

RESOLUCIÓN NÚMERO

(Fecha)

Por la cual se asignan las funciones de Oficial de Protección de Datos Personales a la Oficina de Seguridad de la Información y se fijan obligaciones de las áreas frente a la protección de datos personales en la Unidad Administrativa Especial – Dirección de Impuestos y Aduanas Nacionales – DIAN

**EL DIRECTOR GENERAL DE LA DIRECCIÓN DE IMPUESTOS Y ADUANAS
NACIONALES - DIAN**

En uso de las facultades legales y en especial las conferidas en el numeral 5º. del artículo 6º. del Decreto 4048 de 2008, el artículo 2.2.2.25.4.4. del Decreto Único Reglamentario 1074 de 2015, y

CONSIDERANDO

Que, la Constitución Política en su artículo 15 establece que “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de los datos se respetarán la libertad y demás garantías consagradas en la Constitución ...”

Que la Ley Estatutaria 1581 de 2012, “Por la cual se dictan disposiciones generales sobre la Protección de Datos Personales” en su artículo 1º. señala “Objeto: La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y de los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política.”

Que el Decreto 1074 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.”, en su artículo 2.2.2.25.4.4., establece que “Todo Responsable y Encargado deberá designar a una persona o área que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el presente capítulo.”

Que el artículo 2.2.2.25.6.1 del Decreto 1074 de 2015 establece: “Demostración. Los responsables del 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 y este capítulo...”

Continuación de la Resolución “Por la cual se asignan las funciones de Oficial de Protección de Datos Personales a la Oficina de Seguridad de la Información y se fijan obligaciones de las áreas frente a la protección de datos personales en la Unidad Administrativa Especial – Dirección de Impuestos y Aduanas Nacionales – DIAN”

Así mismo, el artículo 2.2.2.25.6.2. del Decreto 1074 de 2015 dispone que, en los casos de los numerales 1 a 4 del artículo 2.2.2.25.6.1, las medidas efectivas y apropiadas implementadas por el sujeto responsable del tratamiento de los datos personales, deben ser consistentes con las instrucciones impartidas por la Superintendencia de Industria y Comercio y garantizar: i) La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas acordes con Ley 1581 de 2012 y este capítulo, (ii) La adopción de mecanismos internos para poner en práctica las políticas, que incluyan herramientas de implementación, entrenamiento y programas de educación y (iii) La adopción de procesos para la atención de reclamos y consultas de los titulares respecto a cualquier aspecto del tratamiento.

Que la Superintendencia de Industria y Comercio, expidió la Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability) 2016, la cual enmarca la implementación del Programa Integral de Gestión de Datos Personales para el cumplimiento efectivo de las políticas internas, por parte de los sujetos responsables del tratamiento de los datos personales.

Que la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales - DIAN dentro de su Plan Estratégico y, especialmente, como iniciativa estratégica, avanza en la implementación del Programa Integral de Gestión de Datos Personales y como componente de avance de este programa está la definición del compromiso de la organización y de las responsabilidades específicas para otras áreas de la entidad respecto a la recolección, almacenamiento, uso, circulación y eliminación o disposición final de los datos personales que se tratan en la DIAN.

Que el Decreto 2183 de 2017 creó la Oficina de Seguridad de la Información en la DIAN a la que le corresponden funciones relacionadas con la seguridad y *privacidad* de la información.

Que teniendo en cuenta que la protección de datos abarca: (i) La seguridad de la información; (ii) El respeto por la normatividad que la regula; y (iii) La conservación de las bases de datos personales, tanto electrónicas como físicas, (iv) la identificación, medición, control y monitoreo de riesgos asociados al tratamiento de datos, se deben asignar responsabilidades particulares a las áreas sobre protección de datos y asignar al interior de la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales - DIAN las funciones de Oficial de Protección de Datos Personales a la Oficina de Seguridad de la Información, para que asuma la coordinación en la definición, implementación de las políticas, programas, manuales, directrices, lineamientos, procesos y procedimientos adoptados por la DIAN para cumplir las normas sobre protección e implementación de buenas prácticas de gestión de datos personales.

