DIRECION DE IMPUESTOS Y ADUANAS NACIONALES

Resolucion No 000101

09-11-2020

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 Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales (Dian), en uso de las facultades legales y en especial las conferidas en el numeral 5 del artículo 6º del Decreto número 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 ; así como el derecho a la información consagrado en el artículo 20 de la misma*".

Que el Decreto número 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 número 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…*".

Así mismo, el artículo 2.2.2.25.6.2. del Decreto número 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 disposiciones impartidas por la Superintendencia de Industria y Comercio (en adelante SIC) 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 la 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 los numerales 5 y 6 del artículo 2.2.17.1.6. del Decreto 620 de 2020, contemplan los principios de privacidad por diseño y por defecto y el de seguridad, privacidad y circulación restringida de la información, respectivamente, como orientadores para la prestación de los servicios ciudadanos digitales de que disponga la entidad.

Que la SIC, 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, con 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 número 2183 de 2017 creó la Oficina de Seguridad de la Información en la estructura de la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales (DIAN), asignándole 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 entidad para cumplir las normas sobre protección e implementación de buenas prácticas de gestión de datos personales.

Que el artículo 5º de la Resolución número 33 de 2017 de la DIAN, dispuso: "Responsabilidades. El competente para la aprobación, actualización y publicación de la información contenida en los instrumentos de gestión de la información pública es el director de gestión o jefe de oficina responsable del proceso que produzca o administre la información, de conformidad con los lineamientos proferidos por la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales (DIAN)".

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 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 número 204 de 2014 de la DIAN, modificado por el artículo 1º de la Resolución número 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:

Artículo 1º. Asignar a la Oficina de Seguridad de la Información 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.

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 SIC, entre otras, las siguientes:

1. Estructurar, diseñar y administrar el Programa Integral de Gestión de Datos Personales.

2. Presentar para aprobación y monitoreo del Comité Institucional de Gestión y Desempeño de la entidad, el Programa Integral de Gestión de Datos Personales.

3. 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.

4. Realizar el acompañamiento a las áreas que lo requieran, en cuanto a la implementación de las medidas de seguridad y protección de datos personales y el cumplimiento de las obligaciones dispuestas para cada una de las dependencias en el presente acto administrativo.

5. Liderar y coordinar con las demás dependencias de la entidad, para que estas lleven a cabo la implementación de las disposiciones, principios, políticas, lineamientos, directrices, buenas prácticas, procedimientos y documentos que adopte la UAE-DIAN, para el cumplimiento de la normativa de protección de datos personales.

6. Emitir y mantener actualizados las directrices, lineamientos, políticas y procedimientos relacionados con la protección de datos personales en la UAE-DIAN.

7. 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.

8. Promover, con el apoyo de la Coordinación Escuela de Impuestos y Aduanas Nacionales y la Oficina de Comunicaciones, o las dependencias que hagan sus veces, la cultura de protección de datos personales dentro de la UAE-DIAN, por medio de actividades generales y específicas para las áreas, de entrenamiento, sensibilización y capacitación a los servidores públicos de la entidad, respectivamente.

9. 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.

10. Gestionar acciones para que las dependencias de la UAE-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.

11. 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.

12. Obtener las declaraciones de conformidad de la SIC, cuando sea requerido.

13. Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización (talento humano, seguridad, gestión documental, centros de llamadas y gestión de proveedores, etc.)

14. Coordinar con la Oficina de Control Interno y con las demás dependencias, 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 UAE-DIAN.

15. Revisar los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con encargados no residentes en Colombia.

16. Emitir lineamientos para que las áreas responsables de la información personal, que realicen y autoricen medidas de circulación de datos tales como intercambio, transmisión, transferencia, entrega de información a terceros, entre otras; involucren el cumplimiento de las normas de protección de datos personales y las medidas de seguridad y privacidad que deben asumir los nuevos responsables y/o encargados del tratamiento.

17. Expedir la regulación interna para implementar el Programa Integral de Gestión de Datos Personales como circulares, memorandos, entre otros.

18. Solicitar a las dependencias reportes, informes y cualquier otro requerimiento que permita la evaluación y gestión del programa.

19. Supervisar el cumplimiento de los lineamientos a seguir en caso de incidentes de seguridad en materia de protección de datos.

