar la actuación administrativa por parte de este Ente de Control y Vigilancia.
- Para la atención de reclamos o solicitudes de revocatoria de la autorización se seguirán los lineamientos y procedimientos establecidos en la Política de tratamiento de datos personales de la DIAN.
- En general el trámite interno de las solicitudes, consultas o reclamos sobre el tratamiento de datos personales debe cumplir con las mismas actividades descritas en el procedimiento "PR-CAC-0043. Peticiones, quejas, sugerencias, reclamos, felicitaciones y denuncias".

16.2. Procedimiento para peticiones, consultas o reclamos

- El titular de los datos puede formular cualquier consulta o reclamo frente a sus derechos inherentes a sus datos de carácter personal a través del Servicio de Peticiones, Quejas, Sugerencias, Reclamos y Denuncias disponible en la página web de la entidad: www.dian.gov.co/
- La dependencia encargada de atender y/o canalizar las solicitudes de los titulares referentes a la protección de datos personales es la Coordinación de Administración del Sistema de PQSRD - Peticiones, Quejas, Sugerencias, Reclamos y Denuncias o la dependencia que haga sus veces,
- Una vez recibida la consulta o reclamo, la dependencia encargada debe determinar a qué base de datos registrada ante la SIC hace referencia la consulta (el listado de bases de datos registradas ante la SIC y los responsables internos del tratamiento de esas bases, lo suministra la Oficina de Seguridad de la Información en su calidad de Oficial de Protección de Datos). Si la petición o reclamo no permite inferir o no refiere una base de datos particular, la PQSRD debe remitirse a la dependencia funcional responsable del tema objeto de la petición.
- La dependencia responsable de la base de datos o responsable funcional de atender a la petición del titular deberá observar los términos de respuesta establecidos en la Política de Tratamiento de Datos Personales en la DIAN.
- La dependencia que atendió la solicitud deberá llevar un registro sobre las PQSRD que se tramitaron relacionadas con protección de datos personales.
- Como parte del flujo para identificar y responder consultas y reclamos de habeas data, la dependencia encargada deberá reportar a la Superintendencia de Industria y Comercio (SIC) a través del Registro Nacional de Bases de Datos (RNBD), con la asistencia del Oficial de Protección de Datos de la DIAN, las PQSRD que fueron presentadas por los titulares y atendidas por la DIAN.
- La dependencia encargada de las PQSRD en la DIAN generará un reporte general sobre las PQSRD presentadas en un período determinado al Oficial de Protección de datos personales.

16.3. Atención de consultas sobre el tratamiento de datos personales

- Las consultas las puede presentar en cualquier momento y a través de los medios habilitados por la entidad (canal presencial, canal electrónico, Ventanilla Única de Correspondencia, canal telefónico).
- Para considerar una consulta válida, el titular debe presentar el documento de identidad, si esta es presencial o anexar copia si es por otro medio, expresar claramente el objeto de la solicitud y

suministrar una dirección (física o electrónica) de notificación. En caso de apoderado adicionalmente deberá presentar documento que acredite la representación.

- Las consultas se podrán presentar de manera física a través de los puntos de contactos o en las Divisiones de Gestión de Asistencia al Cliente, o en grupos internos de trabajo de Peticiones, Quejas, Sugerencias, Reclamos o en Ventanillas Únicas de Correspondencia de la DIAN o quien haga sus veces atención, a través del Servicio de Peticiones, Quejas, Sugerencias Reclamos y Denuncias, o a través de las líneas de atención al cliente dispuestas por la entidad. Tanto el Servicio como el listado de líneas de atención se encuentran en portal Web de la entidad www.dian.gov.co
- Independiente del medio en el que se presente la consulta, de acuerdo con lo establecido en el artículo 14 de la Ley 1581 de 2012, esta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recepción. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.
- La Subdirección de Servicio al Ciudadano en Asuntos Tributarios o quien haga sus veces direccionará todas las consultas que hagan los titulares de los datos personales, cuando la información repose en otras dependencias de la entidad, como máximo dentro de los dos (2) días hábiles siguientes a su recepción. De este hecho se deberá informar al interesado.

16.4. Rectificación y actualización de datos

La DIAN tiene la obligación de rectificar y actualizar a solicitud del titular o su empleador, la información de este que resulte ser incompleta o inexacta, de conformidad con los términos definidos por ley. Al respecto se tendrá en cuenta lo siguiente:

- En las solicitudes de rectificación y/o actualización de datos personales el titular debe indicar las correcciones a realizar y aportar la documentación que avale su petición.
- Se podrán habilitar mecanismos que le faciliten el ejercicio de este derecho, siempre y cuando estos beneficien al titular.
- Se podrán establecer formularios, sistemas y otros métodos simplificados que se pondrán a disposición de los interesados en las oficinas y/o en la página web.

17. INSTRUMENTOS PARA EL TRATAMIENTO DE DATOS PERSONALES

Para el cumplimiento de las obligaciones legales de la DIAN frente a la recolección, almacenamiento, uso, circulación y disposición final, se implementan los siguientes instrumentos:

17.1. Autorización del Titular

Toda labor desarrollada en la DIAN que implique tratamiento de datos personales y que no corresponda al cumplimiento de su objeto misional o al ejercicio de sus funciones legales, debe contar con la autorización otorgada por el titular, mediante mecanismos físicos, técnicos o tecnológicos, que permita obtener el consentimiento, por medio del cual se pueda concluir de manera inequívoca, que de no haberse surtido una conducta del titular, los datos nunca hubieren sido capturados y almacenados en la base de datos. Cuando la DIAN en ejercicio de actividades no misionales, recolecte datos personales, debe solicitar la autorización de los titulares a través de mecanismos físicos, técnicos o tecnológicos. La evidencia de estas autorizaciones debe ser conservada por cada una de las dependencias de la entidad, conforme lo dispuesto en la tabla de retención documental o las políticas o lineamientos que en materia de gestión documental defina la entidad.

En las excepciones dispuestas, no requiere autorización del titular cuando se trate de: *i)* información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial; *ii)* datos de naturaleza pública; *iii)* casos de urgencia médica o sanitaria; tratamiento de información autorizada por la ley para fines históricos, estadísticos o científicos; y *iv)* datos relacionados con el registro civil de las personas.

Para conocer las finalidades misionales que corresponden a la DIAN, y en específico a cada una de sus dependencias relacionadas con el tratamiento de datos personales, se debe verificar el *Anexo 7 MN0062 Matriz de finalidades para el tratamiento de datos personales.*

El responsable de la dependencia debe obtener la autorización para el tratamiento de los datos personales recolectados, por escrito, cuando el dato personal se obtenga por este medio, o de forma oral, cuando se comunique y acepte expresamente el consentimiento de las personas (en este caso se debe dejar evidencia de esta comunicación). La forma de comunicar estas acciones, dependen del medio que se esté empleando.

En caso de que una dependencia diferente de la que recolectó inicialmente el dato personal requiera utilizar los datos personales que se han obtenido, ello se podrá hacer siempre y cuando en la autorización se haya informado sobre dicho uso, se encuentre en la Política de Tratamiento de Datos Personales o sea un uso previsible dentro de las actividades legales, constitucionales o misionales.

Formas de obtener la autorización

La autorización es generada por la DIAN y puesta a disposición del titular con antelación y de manera previa al tratamiento de sus datos personales mediante cualquiera de las siguientes formas:

- Por escrito, cuando el dato personal se obtenga por este medio. Esta autorización se evidencia en formatos, formularios, anexos de documentos, entre otros.
- De forma oral, cuando se comunique y acepte expresamente el consentimiento de las personas (en este caso se deberá dejar evidencia de esta comunicación). Este tipo de autorización se dan en conversaciones telefónicas, eventos masivos, entrevistas, entre otros.
- De manera inequívoca, cuando se indique, comunique o avise de manera expresa que la ejecución de una acción por parte del titular de los datos frente a la entidad implica la aceptación de la política de tratamiento de datos personales y da su autorización para este fin. Avisos de videovigilancia, avisos informativos de ingreso a instalaciones o a eventos, entre otros.