Conforme con el Compromiso de la Organización, establecido en la Guía para la Implementación del Principio de la Responsabilidad demostrada y para lograr que la implementación del Programa Integral de Gestión de Datos Personales en la DIAN sea efectivo en el cumplimiento de las medidas que promuevan los principios de privacidad y protección de datos, es necesario que las áreas asuman obligaciones generales y específicas respecto de la recolección, almacenamiento, uso, circulación y eliminación o disposición final de los datos personales que se tratan en la DIAN.

Continuación de la Resolución “Por la cual se asignan las funciones de Oficial de Protección de Datos Personales a la Oficina de Seguridad de la Información y se fijan obligaciones de las áreas frente a la protección de datos personales en la Unidad Administrativa Especial – Dirección de Impuestos y Aduanas Nacionales – DIAN”

Que de conformidad con lo dispuesto en el numeral 8 del artículo 8 de la Ley 1437 de 2011, en concordancia con lo dispuesto en el artículo 32 de la Resolución 204 de 2014 de la DIAN, modificado por el artículo 1º de la Resolución 37 de 2018 de la DIAN, el proyecto fue publicado en el sitio web de la Dirección de Impuestos y Aduanas Nacionales - DIAN, con el objeto de recibir opiniones, sugerencias o propuestas alternativas, las cuales fueron revisadas en cuanto a su procedencia, previamente a la expedición de esta reglamentación.

En mérito de lo expuesto,

RESUELVE

ARTICULO 1º. Asignar a la Oficina de Seguridad de la Información de la entidad las funciones de Oficial de Protección de Datos Personales en la Unidad Administrativa Especial – Dirección de Impuestos y Aduanas Nacionales – DIAN, en adelante UAE-DIAN.

La Oficina de Seguridad de la Información, en su función de Oficial de Protección de Datos Personales tendrá la autonomía para estructurar, diseñar, implementar y administrar el programa que le permita a la entidad cumplir con las normas sobre protección de datos personales, así como establecer los controles de ese programa, su evaluación y revisión permanente. No obstante, para la correcta ejecución de sus funciones y actividades, requerirá del cumplimiento de las responsabilidades de las distintas áreas de la DIAN, conforme las directrices, políticas y procedimientos que establezca el Oficial de Protección de Datos de la UAE-DIAN.

ARTÍCULO 2º. Funciones del Oficial de Protección de Datos Personales. Son funciones de la Oficina de Seguridad de la Información, actuando en calidad de Oficial de Protección de Datos Personales de la UAE-DIAN, conforme a la Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability) 2016, emitida por la Superintendencia de Industria y Comercio- SIC, entre otras, las siguientes:

- a. Estructurar, diseñar y administrar el Programa Integral de Gestión de Protección de Datos Personales.
- b. Servir de enlace y coordinador con las demás áreas de la entidad para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales.
- c. Coordinar con las áreas de la entidad para que se desarrolle una implementación efectiva de las políticas, buenas prácticas y procedimientos adoptados por la DIAN para el cumplimiento de las normas de Protección de Datos Personales.
- d. Emitir y mantener actualizados los procedimientos, políticas, lineamientos y directrices relacionados con la Protección de Datos Personales en la DIAN.
- e. Asistir a las áreas para que den trámite a las solicitudes de los titulares para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el Decreto Único Reglamentario 1074 de 2015, cuando las dependencias lo consideren pertinente.
- f. Promover, con el con el apoyo de la Coordinación Escuela y la Oficina de Comunicaciones, o las dependencias que hagan sus veces, una cultura de protección de datos personales dentro de la DIAN a través de actividades de

Continuación de la Resolución “Por la cual se asignan las funciones de Oficial de Protección de Datos Personales a la Oficina de Seguridad de la Información y se fijan obligaciones de las áreas frente a la protección de datos personales en la Unidad Administrativa Especial – Dirección de Impuestos y Aduanas Nacionales – DIAN”

entrenamiento, sensibilización y capacitación a los servidores públicos de la DIAN.