20. 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.

21. 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.

22. 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.

23. Establecer los controles al programa de gestión de datos personales, así como realizar su evaluación y revisión permanente.

24. Las demás, acordes con la naturaleza de sus funciones, de conformidad con la normativa relacionada con la protección de datos personales.

Artículo 3º. *Obligaciones generales de las áreas frente a la protección de los datos personales*. Para la adecuada ejecución de sus funciones el Oficial de Protección de Datos, requerirá del cumplimiento de las responsabilidades de las distintas áreas de la entidad, frente a la privacidad de la información y la protección de datos personales, conforme con las directrices, lineamientos, políticas y procedimientos que establezca el Oficial de Protección de Datos de la UAE-DIAN.

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 Grupo Interno de Trabajo, o quienes hagan sus veces, apoyar la coordinación e implementación del Programa Integral de Gestión de Datos Personales, en los términos y bajo las directrices, lineamientos, políticas y procedimientos que fije el Oficial de Protección de Datos de la UAE-DIAN.

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

1. Solicitar el acompañamiento del Oficial de Protección de Datos, en cuanto a la implementación de las medidas de protección de datos personales necesarias para el cumplimiento de las obligaciones dispuestas en el presente acto administrativo.

2. Designar los enlaces de seguridad y privacidad de la información en cada una de las dependencias, quienes serán los interlocutores y gestores de las actividades que demande la implementación de las medidas y controles del Sistema de Gestión de Seguridad de la Información y de protección de datos personales de responsabilidad del área.

3. Implementar y cumplir con las normas, principios, lineamientos, políticas, procedimientos, manuales, medidas de seguridad, formatos, guías y demás directrices relacionadas con la protección de datos personales en la UAE-DIAN.

4. Responder, conforme con los procedimientos establecidos en la Política de Tratamiento de Datos Personales de la UAE-DIAN, las peticiones, consultas y/o reclamos que interpongan los titulares, respecto de las bases de datos personales de las cuales el área haga tratamiento, así como facilitar el ejercicio de sus derechos, en cuanto al conocimiento, acceso, rectificación, actualización, revocatoria y supresión de los mismos, siempre y cuando el titular no tenga obligaciones legales, contractuales o judiciales que limiten o impidan

sus requerimientos, cada área llevará el control de las PQSR atendidas relacionadas con protección de datos para posterior registro ante la SIC.

5. Adoptar las disposiciones normativas, políticas, lineamientos e instrumentos, 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.

6. 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.

7. Asegurar, desde antes que se recolecten 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.

8. Implementar en el área o proceso, conforme con sus funciones y competencias, los avisos de privacidad, 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.

9. Conocer qué datos personales recolecta o almacena el área, naturaleza de los datos, en calidad de qué figura lo hace (responsable o encargado), cómo los utilizan y revisar si realmente los necesita, conforme con la finalidad para la cual son recolectados.

10. Realizar la identificación, inventario, registro y actualización, previos los requerimientos, lineamientos y aval de la Oficina de Seguridad de la información, en su calidad de Oficial de Protección de Datos, de los activos de información que contienen bases de datos personales (físicas o electrónicas) de la dependencia o proceso, conforme con su finalidad, funcionalidad, pertinencia y temporalidad, así como las disposiciones de la SIC y la Procuraduría General de la Nación, en adelante (PGN).

11. Reportar conforme con el procedimiento establecido, ante la Oficina de Seguridad de la información, en su calidad de Oficial de Protección de Datos, 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 quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento.

12. 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.

13. Facilitar y apoyar el entrenamiento, las capacitaciones, sensibilizaciones y actividades que promuevan la cultura de protección de datos personales en la UAE-DIAN.

14. 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.

15. Verificar que se realice, conforme con los términos y procedimientos establecidos, la conservación, respaldo, pruebas de restauración y disposición final, o eliminación o borrado de las bases de datos de propiedad de la UAE-DIAN, las que se le han asignado por parte de terceros a la UAE-DIAN en calidad de responsable o encargada del tratamiento y las que la entidad ha dispuesto a un encargado o a un tercero (responsable), conforme con la finalidad para la que fueron creadas, transmitidas o transferidas, las tablas de retención documental (en adelante TRD) y los lineamientos dados por la Subdirección de Gestión de Recursos Físicos o la dependencia que haga sus veces en materia de gestión documental.