En caso de obtenerse la **autorización de manera física,** los formatos deben: *(i)* ser lo suficientemente claros; *(ii)* archivarse, física y electrónicamente, de una manera ordenada que permita su fácil ubicación e identificación de quien autorizó, la fecha y el lugar en que se diligenció; *(iii)* la imagen debe ser de alta resolución que permita su eventual reproducción y análisis grafológico mediante imagen de alta resolución; y *(iv)* si se solicita un dato relacionado con la salud o de menores de edad, tales como estado de embarazo, enfermedades, gustos del menor, entre otros, el campo debe resaltarse e indicarse que es un dato sensible y que no es obligatorio su diligenciamiento. La firma del titular debe ser ubicada posterior a la autorización.

En caso de obtenerse la **autorización de manera electrónica,** los formatos deben: *(i)* ser lo suficientemente claros; *(ii)* tener plenamente identificado a quien autoriza, de tal manera que se permita tener la certeza de con quien se realiza la transacción; *(iii)* archivarse electrónicamente, de una manera

ordenada que permita su fácil ubicación e identificación de quien autorizó, la fecha y el lugar en que se diligenció (Dirección, página Web, dirección IP, entre otros); *(iv)* la imagen debe ser de alta resolución que permita su eventual reproducción y análisis grafológico mediante imagen de alta resolución que permita su eventual reproducción y análisis grafológico; *(v)* si se solicita un dato relacionado con la salud o con información se menores de edad, tales como, estado de embarazo, enfermedad, gustos del menor, entre otros, el campo debe resaltarse e indicarse que es un dato sensible y que no es obligatorio su diligenciamiento.

En caso de obtenerse la **autorización de manera telefónica** la llamada debe: (i) ser grabada íntegramente; (ii) tener plenamente identificado a quien autoriza; (iii) archivarse electrónicamente, de una manera ordenada que permita su fácil ubicación e identificación de quien autorizó, la fecha y el lugar en que se diligenció; y (iv) si se solicita un dato relacionado con la salud o información relacionada de un menor de edad, v.gr. estado de embarazo, enfermedad, gustos del menor, entre otros, debe indicarse que es un dato sensible y que no es obligatoria su respuesta.

Conforme a las tres (3) formas de obtener autorización, a continuación, se relacionan los formatos y modelos de autorización implementadas en la DIAN de acuerdo con el proceso o dependencia donde se requiera:

17.1.1. Autorización para el tratamiento de datos personales

El Formato *FT-IIT-2677 Autorización para el tratamiento de datos personales,* corresponde a la autorización general que se debe utilizar al iniciar un trámite y constituye un documento anexo al expediente o base de datos que se conforme con información del Titular.

Debe utilizarse en la recolección de datos de manera presencial o virtual y su evidencia debe conservarse en el expediente del titular o en la base datos que requirió la recolección.

Para el caso de los datos personales que se requieran recolectar con diferentes finalidades, es necesario describir cada una de ellas y contar con la autorización del titular cuando aplique.

17.1.2. Autorización para el tratamiento de datos personales sensibles o por representantes de niños, niñas y adolescentes

El tratamiento de este tipo de datos goza de protección especial, por lo tanto, la autorización para su recolección cuenta con condiciones particulares. El Formato *FT-IIT-2677 Autorización para el tratamiento de datos personales sensibles o por representantes de niños, niñas y adolescentes,* debe ser utilizado cuando el tratamiento sea para datos personales de niños, niñas o adolescentes o datos sensibles. A diferencia del formato anterior en la autorización para el tratamiento de datos sensibles y de niños, niñas y adolescentes será facultativa y no condicionará la relación jurídica con la DIAN. De igual manera la DIAN restringe el tratamiento de datos personales sensibles a lo estrictamente indispensable y debe solicitar consentimiento previo y expreso a los Titulares (representantes legales, apoderados, causahabientes) informando sobre la finalidad exclusiva de su tratamiento. Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles.

17.1.3. Autorización para el tratamiento de datos personales de los contratistas

El Formato *FT-IIT-2677 Autorización para el tratamiento de datos personales de los contratistas* puede utilizarse de manera impresa o electrónica y recoge la autorización respectiva que deberá incorporarse en los contratos de adquisiciones de bienes o servicios, y tiene los siguientes fines:

- Revalidación de la recolección y tratamiento de datos personales para fines contractuales;
- Aceptación/vinculación de los contratistas de la DIAN, a sus políticas sobre el tratamiento de la información.

La cláusula de protección de datos personales debe incorporarse en el contrato en todos los casos y la autorización debe incluirse y suscribirse en el momento de la recolección de los documentos que se lleva a cabo al inicio del proceso de contratación.

17.1.4. Autorización para el tratamiento de datos de los servidores públicos de la DIAN

Todo servidor público en su acto de posesión como funcionario de la DIAN, debe otorgar autorización de tratamiento de datos personales a la entidad. Esta autorización debe hacer parte de su Historia Laboral. En casos de recolección masiva de la autorización a los servidores ya vinculados estas autorizaciones podrán hacer parte del sistema de información de personal de la entidad o de bases de datos especializadas dispuestas como repositorio de estas autorizaciones.

El Formato *FT-IIT-2677 Autorización para el tratamiento de datos personales de los servidores públicos de la DIAN,* tiene los siguientes fines:

- Revalidación de la recolección y tratamiento de datos personales para fines laborales;
- Aceptación/vinculación del equipo humano de la DIAN, a su Política sobre el tratamiento de datos personales.
- La autorización de tratamiento de datos personales para servidores públicos debe incluir la difusión de datos personales para integrar el directorio que incluya el cargo, direcciones de correo electrónico, teléfono y escalas salariales, así como el nombre, ciudad de nacimiento, formación académica, experiencia laboral y profesional que señala la normativa de transparencia y acceso a la información pública. Lo último también será aplicable para la tercerización de servicios.

17.1.5. Autorización por conducta inequívoca

Toda actividad, que se realice en la DIAN o a nombre de la entidad que conlleve la captación de fotografías y videograbaciones de usuarios, servidores públicos de la DIAN, terceros, contratistas, ciudadanos e incluso menores de edad, implica el tratamiento de datos sensibles, toda vez que por medio de las fotografías como de las videograbaciones se capturan datos biométricos relacionados con las características morfológicas de las personas.

La DIAN utiliza sistemas de videovigilancia instalados en diferentes sitios internos y externos de todas las instalaciones y puntos de atención en las distintas sedes. Las tareas de monitoreo y observación realizadas a través de los sistemas de videovigilancia implican la recopilación de imágenes de personas, es decir de datos personales. se debe verificar el *Anexo 3 MN0062 Aviso de Privacidad de Videovigilancia.*

En todas las dependencias de acceso al público en la entidad donde se realice videograbaciones o tomas de fotografía se deberá fijar el modelo de Autorización conducta inequívoca, así como, disponer de Avisos o anuncios que establezcan la existencia de los sistemas de videovigilancia, del aviso de privacidad y la opción que tienen los titulares de conocer la política de tratamiento de datos personales de la DIAN.

Si la captación de datos por videovigilancia, biométricos o sensibles se realiza por medio de terceros a nombre de la DIAN (Empresas de seguridad y vigilancia, contratistas, empresas de administración de edificios, entre otros) es obligatorio que estos obtengan la autorización y entreguen las evidencias de esta al supervisor o responsable por parte de la DIAN.
El modelo previsto como "Autorización Conducta Inequívoca" ver *Anexo 1 MN0062 Autorizaciones: Guion telefónico institucional, Uso en eventos masivos y formatos físicos/electrónico,* contiene la información mínima para la autorización y por consiguiente no debe ser modificado, excepto para aclarar o ampliar la finalidad o uso.