- g. Coordinar para que se realice la articulación y control de los riesgos identificados por las áreas, derivados del tratamiento de datos personales, al Sistema Integrado de Gestión de Riesgos de la entidad.
- h. Gestionar acciones para que las dependencias de la DIAN identifiquen, realicen el inventario, registren, actualicen y reporten a la Oficina de Seguridad de la Información, en calidad de Oficial de Protección de Datos, las novedades relacionadas con bases de datos personales, conforme con los lineamientos de las autoridades competentes y la normativa vigente.
- i. Avalar la actualización y el registro de las nuevas bases de datos de la entidad, identificadas y reportadas por las dependencias correspondientes, en el Registro Nacional de Bases de Datos dispuesto por la SIC.
- j. Obtener las declaraciones de conformidad de la Superintendencia de Industria y Comercio (SIC), cuando sea requerido, para la transferencia o transmisión de datos a nivel internacional a países que no estén certificados como seguros.
- k. Desarrollar acciones para que las áreas realicen la implementación efectiva de las políticas, procedimientos y documentos adoptados por la DIAN para cumplir las normas de privacidad y protección de datos, así como la implementación de buenas prácticas de gestión de datos personales dentro de la DIAN.
- l. Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización (talento humano, seguridad, calls centers y gestión de proveedores, etc.”
- m. Coordinar la implementación de planes de auditoría, evaluación y mejora para verificar el cumplimiento por parte de las áreas, de las políticas, procedimientos y lineamientos relacionados con protección de datos personales en la DIAN.
- n. Revisar los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con Encargados no residentes en Colombia.
- o. Emitir lineamientos para que las áreas competentes que suscriban cualquier figura jurídica que comprenda intercambio, transmisión, transferencia, entrega de información a terceros, involucren el cumplimiento de las normas de protección de datos personales y las medidas de seguridad y privacidad por las partes.
- p. Expedir reglamentación interna para implementar el Programa Integral de Gestión de Datos Personales como circulares, memorandos, entre otros.
- q. Solicitar a las dependencias reportes, informes y cualquier otro requerimiento que permita la evaluación y gestión del programa.
- r. Supervisar el cumplimiento de los lineamientos a seguir en caso de Incidentes de Seguridad en materia de Protección de Datos.
- s. Acompañar y asistir a la UAE-DIAN en la atención de visitas de inspección y a los requerimientos que realicen las autoridades de control y administrativas competentes, en materia de protección de datos personales.
- t. Reportar ante la SIC, los incidentes detectados directamente por la Oficina de Seguridad de la información en su calidad de Oficial de Protección de Datos Personales o los reportados por las áreas, relacionados con la violación a los códigos de seguridad, pérdida, robo y/o acceso no autorizado o fraudulento de información de las bases de datos personales físicas o electrónicas, dentro de los 15 días hábiles siguientes al momento en que se detecten y sean puestos en su conocimiento.
- u. Presentar los informes o el estado de avance del Programa Integral de Gestión de Protección de Datos que la alta dirección o los organismos de control requieran sobre protección de datos personales.

Continuación de la Resolución “Por la cual se asignan las funciones de Oficial de Protección de Datos Personales a la Oficina de Seguridad de la Información y se fijan obligaciones de las áreas frente a la protección de datos personales en la Unidad Administrativa Especial – Dirección de Impuestos y Aduanas Nacionales – DIAN”

- v. Establecer los controles al programa de gestión de datos personales, así como realizar su evaluación y revisión permanente.
- w. Las demás, acordes con la naturaleza de sus funciones, de conformidad con la normativa relacionada con la protección de datos personales.