16. Implementar las medidas de control y monitoreo necesarias para que a las bases de datos propias y de terceros, que reposen en servidores propios de la UAE-DIAN, accedan únicamente las personas autorizadas. Realizar control y monitoreo sobre las cuentas

y los accesos autorizados a funcionarios y a Terceros y aplicar procedimientos oportunos de inactivación cuando dichas cuentas ya no estén en uso o hubieran sido autorizadas a exfuncionarios o a personas (funcionarios o terceros) que ya no deban tener acceso a esas bases. Verificar que las bases de datos se encuentren dispuestas en entornos físicos o digitales seguros y confiables, y que cumplan las políticas de seguridad de la información de la UAE-DIAN para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

17. Implementar las medidas de control y monitoreo necesarias para que a las bases de datos de terceros accedan únicamente los funcionarios autorizados. Realizar control y monitoreo sobre las cuentas y los accesos autorizados a funcionarios y aplicar procedimientos oportunos de inactivación de las cuentas que ya no estén en uso o de cuentas autorizadas a exfuncionarios o a funcionarios que ya no deban tener acceso a esas bases.

18. Prestar apoyo técnico, a solicitud de las dependencias responsables de las solicitudes de entrega, intercambio, transferencia o transmisión de la información, en el análisis de la justificación de uso y necesidad de la información planteada por el requirente de la información.

19. Implementar las formas y cláusulas contractuales, así como los protocolos establecidos, necesarios para que el uso, entrega, intercambio, transferencia y transmisión de la información, nacional e internacional, relacionados con protección de datos personales, se realice conforme con las normas que sobre el tema rigen la materia, los convenios o acuerdos o tratados o normas internacionales y las políticas de la entidad.

20. Asegurar la aplicación de normas y políticas de protección de datos personales en el uso de canales de servicio, redes sociales, medios de comunicación, sitios web, servicios en línea y demás medios de comunicación que operen con medios y cuentas oficiales de la DIAN.

21. Atender los requerimientos de la Oficina de Seguridad de la información, en su calidad de Oficial de Protección de Datos y de los respectivos entes de Control (SIC y PGN), relacionados con la

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

22. Contemplar el enfoque de privacidad por diseño y por defecto, 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.

23. Conservar las evidencias documentales de la 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 supresión o disposición final de los mismos.

24. 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, autorización por recolección de datos biométricos.

Artículo 4º. *Obligaciones específicas de las áreas frente al tratamiento y protección de datos personales*. En los términos y bajo las directrices, lineamientos, políticas y procedimientos emitidos por la entidad, en materia de protección de datos personales, será responsabilidad de las áreas, que se señalan a continuación o quienes hagan sus veces, conforme con sus funciones y competencias:

1. Oficina de Control Interno

a) 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.

2. Dirección de Gestión de Recursos y Administración Económica

a) Asignar los recursos financieros, de conformidad con la disponibilidad presupuestal, técnicos, físicos y de talento humano necesarios para la adopción e implementación del Programa Integral de Gestión de Datos Personales de la UAE-DIAN.

b) 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.

c) 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 datos sensibles y la de niños, niñas y adolescentes y conservar las evidencias correspondientes.

d) Dirigir acciones encaminadas a incluir en los planes periódicos de entrenamiento, inducción, reinducción, formación y capacitación, para los empleados de la entidad, programas, temas o módulos, generales o específicos, sobre protección de datos personales en la UAE-DIAN.

e) Establecer las políticas y normas de administración documental de la UAE-DIAN, en concordancia con las políticas de seguridad y privacidad de la información.

2.1. Subdirección de Gestión de Personal

a) Implementar 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, empleados y familiares, y especialmente los relacionados con datos sensibles y de niños, niñas y adolescentes, desde los procesos de reclutamiento y

selección hasta su retiro definitivo de la entidad o por el tiempo que disponga la TRD del área.

b) Emitir lineamientos y desarrollar acciones para que en los planes periódicos de entrenamiento, inducción, reinducción y capacitación se desarrollen cursos, programas, módulos, temas o cualquier otro tipo actividades de formación, generales o específicas) dirigidas a fortalecer la cultura por la protección de los datos personales en la entidad.