La información recolectada se utilizará para fines de seguridad de las personas, los bienes e instalaciones, el cumplimiento de disposiciones legales y el cumplimiento de disposiciones contractuales. Esta información puede ser empleada como prueba en cualquier tipo de proceso ante cualquier tipo de autoridad y organización.

17.1.6. Autorización para llamada telefónica institucional

La Autorización Guion Telefónico Institucional, ver *Anexo 1 MN0062 Autorizaciones: Guion telefónico institucional, Uso en eventos masivos y formatos físicos/electrónico,* se debe utilizar en aquellas formas en que la DIAN realice tratamiento de datos personales a través de llamadas. A efectos de acreditar la autorización y cumplir con los deberes establecidos en la normativa de tratamiento de datos personales, es necesario que:

- La llamada sea grabada íntegramente, desde que se lee la autorización hasta que se lleva a cabo la captura de los datos;
- Si la llamada se realiza en tiempo real debe solicitarse la autorización.
- Se realice algún tipo de validación para que se tenga plenamente identificada a la persona que otorga la autorización;
- La autorización sea archivada electrónicamente de una manera ordenada que permita su fácil ubicación, la identificación de quien autorizó, la fecha y el número telefónico al cual accedió el titular o desde el cual se llamó al titular;
- En caso de que se solicite un dato relacionado con la salud o con un menor de edad (embarazo, enfermedad, gustos de un menor de edad, entre otros) debe indicarse que es un dato sensible y que no está obligado a autorizar su tratamiento.

Este modelo contiene la información mínima para la autorización y por consiguiente no debe ser modificado, excepto para aclarar, ampliar la finalidad o uso o para indicar que si se trata de un dato sensible no es obligatoria su respuesta.

17.1.7. Autorización para el uso de derechos de imagen y protección de datos personales

Esta autorización generalmente puede darse en actividades relacionadas con las comunicaciones internas y externas, manejo de medios, redes sociales, eventos, entrevistas, entre otros. Se debe solicitar la autorización de los derechos de imagen sobre fotografías o procedimientos análogos y/o

digitales a la fotografía, o producciones audiovisuales (videos), así como los derechos patrimoniales de autor (reproducción, comunicación pública, transformación y distribución) y derechos conexos y, en general, todos aquellos de Propiedad Intelectual que tengan que ver con el derecho de imagen.

Para obtener esta autorización debe diligenciarse el formato *FT-PEC-2636 Autorización uso de derechos de imagen y de tratamiento de datos personales*.

Por tratarse de los datos personales del Titular se debe incluir en la autorización de uso de derechos de imagen, los derechos que le confiere la ley 1581 de 2012 (Ley de protección de datos) y la Política de Tratamiento de Datos Personales establecida por la DIAN.

Derivado de la operación de la DIAN, esta puede recolectar imágenes de niños, niñas y adolescentes a través de sus sistemas de videovigilancia y eventos institucionales, por lo que deberá contar con las autorizaciones de los representantes legales para el tratamiento de los datos de los niños, niñas y adolescentes. No obstante, en caso de que un representante legal no autorice dejar registro de las grabaciones, se deberá seguir un procedimiento específico. En primer lugar, se debe respetar la decisión del representante legal, sin embargo, es importante que la DIAN informe al representante legal sobre las implicaciones que esto puede tener para la seguridad y protección de los niños, niñas y adolescentes, así como para el cumplimiento de sus funciones institucionales. Se deberá comentar con el representante legal sobre las finalidades por las cuales se recaban las imágenes, la mayoría de las veces es por seguridad de los asistentes o participantes, así como de los mismos niños. En ningún momento la DIAN difundirá o compartirá la información de los niños, niñas y adolescentes con terceros para un tratamiento distinto a las finalidades para las cuales se recaba dicha información. En caso de que el representante legal no dé la autorización del tratamiento de los datos, la DIAN deberá establecer mecanismos para difuminar u ocultar los rostros de los niños, niñas y adolescentes en los sistemas de videovigilancia, a fin de hacer irreconocible a los mismos. En cualquier caso, es fundamental mantener una comunicación clara y transparente con los representantes legales y buscar soluciones que concilien la protección de los derechos de los niños, niñas y adolescentes con las necesidades operativas de la DIAN.

La Oficina de Comunicaciones Institucionales, sus corresponsales y demás dependencias que requieran recolectar este tipo de datos, deberán contar con un inventario del material de difusión que contiene imágenes, especialmente la de niños, niñas y adolescentes, eliminando aquel respecto del cual no cuente con la autorización del Titular o representante legal. En todo caso antes de cualquier difusión de imágenes, fotografías, videos, entre otros, que contengan datos personales, deben asegurarse de que cuenten con la Autorización del Titular.

17.1.8. Autorización para tratamiento de datos biométricos

En las dependencias de la entidad en las que se disponga de sistemas de captura de datos biométricos (tales como registros de huellas dactilares, control óptico, entre otros), se deberá informar al Titular sobre el procedimiento a realizar, la finalidad de este, dar a conocer el aviso de privacidad y obtener el consentimiento de este para su captura, mediante el formato *FT-IIT-2677 Autorización para tratamiento de datos biométricos.*

Cuando la captura de estos datos se realice a través de un tercero (contratista), este debe adoptar y cumplir las medidas descritas en el presente documento. En todo caso se deberá conservar evidencia de la obligación de informar a los Titulares y del consentimiento dado.

La DIAN utilizará los mecanismos con que cuenta actualmente; e implementará y adoptará las acciones tendientes y necesarias para mantener registros o mecanismos técnicos o tecnológicos idóneos de cuándo y cómo obtuvo autorización por parte de los Titulares de datos personales para el tratamiento de este tipo de datos. Para dar cumplimiento a lo anterior, se podrán establecer archivos físicos o repositorios electrónicos realizados de manera directa o a través de terceros contratados para tal fin.

17.1.9. Autorización para el tratamiento de datos personales - Eventos Masivos

En la realización de eventos que demandan la asistencia masiva de personas (funcionarios, familiares, contratistas, usuarios, partes interesadas) tales como capacitaciones, actividades sociales, deportivas, recreativas, culturales, de promoción de servicios, las relacionadas con eventos de cultura de la contribución, ruedas de prensa, entre otros, donde se disponga de cámaras o demás elementos que registren a las personas en videos o por medio de fotografías, se debe dar lectura al modelo de autorización, antes de dar inicio al evento con el fin de proceder a obtener la autorización para el tratamiento de datos personales de la siguiente forma:

- En los sitios de acceso al evento debe fijarse en carteles, pancartas, presentaciones etc. de manera tal que los asistentes dispongan de esta información y decidan su autorización permaneciendo en el recinto (presencial o virtual).
- Se debe dejar evidencia de la publicación de este aviso.
- Antes de iniciar el evento con la lectura del texto propuesto en el *Anexo 1 MN0062 Autorizaciones: Guion telefónico institucional, Uso en eventos masivos y formatos físicos/electrónico*
- Se recomienda que la invitación o inscripción al evento contenga la autorización para el tratamiento de datos personales y dejar evidencia de esta.
- Si el evento se realiza por medio de terceros a nombre de la DIAN (Cajas de Compensación, universidades, colegios, contratistas, etc.) es obligatorio que estos obtengan la autorización y entreguen las evidencias de esta al supervisor o coordinador de la actividad por parte de la DIAN.

Si en el evento se utiliza listas de asistencia se debe incluir el texto de autorización propuesto en el *Anexo 1 MN0062 Autorizaciones: Guion telefónico institucional, Uso en eventos masivos y formatos físicos/electrónico,* en la opción “Autorización para el tratamiento de datos personales – realización de eventos masivos”.