ARTÍCULO 3º.- Obligaciones de las áreas frente a la protección de los datos personales. Será responsabilidad de los Directores de Gestión, Defensor del Contribuyente y del Usuario Aduanero, Jefes de Oficina, Directores Seccionales, Subdirectores, Jefes de Coordinación, Jefes de División y Jefes de Grupos Internos de Trabajo, apoyar la coordinación e implementación del Programa Integral de Gestión de Datos Personales, en los términos y bajo las políticas, directrices y lineamientos que fije el Oficial de Protección de Datos de la UAE-DIAN.

Además de lo anterior, cada una de las áreas, bajo la dirección de sus respectivos jefes, deberá cumplir con las siguientes obligaciones generales y específicas, respecto de la recolección, almacenamiento, uso, circulación y eliminación o disposición final de los datos personales que se recolectan y tratan en la DIAN.

Obligaciones Generales de las Áreas.

1. Implementar y cumplir con las normas, políticas, lineamientos, procedimientos, manuales, medidas de seguridad y demás directrices relacionadas con la protección de datos personales en la DIAN.
2. Responder las peticiones, consultas y reclamos que interpongan los Titulares de datos personales, así como facilitar el ejercicio sus derechos, respecto al conocimiento, acceso, rectificación, actualización, revocatoria y supresión de los mismo, siempre y cuando el Titular no tenga obligaciones legales, contractuales o judiciales que limiten o impidan sus requerimientos.
3. Adoptar las disposiciones normativas, políticas y lineamientos relacionados con protección de datos personales, en la caracterización, definición, elaboración y evaluación de los procesos, procedimientos, herramientas conceptuales, tecnológicas, formularios, formas, formatos, instructivos, cartillas y servicios informáticos electrónicos, necesarios para la estandarización y desarrollo adecuado de las actividades del área o proceso.
4. Incorporar en las especificaciones de diseño de procesos, infraestructura física o prácticas de negocio, medidas de seguridad y confianza que protejan la privacidad de la información.
5. Asegurar, desde antes que se recolecte los datos y durante todo el ciclo de vida de los mismos, que la privacidad y la seguridad sean parte del diseño, arquitectura y configuración predeterminada del proceso de gestión de información y de las infraestructuras que lo soportan.
6. Adecuar e implementar en el área o proceso, los avisos, autorizaciones, cláusulas, convenios, contratos, compromisos de confidencialidad, protocolos y demás instrumentos jurídicos que garanticen la protección de la información por cuenta de empleados, contratistas o terceros.
7. Conocer qué datos personales recolecta o almacena el área, en calidad de qué figura lo hace (responsable o encargado), cómo los utiliza y revisar si realmente los necesitan, conforme con la finalidad para lo cual los recolectan.
8. Realizar la identificación, inventario, registro y actualización, previo los requerimientos, lineamientos y aval de la Oficina de Seguridad de la información,

Continuación de la Resolución “Por la cual se asignan las funciones de Oficial de Protección de Datos Personales a la Oficina de Seguridad de la Información y se fijan obligaciones de las áreas frente a la protección de datos personales en la Unidad Administrativa Especial – Dirección de Impuestos y Aduanas Nacionales – DIAN”

en su calidad de Oficial de Protección de Datos Oficial de Protección de datos, de las bases de datos personales (físicas o electrónicas) del área o proceso, conforme con su finalidad, funcionalidad, pertinencia y temporalidad y las directrices y disposiciones de la Superintendencia de Industria y Comercio y la Procuraduría General de la Nación.