2.2. Subdirección de Gestión de Recursos Físicos

a) Emitir lineamientos y desarrollar 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 información personal por acceso a los edificios y áreas, mediante sistemas de videovigilancia, captura de datos biométricos, medidas de seguridad físicas, adecuación mobiliaria, entre otros.

b) Implementar las formas, cláusulas contractuales y demás mecanismos necesarios para que durante el proceso de contratación se dé cumplimiento a las disposiciones normativas de protección de datos personales.

c) Diseñar e implementar las políticas, directrices y acciones en materia de gestión documental, en concordancia con las políticas de protección de datos personales, que permitan asistir a las áreas frente al tratamiento, protección y disposición final de los datos personales en medios físicos y electrónicos.

2.3. Subdirección de Gestión de Control Disciplinario Interno

a) Promover acciones preventivas frente al uso adecuado de la información, especialmente la relacionada con protección de datos personales, Ley Hábeas Data y Ley de Transparencia.

b) Adelantar las acciones pertinentes frente al incumplimiento de las normas de protección de datos personales por parte de los servidores de la UAE-DIAN.

3. Dirección de Gestión Organizacional

a) 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.

b) 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.

c) Emitir directrices y lineamientos para que se adopten las disposiciones, 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.

d) 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.

e) Contemplar el principio de privacidad por diseño y por defecto en los servicios que requieran desarrollar e implementar las áreas, como son los de interoperabilidad, trámites y servicios de ciudadanía digital.

f) 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.

g) 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.

3.1. Subdirección de Gestión de Tecnologías de la Información y las Comunicaciones

a) 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.

b) 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.

c) 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.

d) 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; relacionados con protección de datos personales, se realice conforme con las normas que sobre el tema rigen la materia, los convenios, acuerdos o tratados internacionales, las disposiciones de la SIC, de la PGN y las políticas de la entidad.

e) 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.

f) 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.

g) 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.

3.2. Subdirección de Gestión de Procesos y Competencias Laborales

a) 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 UAE- DIAN.

b) Identificar en los documentos del Sistema de Gestión de Calidad, la clasificación de la información (pública, pública clasificada y pública reservada) así como la categoría de datos personales.

c) 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.

4. Dirección de Gestión de Ingresos

4.1. Subdirección de Gestión de Asistencia al Cliente

a) Adoptar en el canal presencial (Puntos de contacto y quioscos de autogestión), telefónico (Contact Center) y virtual (chat) y los que sean implementados y administrados por la Subdirección de Gestión de Asistencia al Cliente, 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 UAE-DIAN.

b) Gestionar, dentro de los términos establecidos por las normas sobre protección de datos y la política de tratamiento de datos personales de la UAE-DIAN, las PQSRD relacionadas con 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 entidad.

c) Incorporar en los diseños físicos, digitales y tecnológicos, asociados a nuevos canales, trámites, servicios o desarrollos que estén bajo la responsabilidad funcional de la Subdirección de Gestión de Asistencia al Cliente, para facilitar la interacción con el 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.

d) Asegurar la aplicación de normas y políticas de protección de datos personales en el uso de los canales habilitados a los ciudadanos que son administrados y están bajo la responsabilidad funcional de la Subdirección de Gestión de Asistencia al Cliente, así como en las actividades relacionadas con cultura de la contribución y el Registro Único Tributario RUT.

Parágrafo. Será de obligatorio cumplimiento para todas las áreas de la UAE-DIAN, la adopción y adecuación de las medidas y responsabilidades aquí dispuestas, en los planes, procesos, procedimientos, infraestructura, recursos físicos, humanos y tecnológicos de la entidad.

Artículo 5º. *Publicación*. Publicar la presente resolución, conforme lo ordenado por el artículo 65 del Código de Procedimiento Administrativo y de lo contencioso Administrativo.

Artículo 6º. La presente resolución rige a partir de la fecha de su publicación.

Publíquese y cúmplase.

Dada en Bogotá, D. C., a 9 de noviembre de 2020.

El Director General,

José Andrés Romero Tarazona.

Publicada en D.O. 51.494 del 10 de Noviembre de 2020.