17.1.10. Autorización para el tratamiento de datos personales

Este texto debe usarse en los formatos que tiene la entidad por medio de los cuales recolecta datos personales en razón a los procedimientos relacionados con temas no misionales que desarrollan las dependencias. Esta autorización debe fijarse antes de la firma o del medio de aceptación del Titular. Ver *Anexo 1 MN0062 Autorizaciones: Guion telefónico institucional, Uso en eventos masivos y formatos físicos/electrónico,* en la opción “Autorización para el tratamiento de datos personales - Uso en formatos físicos o electrónicos”.

En virtud del principio de privacidad por diseño, todo formato, formulario o forma que se establezca en el sistema de gestión de la entidad que recolecte datos personales, especialmente en los procesos no misionales, debe contemplar el modelo de autorización previsto en este anexo. Las finalidades están definidas en el *Anexo 7 MN0062 Matriz de finalidades para el tratamiento de datos personales.*

17.1.11. Evidencia de la Autorización

Las dependencias responsables de solicitar autorizaciones deben implementar y adoptar las acciones tendientes y necesarias para mantener registros de la evidencia física o electrónica mediante el uso mecanismos técnicos o tecnológicos idóneos de cuándo y cómo obtuvo la autorización por parte de los Titulares de datos personales para el tratamiento de estos. Para dar cumplimiento a lo anterior, se podrán establecer archivos físicos o repositorios electrónicos realizados de manera directa o a través de terceros contratados para tal fin.

17.2. Aviso de privacidad

Siempre que se trate de la recolección o recopilación de datos personales, el responsable de la dependencia debe garantizar que el titular de los datos conozca los derechos, la finalidad y las medidas que adopta la entidad para preservar la seguridad y confidencialidad de la información suministrada. El aviso de privacidad (*Ver anexo 2 MN0062 Aviso de privacidad*) debe fijarse siempre que se recolecten datos personales independientemente que requiera o no solicitar autorización para la recolección.

El responsable de cada dependencia debe incorporar e informar de manera clara y expresa, en el aviso de privacidad, elementos mínimos con destino a los titulares tales como:

- Nombre o razón social y datos de contacto del responsable del tratamiento
- El tratamiento al cual serán sometidos los datos y las finalidades bajo las cuales serán tratados en la DIAN.
- Los derechos que le asisten al Titular de acuerdo con la Ley 1581 de 2012 y la política de tratamiento de datos personales adoptada por la DIAN.
- Los mecanismos dispuestos por el responsable para que el Titular conozca la política de tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el aviso de privacidad correspondiente. En todos los casos, debe informar al Titular cómo acceder o consultar la política de tratamiento de información".
- Cuando se recolecten datos personales sensibles, el aviso de privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos.

En virtud del principio de privacidad por diseño, todo formato, formulario o forma que se establezca en todos los procesos del sistema de gestión de la Entidad, que recolecten datos personales físicos o electrónicos, deben contemplar el modelo de aviso de privacidad previsto en este anexo. Debe estar anexo a todas las formas de recolección de datos, cuando la captura se realice de manera impresa, o de manera virtual cuando el Titular ingrese a los medios digitales disponibles en la Entidad (página web, sistemas electrónicos, chats, redes sociales, entre otros).

17.2.1. Principio de privacidad por diseño

La OSI en su calidad de Oficial de Protección de Datos Personales y en cumplimiento de las obligaciones establecidas en la Resolución 101 de 2020, especialmente la relacionada con la de definir lineamientos que promuevan la protección de datos personales en la Entidad, emite las siguientes disposiciones relacionadas con el principio de privacidad por diseño:

1. La DGIT como única dependencia encargada de la compra o desarrollo de aplicaciones en la DIAN deberá tener presente, desde la planeación y el diseño de aplicaciones, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado para la protección de datos personales.

2. Todas las dependencias de la DIAN para el diseño, implementación y/o generación de nuevos servicios de la entidad, canales de atención, nuevos procesos, adecuación, renovación o disposición de espacios físicos, nuevas formas físicas o digitales de interoperabilidad o circulación de la información tanto interna o externamente, deben tener presente de carácter obligatorio todos los lineamientos de protección de datos personales para el adecuado Tratamiento.

17.2.2. Medios o formas de difusión e implementación

Para la difusión e implementación del aviso de privacidad, el Responsable del tratamiento podrá hacer uso de documentos, formatos electrónicos, medios verbales o cualquier otra tecnología, que asegure el cumplimiento del deber de informar al Titular, como por el ejemplo:

17.2.3. Prueba de aviso de privacidad

Las dependencias de la DIAN que deban implementar los avisos de privacidad en la recolección de datos personales deben conservar soportes del uso y fijación de los avisos de privacidad; para el caso de los avisos físicos se deben conservar fotos de los lugares donde se ubiquen; para el caso de medios

electrónicos, sonoros y ópticos o audiovisuales, manejar protocolos de implementación y obtener prueba física y tecnológica del uso del aviso de privacidad.

El aviso de privacidad debe ponerse a disposición de los titulares a través de medios escritos, electrónicos, verbales o de cualquier otra tecnología siempre y cuando cumpla con el deber de informar al titular cuando exista la recopilación de datos personales.

El aviso de privacidad debe fijarse en los sitios de acceso a edificios e instalaciones que recopilen datos biométricos, fotográficos o por videograbaciones, en lugares visibles y de fácil acceso, así como en todos los puntos de atención de la entidad. La DIAN debe facilitar el medio para que el Titular tenga acceso a la Política de tratamiento de sus datos personales.

El aviso de privacidad debe ubicarse en un lugar visible como las recepciones, las entradas, los parqueaderos, y todos aquellos accesos peatonales o vehiculares en los cuales se recolecte información de los titulares, así como los canales digitales o virtuales como por ejemplo el sitio web de la entidad.

En los casos en que la política de Tratamiento de datos personales de la DIAN no pueda ser informada, el responsable de los datos personales debe comunicarla por medio de avisos de privacidad, los cuales contendrán los aspectos más relevantes de la Política.

17.2.4. Disclaimer sobre el Tratamiento de Datos Personales para Utilizar en las Comunicaciones Vía Correo Electrónico

Con este aviso se busca en primer lugar informarles a los receptores de correos electrónicos sobre el compromiso de la Entidad frente a la Protección de sus Datos Personales y en segundo lugar comunicarle sobre la oportunidad de manifestar su voluntad de no recibir comunicaciones futuras, cuando no medien finalidades misionales, legales o contractuales con la entidad. En ese sentido, se debe cumplir dicha solicitud y no volver a remitirle información a la persona, ya que esta podrá instaurar una queja contra la DIAN.

El modelo previsto en el *Anexo 4 MN0062 Disclaimer sobre el tratamiento de datos personales* "Disclaimer sobre el Tratamiento de Datos Personales para utilizar en las comunicaciones vía correo electrónico", contiene la información mínima que debe conocer el titular y por consiguiente no debe ser modificado, excepto para aclarar o ampliar la finalidad o uso.

17.2.5. Disclaimer sobre el Tratamiento de Datos Personales para Utilizar en formularios y formatos.

Este aviso debe ser fijado en todos los formatos y formularios, físicos o electrónicos, que realicen recolección de datos personales. Las dependencias deben identificar dentro de sus procedimientos, aquellas actividades, formularios y formatos que demandan la recolección de datos personales, independiente de si requieren o no la autorización, e incluir el texto de aviso para que el Titular sea informado de la Política de Tratamiento de los Datos Personales por parte de la DIAN y la forma en que puede ejercer sus derechos.

El modelo previsto en el *Anexo 4 MN0062 Disclaimer sobre el tratamiento de datos personales*

como “Disclaimer sobre el tratamiento de datos personales para utilizar en formularios y formatos”, contiene la información mínima que debe conocer el titular y por consiguiente no debe ser modificado, excepto para aclarar o ampliar la finalidad o uso.