9. Reportar conforme con el procedimiento establecido, ante la Oficina de Seguridad de la información, en su calidad de Oficial de Protección de Datos el Oficial de Protección de Datos Personales, cualquier incidente, violación a los códigos de seguridad, pérdida, robo y/o acceso no autorizado o fraudulento de información de las bases de datos personales físicas o electrónicas, con el fin de generar el reporte del incidente ante la SIC dentro de los 15 días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento.
10. 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.
11. Facilitar y apoyar el entrenamiento, las capacitaciones, sensibilizaciones y actividades que promuevan la cultura de protección de datos personales en la DIAN.
12. Realizar en conjunto con la Coordinación de Perfilamiento de Riesgos o quien haga sus veces, el análisis de riesgos que permitan identificar las amenazas y vulnerabilidades relacionadas con las bases de datos en las que se realice tratamiento de datos personales y que se encuentren bajo responsabilidad del área.
13. Verificar que se realice, conforme con los términos y procedimientos establecidos, la conservación y disposición final, o eliminación o borrado de la(s) base(s) de dato(s) tanto de propiedad de la DIAN como las que se han dispuesto a un encargado o a un tercero, conforme con la finalidad para la(s) que fue(ron) creadas, transmitidas o transferidas, las Tablas de Retención Documental y los lineamientos dados por la Subdirección de Gestión de Recursos Físicos o la que haga sus veces en materia de gestión documental.
14. Implementar las medidas de control y validación necesarias para que a las bases de datos accedan únicamente las personas autorizadas, se encuentren dispuestas en entornos físicos o digitales seguros y confiables, así como conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
15. Adecuar los procesos y procedimientos del área para que las actividades de entrega, transferencia, transmisión o intercambio de información nacional e internacional que contiene datos personales, sean acordes con la normativa vigente, las medidas jurídicas, de seguridad y las políticas y procedimientos que sobre protección de datos tenga o emita la Entidad.
16. Implementar las formas y cláusulas contractuales, así como los protocolos establecidos, necesarios para que el uso, intercambio, transferencia y transmisión de la información, nacional e internacional, relacionada con protección de datos personales se realice conforme con las normas que sobre el tema rigen la materia, los convenios y normas internacionales y las políticas de la Entidad.
17. Asegurar la aplicación de normas y políticas de protección de datos personales en el uso de las redes sociales, medios de comunicación, sitio web y demás canales de comunicación que operen en la Entidad.
18. Atender los requerimientos de la Oficina de Seguridad de la información, en su calidad de Oficial de Protección de Datos relacionados con la implementación de

Continuación de la Resolución “Por la cual se asignan las funciones de Oficial de Protección de Datos Personales a la Oficina de Seguridad de la Información y se fijan obligaciones de las áreas frente a la protección de datos personales en la Unidad Administrativa Especial – Dirección de Impuestos y Aduanas Nacionales – DIAN”

políticas, procedimientos y lineamientos adoptados para la Protección de Datos Personales en la DIAN ;

19. Contemplar el enfoque de privacidad por diseño, en los servicios de interoperabilidad, trámites, servicios de ciudadanía digital que requieran las áreas, las empresas públicas y privadas y los ciudadanos y/o usuarios.
20. Conservar las evidencias documentales de publicación de los avisos de privacidad, suscripción de compromisos de confidencialidad, autorizaciones de los titulares, así como las peticiones elevadas por los mismos, respecto al tratamiento de datos, que se generen desde la recolección hasta la disposición final de los mismos.
21. Implementar las medidas de protección de datos personales en las distintas sedes de la entidad, para garantizar su adecuado tratamiento, desde su recolección hasta su disposición final, tales como, avisos de privacidad, autorizaciones de recolección masivas, sistemas de video vigilancia, recolección de datos biométricos.

Obligaciones específicas de las áreas:

Oficina de Control Interno

1. Contemplar en los planes de Auditoría Interna componentes de evaluación tanto de la implementación del Programa Integral de Gestión de Datos Personales, como de las políticas, lineamientos, manuales y procedimientos relacionados con Protección de Datos Personales.

Dirección de Gestión de Recursos y Administración Económica

1. Asignar los recursos financieros, técnicos, físicos y de talento humano necesarios para la adopción e implementación del Programa Integral de Gestión de Datos Personales de la DIAN.
2. Dirigir acciones para que en cada una de las sedes de la Entidad se cumplan las políticas, procedimientos y lineamientos sobre protección de datos personales, especialmente lo relacionado con recolección de datos personales por acceso a los edificios y áreas, mediante sistemas de videovigilancia, captura de datos biométricos, medidas de seguridad físicas, adecuación mobiliaria, entre otros.
3. Dirigir acciones que contribuyan a la implementación de políticas, procedimientos, mecanismos, instrumentos, avisos de privacidad, autorizaciones, cláusulas y compromisos de confidencialidad, para el tratamiento y protección de datos personales desde su recolección hasta su disposición final, de los aspirantes a ocupar empleos en la Entidad, contratistas, partes interesadas, empleados y familiares, especialmente la relacionada con niños, niñas y adolescentes y conservar las evidencias correspondientes.
4. Dirigir acciones encaminadas a incluir en los planes de entrenamiento, inducción, reinducción, formación y capacitación, para los empleados de la Entidad, programas, temas o módulos sobre Protección de Datos Personales en la DIAN.
5. Establecer las políticas y normas de administración documental de la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales (DIAN), en concordancia con las políticas de seguridad y privacidad de la información.

Subdirección de Gestión de Personal

1. Implementar procedimientos, mecanismos, instrumentos, avisos de privacidad, autorizaciones, cláusulas y compromisos de confidencialidad, para el tratamiento y

Continuación de la Resolución “Por la cual se asignan las funciones de Oficial de Protección de Datos Personales a la Oficina de Seguridad de la Información y se fijan obligaciones de las áreas frente a la protección de datos personales en la Unidad Administrativa Especial – Dirección de Impuestos y Aduanas Nacionales – DIAN”

protección de datos personales desde su recolección hasta su disposición final, de los aspirantes a ocupar empleos en la Entidad, empleados y familiares, especialmente los relacionados con niños, niñas y adolescentes, desde los procesos de reclutamiento y selección hasta su retiro definitivo de la Entidad o el que disponga la TRD documental del área.

2. Dirigir acciones para que en los programas y/o planes de entrenamiento, inducción, reinducción y capacitación se desarrollen cursos, módulos, temas o cualquier otro tipo de formación dirigida a fortalecer la cultura por la protección de los datos personales en la Entidad.

Subdirección de Gestión de Recursos Físicos

1. Dirigir acciones para que en cada una de las sedes de la Entidad se cumplan las políticas, procedimientos y lineamientos sobre protección de datos personales, especialmente lo relacionado con recolección de datos personales por acceso a los edificios y áreas, mediante sistemas de videovigilancia, captura de datos biométricos, medidas de seguridad físicas, adecuación mobiliaria, entre otros.
2. Implementar políticas, procedimientos, mecanismos de recolección e instrumentos jurídicos necesarios para el tratamiento y protección de datos personales de contratistas y proveedores.
3. Diseñar e implementar las políticas, directrices y acciones relacionadas con la gestión documental, que permita a las áreas dar cumplimiento a las normas y lineamientos de protección de datos personales desde su recolección hasta su disposición final, tanto en medios físicos como en digitales.
4. Asistir a las áreas de la Entidad para que definan adecuadamente la disposición final de las bases de datos físicas y electrónicas, conforme con las normas de gestión documental y las de protección de datos personales.

Subdirección de Gestión de Control Disciplinario Interno

1. Promover acciones preventivas disciplinarias frente al uso adecuado de la información, especialmente la relacionada con protección de datos personales, ley habeas data y ley de transparencia.
2. Adelantar las acciones pertinentes frente al incumplimiento de las normas de protección de datos personales por parte de los servidores de la DIAN

Dirección de Gestión Organizacional

1. Emitir lineamientos y directrices para que las áreas adopten la normativa y políticas relacionadas con protección de datos personales en el Sistema de Gestión de Calidad, especialmente en la caracterización, definición, elaboración y evaluación de los procesos, procedimientos, herramientas conceptuales, tecnológicas, los formularios, formas, formatos, instructivos y cartillas y de los servicios informáticos electrónicos y servicios ciudadanos digitales, necesarios para la estandarización y desarrollo adecuado de las actividades de la Entidad, en concordancia con la normativa vigente.