17.3. Compromisos de confidencialidad y de no divulgación de la información reservada o clasificada

17.3.1. Compromiso de confidencialidad

La entidad establece como control de seguridad y privacidad de la información, de obligatorio cumplimiento, la suscripción del formato *FT-IIT-2635 Compromiso de confidencialidad y no divulgación de la información reservada o clasificada*, con el fin de que quien lo firma se obliga a respetar el secreto y la confidencialidad de la información que se le va a compartir y a usarla sólo para el fin o fines que se estipule (n) en el compromiso. El formato cuenta con un compromiso diferente para funcionarios, contratistas y terceras personas. A continuación, se explica la finalidad para cada uno:

Tipos de Compromiso	Definición
Compromiso de confidencialidad y no divulgación de la información reservada o clasificada para funcionarios	El compromiso de confidencialidad de la DIAN suscrito por los servidores públicos de la Entidad es un documento en el cual el funcionario que lo firma se obliga a respetar el secreto y la confidencialidad de la información que gestiona y a usarla sólo para el fin que se estipule en el compromiso. Debe suscribirse en el momento de la vinculación del funcionario a la Entidad y una vez diligenciado debe ser adjuntado a la Historia Laboral del funcionario.
Compromiso de confidencialidad y no divulgación de la información reservada o clasificada para los contratistas	El compromiso de confidencialidad de la DIAN con los contratistas es un documento mediante el cual la parte que lo firma se obliga a respetar el secreto y la confidencialidad de la información que se le va a compartir en razón a sus obligaciones contractuales y a usarla sólo para el fin o fines que se estipulen en el compromiso. Se recomienda la suscripción de este compromiso durante la firma del acta de inicio. Este documento debe hacer parte del informe de supervisión del contrato y posteriormente de la serie documental Contratos.
Compromiso de confidencialidad y no divulgación de la información reservada o clasificada para terceras personas	El compromiso de confidencialidad de la DIAN con terceras personas es un documento mediante el cual la parte que lo firma se obliga a respetar el secreto y la confidencialidad de la información que se va a compartir y a usarla sólo para el fin o fines que se estipule (n) en el compromiso. Como su nombre lo indica lo suscriben personas que reciben información clasificada o reservada por algún tema o proyecto de interés de la DIAN y que al momento de suscribirla aún no tienen un vínculo laboral, legal o contractual con la Entidad. Ejemplo: aspirantes en procesos de selección, investigaciones, presentación de proyectos o propuestas económicas, intercambio de información entre otros. Este documento debe ser conservado en la serie documental relacionada con la acción o función que obligó a la suscripción.

Tabla 5. Compromisos de confidencialidad

17.3.2. Compromiso de Uso del Servicio, Confidencialidad y no Divulgación de la Información Reservada o Clasificada

La entidad establece como instrumento de control de seguridad y privacidad de la información, de obligatorio cumplimiento, la suscripción del formato *FT-IIT-2642 Compromiso de uso del servicio, confidencialidad y no divulgación de la información reservada o clasificada*, cuyo fin es facilitar la interoperabilidad de la información entre entidades y organismos que en razón a sus funciones requieran que la DIAN les facilite información mediante el uso de plataformas tecnológicas tales como web services, nube, servidores entre otros. No debe suscribirse cuando existe un documento jurídico equivalente que remplace las obligaciones de este compromiso. Cada vez que se requiera un servicio de web services, la Dirección de Gestión de Innovación y Tecnología o quien haga sus veces, verificará el tipo de información (pública, pública clasificada o pública reservada) que será objeto de consumo por el Tercero, con el fin de implementar y recomendar los mecanismos o medidas de seguridad y privacidad de la información que protejan los datos.

17.4. Cláusulas contractuales para la protección de datos personales

El objetivo de las cláusulas contractuales de seguridad y privacidad de la información, es la protección de la confidencialidad, integridad y disponibilidad de los datos, sin embargo, es necesario hacer mención que la(s) cláusula(s) puede(n) estar contenida(s) dentro un contrato cuyo desarrollo del objeto principal no es en esencia la transmisión o transferencia de información sino que demanda de circulación de información confidencial o con datos personales privados, semiprivados o sensibles para el logro de su objeto contractual, razón por la cual, una o varias cláusulas pueden definir condiciones para que la seguridad, confidencialidad y privacidad se cumplan durante el desarrollo del contrato sin afectar o exponer la información.

Las cláusulas establecidas dentro de los contratos para la protección de datos personales se someten al tiempo de duración del objeto del contrato principal.

Las cláusulas que deben hacen parte en un contrato, convenio, acuerdo o demás negocio jurídico que incluya la circulación, deben ser las de confidencialidad.

17.4.1. Cláusula de Confidencialidad

De toda relación contractual que suscriba la DIAN, esta cumplirá el papel de Responsable del tratamiento, y en virtud de tal calidad se debe dar cumplimiento a los deberes que le asisten, contenidos en la Ley 1581 de 2012, en especial, para el presente caso, las dirigidas a dar cumplimiento a las medidas de seguridad de la información, el acceso y circulación restringida y confidencialidad de la información y datos personales, contenidos como principios rectores en el tratamiento de datos personales en el artículo 4 de la Ley 1581 de 2012.

Para este caso, como regla general, se requiere que la DIAN:

- En toda relación contractual se incluya la cláusula de confidencialidad como medida de seguridad, independiente del objeto contractual que motive el contrato.
- Se suscriba con cada persona natural, y en caso de ser persona jurídica sea suscrita por el representante legal, quien se debe comprometer a extender su contenido a las personas naturales que destine para el cumplimiento del objeto contractual.

- Se suministre, en todo caso, únicamente la información necesaria para dar cumplimiento al objeto contractual y sus deberes, restringiendo el acceso a la demás información de la entidad.
- Si el objeto contractual se basa en el suministro o tráfico masivo de información se sugiere sea suscrito un contrato o acuerdo adicional, con la descripción de la responsabilidad mucho más detallada, sumado a la cláusula o contrato de transmisión o transferencia, según corresponda.

17.4.2. Cláusula de Protección de Datos

Los contratos que por el desarrollo de su objeto o sus obligaciones requieran realizar tratamiento de datos personales, deben contener la cláusula descrita en el *Anexo 5 MN0062 Cláusulas de protección, transferencia, transmisión y disposición final de datos personales* como "cláusula de protección de datos personales", que como su nombre lo indica, conlleva a que el que suscriba el contrato o instrumento jurídico que se asimile conozca las responsabilidades y obligaciones respecto de la información personal que tratará.

17.4.3. Cláusula de Transferencia de datos personales

Es la disposición establecida en un contrato cuyo objeto radica en el envío de bases de datos con datos personales a terceros en modalidad de Transferencia y el establecimiento de la obligación de tratar la información con medidas de seguridad y confidencialidad.

La cláusula de transferencia debe usarse en aquellos contratos, convenios o cualquier instrumento jurídico, mediante el cual el desarrollo de su objeto principal implique transferir datos personales a nivel nacional o internacional de datos. Es común que deba ir en convenios interadministrativos, convenios interinstitucionales, convenios de interoperabilidad, convenios internacionales de carácter misional que promuevan la facilitación de asuntos tributarios o aduaneros y que requieran del intercambio o de la transferencia de la información personal. Mediante esta cláusula la DIAN transfiere la responsabilidad del tratamiento a un nuevo responsable quien es el que suscribe el contrato y recibe los datos. (Ver *Anexo 5 MN0062 Cláusulas de protección, transferencia, transmisión y disposición final de datos personales "*cláusula de transferencia de datos personales"*)*.