Continuación de la Resolución “Por la cual se asignan las funciones de Oficial de Protección de Datos Personales a la Oficina de Seguridad de la Información y se fijan obligaciones de las áreas frente a la protección de datos personales en la Unidad Administrativa Especial – Dirección de Impuestos y Aduanas Nacionales – DIAN”

2. Dirigir acciones para que el Sistema de Gestión de Riesgos de la Entidad incorpore para su tratamiento, los riesgos relacionados con Protección de Datos Personales identificados por las áreas o procesos.
3. Emitir lineamientos, disposiciones y directrices para que se adopten las políticas, normas y procedimientos relacionados con protección de datos personales en la reglamentación, implementación y evaluación de las políticas, alternativas y especificaciones técnicas para la adquisición, construcción y desarrollo de la tecnología de la información, hardware, software, comunicaciones, seguridad informática y de los servicios informáticos electrónicos y servicios ciudadanos digitales, dentro de la arquitectura técnica de la Entidad.
4. Incorporar en las especificaciones de diseño de procesos, infraestructura física o prácticas de negocio y de continuidad del negocio, medidas de seguridad y confianza que protejan la privacidad de la información.
5. Contemplar el enfoque de privacidad por diseño en los servicios de interoperabilidad, trámites y servicios de ciudadanía digital que requieran las áreas, las empresas públicas y privadas y los ciudadanos.
6. Dirigir 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. Desde antes que se recolecte información y durante todo el ciclo de vida de la misma, se debe asegurar que 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.
7. Identificar y clasificar la data con categoría "Datos Personales" con el fin de implementar medidas legales, de seguridad y protección, frente a las acciones de analítica de la información, gobernanza de datos, segregación, agregación e inteligencia artificial.

Subdirección de Gestión de Tecnologías de la Información y las Comunicaciones

1. Asegurar que la privacidad y la seguridad hagan parte del diseño, arquitectura y configuración predeterminada del proceso de gestión de información y de las infraestructuras que lo soportan.
2. Realizar los diseños digitales y tecnológicos teniendo en cuenta la protección de la información. Por lo anterior en las especificaciones de diseño de tecnologías, procesos, prácticas de negocio, de continuidad del negocio e infraestructuras físicas, se deben contemplar e incorporar medidas que aseguren la protección de la privacidad de la información.
3. Adoptar medidas preventivas de diversa naturaleza (tecnológica, organizacional, humana, procedimental) desde antes que se recolecte información y durante todo el ciclo de vida de la misma, 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.
4. Implementar las formas y cláusulas contractuales, así como los protocolos establecidos, necesarios para que el uso, intercambio, transferencia y transmisión de la información, nacional e internacional, relacionada con protección de datos personales se realice conforme con las normas que sobre el tema rigen la materia,

Continuación de la Resolución “Por la cual se asignan las funciones de Oficial de Protección de Datos Personales a la Oficina de Seguridad de la Información y se fijan obligaciones de las áreas frente a la protección de datos personales en la Unidad Administrativa Especial – Dirección de Impuestos y Aduanas Nacionales – DIAN”

los convenios internacionales, las disposiciones de la Superintendencia de Industria y Comercio y de la Procuraduría General de la Nación y las políticas de la Entidad.

5. Implementar en los sistemas informáticos, plataformas, documentos electrónicos, servicios ciudadanos digitales, entre otros, avisos de privacidad, autorizaciones, mensajes de texto, cláusulas y compromisos de confidencialidad, en el tratamiento de datos personales desde su recolección hasta su disposición final.
6. Contemplar el enfoque de privacidad por diseño, en los servicios de interoperabilidad, trámites, servicios de ciudadanía digital que requieran las áreas, las empresas públicas y privadas y los ciudadanos y/o usuarios.
7. Diseñar mecanismos que permitan la conservación de los avisos de privacidad, compromisos de confidencialidad y autorizaciones para el tratamiento de datos otorgadas por los titulares, que se generen desde la recolección hasta la disposición final de los datos.