Para este caso, la DIAN debe:

- Tener autorización o esté legitimada para el Tratamiento del dato.
- Autorización por el titular para enviar el dato a terceros, en los casos señalados por la Ley.
- Transferir datos recolectados antes del 27 de junio de 2013 sobre los cuales aplicó el proceso indicado en el artículo 10 del Decreto 1377 de 2013 que fue incorporado en el Decreto 1074 de 2015, siempre y cuando en su Política de Tratamiento de Datos Personales se contemple la facultad de enviar datos a terceros ubicados dentro o fuera del territorio de la República de Colombia.

17.4.4. Cláusula de transmisión de datos personales

Es la disposición establecida en un contrato cuyo objeto radica en el envío de bases de datos con datos personales a terceros en modalidad de transmisión y el establecimiento de la obligación de tratar la información con medidas de seguridad y confidencialidad. *(Ver Anexo 5 MN0062 Cláusulas de protección, transferencia, transmisión y disposición final de datos personales* en "cláusula de transmisión de datos personales").

La cláusula de transmisión debe incluirse en aquellos contratos, convenios o cualquier instrumento jurídico, mediante el cual el desarrollo de su objeto principal implique la transmisión nacional o internacional de datos. Es común que deba ir en contratos, convenios interadministrativos, convenios interinstitucionales, que requieran la entrega de la información personal por parte de la DIAN para poder llevar a cabo la actividad contractual pactada. Estas cláusulas generalmente son usadas en contratos de tercerización tales como centros de llamada, centros de cobro, mesas de servicio, servicios en la nube, entre otros.

Para este caso, la DIAN debe:

- Tener autorización o esté legitimada para el tratamiento del dato.
- Transmitir datos recolectados antes del 27 de junio de 2013, sobre los cuales aplicó el proceso indicado en el artículo 10 del Decreto 1377 de 2013 que fue incorporado en el Decreto 1074 de 2015, siempre y cuando en su Política de tratamiento de Información se contemple la facultad de tratar los datos para los fines en los que la DIAN desee o necesite realizar la transmisión a un encargado ubicado dentro o fuera del territorio Nacional.

17.4.5. Cláusula de Disposición Final de los datos personales

Esta cláusula debe ser incluida en todos los instrumentos jurídicos que por el desarrollo de su objeto contractual o sus obligaciones demanden la entrega de datos personales por parte de la DIAN. El objetivo de esta cláusula es dejar claro lo que sucederá con las bases de datos entregadas después que cese el término de duración contractual y la finalización del objeto por las cuales fueron entregadas. La cláusula debe indicar la disposición final de los datos y si fueron eliminadas las bases, dejar constancia de la forma en que se llevó a cabo esta disposición final. *(Ver anexo 5 MN0062 Cláusulas de protección, transferencia, transmisión y disposición final de datos personales* en “cláusula de disposición final de los datos personales”).

17.5. Contratos, convenios o acuerdos de transmisión y/o transferencia de datos personales

Son instrumentos jurídicos cuyo objeto radica en el envío de bases de datos que contienen datos personales. A través de estos documentos, el responsable el cual almacena y trata bases de datos con datos personales acuerda las condiciones macro, establece las responsabilidades y obligaciones respecto de un tercero, que ejercerá el rol de encargado (en contratos de transmisión) o como responsable (en contratos de transferencia); acerca del tratamiento de las bases de datos objeto del envío, define medidas de seguridad y confidencialidad de la información enviada.

La DIAN en ejercicio de sus funciones o para facilitar operaciones de circulación de información tanto nacional como internacional, puede suscribir acuerdos, convenios, contratos o cualquier otro tipo de instrumento jurídico que deje claras las finalidades, alcance, obligaciones y responsabilidades con las que se llevará a cambio la transferencia o intercambio de esa información personal. Los modelos de las condiciones y cláusulas que deben contener estos instrumentos jurídicos están contenidos en el *Anexo 6 MN0062 Modelos de contratos para transmisión y transferencia de datos personales.*

18. REGISTRO NACIONAL DE BASES DE DATOS

El artículo 19 de la Ley 1581 de 2012 indica que la Superintendencia de Industria y Comercio, a través de la Delegatura para la Protección de datos personales, ejercerá la vigilancia para garantizar que en el tratamiento de datos personales se respeten todos los principios, garantías y procedimientos previstos en la ley en mención.

En cumplimiento de dicha obligación, se cuenta con el Registro Nacional de Bases de Datos -RNBD, en virtud del artículo 25 de la ley en mención se define como "un directorio público de las bases de datos personales sujetas a tratamiento, que operan en el país […] y de libre consulta para los ciudadanos", regulado mediante Decreto 886 de 2014 que fue incorporado en el Decreto 1074 de 2015.

En el Capítulo 26 del Decreto Único Reglamentario 1074 de 2015 del Sector Industria y Comercio y el Decreto 886 de 2014 que fue incorporado en el Decreto 1074 de 2015, contienen disposiciones generales en las que se reglamentan los términos y condiciones bajo los cuales se deben inscribir en el Registro Nacional de Bases de Datos, los responsables y encargados de tratamiento de las Bases y de Datos y la información correspondiente.

18.1. Deber de inscripción de las bases de datos en el registro nacional de bases de datos – RNBD

De conformidad con el Artículo 2.2.2.26.2, del Capítulo 26 del Decreto 1074 de 2015, serán objeto de inscripción en el Registro Nacional de Bases de Datos – RNBD, las bases de datos que contengan datos personales cuyo tratamiento automatizado o manual se realice por personas naturales o jurídicas de naturaleza privada, en el territorio colombiano o fuera de él.

De conformidad con lo anterior, el deber de inscripción de las Bases de Datos, so pena de las multas y sanciones a que haya lugar por el incumplimiento, radica también en cabeza de las Entidades Públicas.

Adicionalmente, el parágrafo del artículo 23 de la Ley 1581 de 2012, prescribe que:
"[…] En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva".

18.2. Bases de datos objeto de inscripción en el registro nacional de bases de datos

El Artículo 2.2.2.26.2, del Capítulo 26 del Decreto 1074 de 2015 indica de forma general que, deberán registrarse todas las Bases de Datos que contengan datos personales. Ahora bien, en virtud del marco normativo vigente, las obligaciones legales, contractuales y el objetivo misional de la entidad, se han identificado cuatro (4) grupos de Bases de Datos que unifican y consolidan conceptualmente las bases de datos, así:

Usuarios	Funcionarios/Servidores Públicos	Proveedores/Contratistas:	Grupos de interés y Partes Interesadas:
• Bases de Datos que contengan información relacionada con personas naturales que desarrollan la actividad misional institucional de la Entidad Pública. Para el caso de la DIAN en esta clasificación estarían los contribuyentes y usuarios aduaneros y cambiarios.	• Bases de Datos que contengan información relacionada con los servidores públicos adscritos a la planta de personal interna de la Entidad Pública.	• Bases de Datos que contengan información relacionada con terceros que se vinculan a la Entidad en virtud de una relación contractual derivada del apoyo a la actividad misional/institucional de la Entidad Pública.	• Bases de Datos que contengan información de personas que representen algún tipo de utilidad para la organización pero que no se adecúa a la descripción de las tipologías anteriores.

Ilustración 4. Grupos de bases de datos

18.3. Identificación, levantamiento y registro de bases de datos que contengan datos personales.

Teniendo en cuenta el tipo de Titulares de datos en la DIAN y para efectos de Tratamiento de la información, la DIAN clasifica sus Bases de Datos con datos personales en las siguientes categorías:

(i) Bases de Datos de procesos misionales.
(ii) Bases de Datos de procesos no misionales.

Las bases de datos con información de personas naturales deben conformarse teniendo en cuenta los principios de *finalidad, utilidad, pertinencia y temporalidad*, estas hacen parte de los activos de información de la dependencia o proceso y en tal sentido es de exclusiva responsabilidad de la dependencia, en cabeza de su Director, Defensor, Jefe de Oficina o Subdirector, atender las obligaciones establecidas para la identificación, inventario, clasificación y actualización de activos de información conforme con el procedimiento “PR-IIT-0366 Gestión de Activos de Información”, la normativa y guías establecidas.

18.4. Sistema de información para el control de bases de datos personales

La entidad cuenta dentro de su sistema de información de Gestión, Riesgo y Cumplimiento -*GRC*- con un aplicativo para realizar la creación, modificación, actualización, supresión o control a los activos de información de la entidad y los de categoría; “Bases de datos personales”, administradas y registradas ante la SIC. Cada dependencia cuenta, como mínimo, con un usuario asignado quien estará a cargo de la gestión de cada una de sus bases de datos, conforme con los lineamientos del Oficial de Protección de Datos, o quien haga sus veces.

La administración de usuarios para la gestión de las bases de datos personales en el Registro Nacional de Bases de Datos (RNBD) de la SIC, estará a cargo de la Oficina de Seguridad de la Información-OSI. Esta opción permite administrar los usuarios de quienes acceden al sistema, para asociarles perfiles, dependiendo del tipo de información que deban registrar; así mismo, permite la creación y eliminación de usuarios y el cambio de contraseña. Adicionalmente la DIAN cuenta con un aplicativo de Gestión, Riesgo y Cumplimiento-GRC, en donde el módulo de inventarios de activos de información incluye la identificación de bases de datos personales, como activo de información de la DIAN.

A su vez, la Oficina de Seguridad de la Información-OSI, es el interlocutor oficial ante la Superintendencia de Industria y Comercio para lo concerniente con la gestión de la información del Registro Nacional de Bases de Datos-RNBD, de acuerdo con la normatividad vigente.

De otra parte, la Oficina de Seguridad de la Información-OSI cuenta con un equipo de trabajo para efectuar el acompañamiento y brindar la capacitación requerida por parte de las dependencias para facilitar este ejercicio.

Adicional al sistema de información de la Entidad, en la plataforma de la Superintendencia de Industria y Comercio–SIC-Registro Nacional de Bases de Datos (RNBD), los funcionarios responsables de las bases de datos deben realizar las actualizaciones pertinentes conforme con la dinámica que tienen las bases de datos registradas y los plazos definidos por la SIC de acuerdo con el tipo de novedad.

18.5. Actualización de las bases de datos registradas en el RNBD

La Superintendencia de Industria y Comercio, mediante la Circular Externa 001 de 2016 y la Circular Externa 003 de 2018 estableció por norma, la obligación de actualizar las bases de Datos Personales, Por lo tanto, los Responsables del Tratamiento deben actualizar la información inscrita en el Registro Nacional de Bases de Datos (RNBD) en los siguientes casos y fechas:

- En los primeros 10 días hábiles de cada mes, cuando existan cambios sustanciales entendidos estos como: Los que se relacionen con la finalidad de la Base de Datos; el Encargado del Tratamiento; los canales de atención al Titular; la clasificación o tipos de Datos Personales almacenados en cada Base de Datos; las medidas de seguridad de la información implementadas; la Política de Tratamiento de la Información y la Transferencia y Transmisión Internacional de Datos Personales. Circular Única de la Superintendencia de Industria y Comercio.
- Anualmente, entre el 2 de enero y el 31 de marzo, a partir de 2020.
- En todo caso, dentro de los quince (15) primeros días hábiles de los meses de febrero y agosto de cada año, se deberá actualizar la información correspondiente a los reclamos presentados por Titulares de Datos Personales en las Bases de Datos inscritas, del semestre inmediatamente anterior.

18.6. Identificación de nuevas bases de datos por cambios organizacionales, tecnológicos, estructurales o por nuevas funciones asignadas, entre otros

En razón a la dinámica o los cambios organizacionales, es necesario que las dependencias de la DIAN revisen permanentemente los tipos de activos de información que gestionan y si estos corresponden a la categoría de datos personales, deben realizar la evaluación para determinar si se trata de una nueva base de datos personal (física o digital), de ser así y conforme con la normatividad vigente, las bases de datos que se creen con posterioridad a las ya registradas, deberán inscribirse dentro de los dos (2) meses siguientes, contados a partir de su creación.

La identificación de nuevas bases de datos debe obedecer al cumplimiento de varios criterios:

- Funcionalidad. ¿hay alguna función de la dependencia que demande el constituir esta base datos?
- Finalidad: Que objetivo cumplo o busco con el tratamiento de esta información
- Pertinencia: ¿es pertinente crear, mantener o hacer tratamiento a esta información?
- Temporalidad: ¿Cuánto tiempo la debo tener?

Una vez se han detectado que efectivamente hay nuevas bases por registrar, debe indagarse y tener claro los siguientes ítems que hacen parte de la información que requiere el registro:

- Identificar la cantidad de Titulares por cada base de datos.
- Tener claro si la DIAN es responsable o hay un encargado (persona ajena a la entidad) de esta base de datos.
- Verificar los tipos de datos personales contenidos en cada base de datos.
- Identificar la ubicación de la base de datos. Ejemplo: servidor, computador personal, archivo físico.
- Determinar las medidas de seguridad aplicadas a la base de datos con el fin de minimizar riesgos.
- Identificar la forma de obtención de los datos.
- En caso de realizarse transferencia o transmisión internacional de los datos, deberá verificarse a qué países.
- Deberá contarse con la información de acceso al sistema, es decir, conocer el correo electrónico inscrito para ello y su clave de acceso.

Al ingresar al Registro Nacional de Bases de Datos - RNBD con el usuario asignado por favor tenga en cuenta el paso a paso para el registro y/o actualización de las bases de datos en la SIC. Ver el “Manual de Usuario del Registro Nacional de Bases de Datos – RNBD” en la página web de la SIC https://www.sic.gov.co/registro-nacional-de-bases-de-datos.

18.7. Medidas de Seguridad sobre las Bases de Datos con información de datos personales

- El almacenamiento, uso, consulta y protección de Bases de Datos personales en medios físicos y electrónicos será realizado cumpliendo con las medidas y políticas de seguridad definidas en el Sistema de Gestión de Seguridad de la Información y en las disposiciones establecidas en las políticas y lineamientos en materia de gestión documental de la DIAN.

- Toda la información calificada como pública clasificada o pública reservada debe, entre otras medidas de seguridad, almacenarse de manera cifrada, conforme con los lineamientos establecidos por la Dirección de Gestión de Innovación y Tecnología o quien haga sus veces.

- No está permitido el acceso, uso y/o reproducción de información a Bases de Datos con datos personales, a través de medios portátiles, de acceso público (sitios compartidos) o a los cuales se tenga acceso remoto.

- Cada base de datos dentro del registro del RNBD de la SIC, sugiere que debe contener unas medidas de seguridad, las cuales deben atenderse conforme con la capacidad de la entidad y los recursos disponibles.

19. FORMACIÓN Y CAPACITACIÓN

19.1. Procesos de formación y capacitación

La Oficina de Seguridad de la Información en su calidad de Oficial de Protección de datos personales de la DIAN, será la instancia que dará lineamientos a la Subdirección de Escuela de Impuestos y Aduanas o quien haga sus veces, para que realice el diseño, planeación, ejecución y evaluación de programas encaminados a la sensibilización, formación y capacitación sobre protección de datos personales especialmente enfocados en los siguientes campos:

- Programas de inducción, reinducción y/o entrenamiento que contengan temas o cursos especializados sobre seguridad y privacidad de la información y protección de datos personales.
- Programas de capacitación, internos o externos, en materia de protección de datos personales a todos los funcionarios de la entidad.
- Actividades de capacitación especializadas relacionadas con tratamiento de datos sensibles, de niños, niñas y adolescentes, datos biométricos, principio de responsabilidad demostrada, entre otros.
- Programas de capacitación para la alta dirección y para aquellos funcionarios que por el tipo de función que desempeñan tengan mayor responsabilidad en gestión de datos personales.
- Programas de capacitación para aliados estratégicos que realicen tratamiento de datos personales en nombre de la entidad, cuando ello se considere pertinente.
- Mediciones sobre la participación de los funcionarios en las actividades mencionadas que faciliten la administración y seguimiento de las evaluaciones.
- Mediciones sobre el conocimiento adquirido en la formación y capacitación a los distintos funcionarios, a través de evaluaciones en cada una de las capacitaciones.