Subdirección de Gestión de Procesos y Competencias Laborales

1. Asistir a las áreas para que en el diseño de la caracterización de los procesos, procedimientos y sus documentos soporte, herramientas tecnológicas, formularios y de los servicios informáticos electrónicos y servicios ciudadanos digitales, se incorporen los instrumentos y mecanismos para la recolección, protección y tratamiento de datos personales, tales como, áreas responsables de la generación y uso de la información, avisos de privacidad, autorizaciones, protocolos, interoperabilidad de los datos y demás disposiciones que deban adecuarse o incorporarse desde el Sistema de Gestión de Calidad de la Entidad relacionados con el cumplimiento de la normativa y políticas de protección de datos personales de la DIAN.
2. Identificar en los documentos del Sistema de Gestión de Calidad, la clasificación de la información (pública clasificada y pública reservada) así como la categoría de datos personales.
3. 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.

Subdirección de Gestión de Asistencia al Cliente

1. Adoptar en los puntos y canales dispuestos por la DIAN donde se realice tratamiento de datos personales, las autorizaciones, avisos, protocolos, compromisos, normas, políticas, lineamientos, procedimientos, formatos e instructivos relacionados con protección de datos personales de los titulares de información en la DIAN.
2. Gestionar mediante el sistema de información de PQRS dispuesto por la Entidad, dentro de los términos establecidos por las normas sobre protección de datos, las solicitudes de modificación, rectificación o supresión de los datos presentadas por los titulares y relacionadas con protección de datos personales, así como los informes correspondientes, conforme con lo establecido en las normas legales y la política de tratamiento de datos personales de la DIAN.
3. Incorporar en los diseños físicos, digitales y tecnológicos, asociados a nuevos canales, trámites, servicios o desarrollos para facilitar la interacción con el

Continuación de la Resolución “Por la cual se asignan las funciones de Oficial de Protección de Datos Personales a la Oficina de Seguridad de la Información y se fijan obligaciones de las áreas frente a la protección de datos personales en la Unidad Administrativa Especial – Dirección de Impuestos y Aduanas Nacionales – DIAN”

ciudadano, el enfoque de privacidad por diseño, lo cual contempla la incorporación en las especificaciones, elementos que aseguren la protección de la privacidad de la información.

4. Asegurar la aplicación de normas y políticas de protección de datos personales en el uso de los canales habilitados a los ciudadanos, actividades relacionadas con cultura de la contribución y Registro Único Tributario RUT.

PARÁGRAFO. - Será de obligatorio cumplimiento para todas las áreas de la Entidad, la adopción y adecuación de las medidas y responsabilidades aquí dispuestas, en los planes, procesos, procedimientos, infraestructura, recursos físicos, humanos y tecnológicos, entre otros. La Oficina de Seguridad de la Información, en cumplimiento de las funciones de Oficial de Protección de Datos Personales y las áreas responsables de implementación **tendrán un plazo de doce (12) meses**, contados a partir de la fecha de publicación del manual de políticas y procedimientos de protección de datos personales, para desarrollar e implementar las acciones dispuestas en el presente acto.

ARTICULO 4º.- La presente resolución rige a partir de la fecha de su publicación.

PÚBLIQUESE Y CÚMPLASE

Dada en Bogotá D.C., a los días del mes de del 2020

JOSÉ ANDRÉS ROMERO TARAZONA
Director General

Proyectó: Yamile Chica Rodríguez/ Inspector II de Oficina de Seguridad de la Información
Revisó y Aprobó: Amanda Isabel Trujillo Mora/Oficina de Seguridad de la Información
Aprobó: Nohora Jazmín Nieto Mendoza /Oficina de Seguridad de la Información
Revisó: María Helena Caviedes Camargo / Inspector III DGJ
Revisó y aprobó: Liliana Andrea Forero Gómez/Directora de Gestión Jurídica