20. SEGUIMIENTO, MONITOREO Y MEJORA CONTINUA

La Oficina de Seguridad de la Información en su calidad de Oficial de Protección de datos personales de la DIAN, debe definir dentro del Programa Integral de Gestión de datos personales, los instrumentos de control y seguimiento para la adecuada implementación del programa y realizar en conjunto con las dependencias, actividades de asistencia y asesoría, para asegurar el cumplimiento de las disposiciones normativas sobre la protección de los datos personales.

Para lo anterior, se deberán tener en cuenta al implementar medidas de seguimiento, monitoreo y mejora, por lo menos los siguientes controles:

- Controles en la implementación de las políticas, lineamientos y procedimientos establecidos en el presente manual.
- Controles a los procesos de recolección de información.
- Controles con respecto al almacenamiento.
- Controles a los procesos de formación y capacitación.
- Controles a las actividades de circulación de la información tales como Transferencia y/o transmisión de información a nivel nacional y/o internacional, intercambio, entrega, entre otros.
- Control para la Gestión de los encargados del tratamiento.
- Control a la atención de consultas, quejas y reclamos.
- Controles a los procesos y medidas de seguridad.

La Oficina de Seguridad de la Información hará seguimiento a las acciones desarrolladas en los planes de gestión de la entidad, que permitan evaluar las acciones que evidencien el cumplimiento del Principio de Responsabilidad Demostrada (accountability) así como las actividades asociadas a la implementación del Programa Integral de Gestión de Datos Personales que incluyen componentes relacionados con el registro de las bases de datos personales, implementación de políticas y procedimientos relacionados con la protección de datos personales, gestión de riesgos e incidentes y la sensibilización a los funcionarios de la Entidad. Así mismo, implementará acciones para hacer seguimiento al Modelo de Seguridad y Privacidad de la Información-MSPI de la entidad y al Sistema de Gestión de Seguridad y Privacidad de la Información-SGSPI, en lo relacionado con la implementación de los controles de la norma NTC-ISO/IEC 27001:2022 y la NTC-ISO/IEC 27701:2019.

Conforme con lo señalado en el Modelo Integrado de Planeación y Gestión-MIPG, la Oficina de Control Interno como dependencia responsable de hacer seguimiento y monitoreo de la gestión de la entidad, deberá incluir dentro de la programación de las auditorías independientes, el seguimiento a la implementación de la Política de Tratamiento de Datos Personales emitida por la Entidad y los lineamientos y procedimientos contemplados en el presente Manual.

En cumplimiento a las responsabilidades establecidas en el art.11 de la resolución 21 de enero de 2022, corresponde a la alta Dirección a través del Comité Institucional de Gestión y Desempeño, hacer seguimiento a las acciones y estrategias adoptadas para la operación del Modelo Integrado de Planeación y Gestión-MIPG en lo que respecta a la implementación y desarrollo de las políticas de desempeño institucional, en especial lo relacionado con la política de gobierno digital y seguridad digital.

El presente manual se revisará y/o actualizará al menos una vez al año o cuando ocurran cambios organizacionales, teniendo en cuenta los que se puedan presentar en relación con la legislación vigente, los lineamientos impartidos por las entidades líderes de política de desempeño Institucional como el Ministerio de Tecnologías de la Información- MINTIC, la Procuraduría General de la Nación y en especial los brindados por la Superintendencia de Industria y Comercio-SIC, entidad de control que regula y vigila la Protección de Datos Personales en el País. Así mismo, se tendrán en cuenta las recomendaciones que puedan ser brindadas por Organismos Internacionales como la OCDE, con el fin de acoger las buenas prácticas que en cuanto a privacidad de la información se puedan adoptar.

21. CONTROL DE CAMBIOS

Versión	Vigencia		Descripción de Cambios	Tipo de información
	Desde	Hasta		
1	02/10/2020	19/12/2021	Versión inicial.	No aplica
2	20/12/2021	01/04/2024	Versión 2 que reemplaza lo establecido en la versión 1, Se generaron ajustes en el documento, relacionados con el nombre del proceso de acuerdo con la nueva estructura de procesos establecida en el considerando	No aplica

Versión	Vigencia		Descripción de Cambios	Tipo de información
	Desde	Hasta		
			de la Resolución 060 del 11 de junio del 2020 y el Código alfabético del mismo en los numerales 12.5.2.3 (página 41), 12.5.5.1 (página 46), 15 (página 52), 16 (página 53), 16.1 (página 53), 17.1.1 (página 57), 17.1.2 (página 57), 17.1.3 (página 57), 17.1.4 (página 58), 17,1,7 (página 59), 17,1,8 (página 60), 17.3.1 (página 63) 17,3,2 (página 64) y 18.3 (página 68). Cabe aclarar, que el contenido técnico del documento no presenta cambios respecto a la versión anterior. Por lo tanto, cualquier consulta respecto a los contenidos técnicos de los mismos debe efectuarse a los elaboradores técnicos y revisores de la versión anterior. En el contenido del documento donde se relaciona una dependencia, se adicionó la frase "o quien haga sus veces".	
3	02/04/2024		Se realizaron ajustes de tipo de letra, tamaño y por temas de redacción (se eliminan párrafos similares, se reemplaza en todo el documento la palabra área por dependencia). Se agregaron y se actualizaron algunas definiciones en el punto 3. "definiciones y siglas". Se actualizó en la tabla de el punto 12.3 "almacenamiento y conservación de los datos personales obtenidos", se suprime el proceso o subproceso, puesto que actualmente la entidad está reestructurando los procesos. Se adicionó en el punto 12.5.5.2 contexto sobre: responsable y encargado del tratamiento, evaluación del impacto del tratamiento de datos personales, privacidad por diseño y por defecto, limitación al uso de la información.	Información Pública

Versión	Vigencia		Descripción de Cambios	Tipo de información
	Desde	Hasta		
			Se actualizó el nombre del anexo por cláusula, dado que se agrupó en un solo anexo como cláusulas, puntos 17.4 en adelante. En el punto 20. "seguimiento, monitoreo y mejora continua", se actualizó la resolución del Comité Institucional de Gestión y Desempeño y sus funciones asociadas.	

Elaboró	Diana María Toro Giraldo	Gestor II	Oficina de Seguridad de la Información
Revisó:	Héctor Mauricio Palacios Rincón	Gestor II	Oficina de Seguridad de la Información
Aprobó:	Edgar Fernando Avilés Gómez	Jefe Oficina de Seguridad de la Información (E)	Oficina de Seguridad de la Información

22. ANEXOS

- Anexo 1 MN0062 Autorizaciones: Guion telefónico institucional, Uso en eventos masivos y formatos físicos/electrónico.
- Anexo 2 MN0062 Aviso de privacidad.
- Anexo 3 MN0062 Aviso de privacidad de videovigilancia.
- Anexo 4 MN0062 Disclaimer sobre el tratamiento de datos personales.
- Anexo 5 MN0062 Cláusulas de protección, transferencia, transmisión y disposición final de datos personales.
- Anexo 6 MN0062 Modelos de contratos para transmisión y transferencia de datos personales.
- Anexo 7 MN0062 Matriz de finalidades para el tratamiento de datos personales.