Industria y Comercio
SUPERINTENDENCIA

Guía para la Implementación del Principio de Responsabilidad Demostrada (*Accountability*)

I INTRODUCCIÓN

II CONSIDERACIONES PRELIMINARES

A. ¿Qué es la Responsabilidad Demostrada o *Accountability*?

B. Beneficios para la organización

III FUNDAMENTOS BÁSICOS – DESARROLLO DE UN PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

1. *Compromiso de la organización*
   - 1.1 Desde la dirección
   - 1.2 Oficial de protección de datos
   - 1.3 Presentación de informes
2. *Controles del programa*
   - 2.1 Procedimientos operacionales
   - 2.2 Inventario de las bases de datos con información personal
   - 2.3 Políticas
   - 2.4 Sistema de administración de los riesgos asociados al tratamiento de datos personales
   - 2.5 Requisitos de formación y educación
   - 2.6 Protocolos de respuesta de violación y manejo de incidentes
   - 2.7 Gestión de los Encargados del Tratamiento en las transmisiones internacionales de datos personales
   - 2.8 Comunicación Externa

IV EVALUACIÓN Y REVISIÓN CONTINUA

A. Desarrollar un plan de supervisión y revisión

B. Evaluar y revisar los controles del programa

V DEMOSTRACIÓN DEL CUMPLIMIENTO

I INTRODUCCIÓN

El concepto de responsabilidad demostrada aplicada al tratamiento de datos personales tiene más de 30 años. Ya en 1980, las Guías para la protección de la privacidad y los flujos transfronterizos de datos personales[1] introdujeron el concepto, conocido en inglés como **accountability**, donde se enfatizaba el rol del Responsable del Tratamiento como el llamado a implementar medidas dentro de la organización que le permitieran cumplir con el resto de principios consagrados por dicho instrumento. Trabajando en esa línea, y reconociendo la importancia de un enfoque basado en el compromiso de la organización con incrementar sus estándares de protección para garantizarle a los ciudadanos un tratamiento idóneo de su información personal, algunas autoridades de protección de datos en el mundo han publicado guías que le permiten a las organizaciones cumplir con la ley e implementar ese alto estándar dentro de su gestión operativa.

Este documento responde al llamado de la industria que ha solicitado mayor orientación en el camino de construir un **Programa Integral de Gestión de Datos Personales**[2] [3] y se dirige a quienes estén sometidos al cumplimiento del régimen general de protección de datos personales y sean vigilados por la Superintendencia de Industria y Comercio.

1 OECD. ***Guidelines on the Protection of Privacy and Transborder Flows of Personal Data***, 1980.

2 El documento toma como base de partida el trabajo previo adelantado por la Oficina del Comisionado de Privacidad de Canadá, la Oficina del Comisionado de Privacidad e Información de Alberta y la Oficina del Comisionada de Privacidad e Información de Columbia Británica muchos de cuyos contenidos se han incorporado acá (ver: Oficina del Comisionado de Privacidad de Canadá, Oficina del Comisionado de Privacidad e Información de Alberta y Oficina del Comisionado de Privacidad e Información de Columbia Británica. ***Getting Accountability Right with a Privacy Management Program***. Disponible en: https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.pdf).

3 Las guías recogen también los esfuerzos del sector privado que desde hace varios años han venido investigando y publicando materiales sobre los elementos esenciales para la implementación del principio de responsabilidad demostrada en las organizaciones (ver CENTRE FOR INFORMATION POLICY LEADERSHIP (Secretariat). ***The Accountability Project y The Essential Elements of Accountability***. 2009 y NYMITY. ***A privacy office guide to demonstrating accountability y Nymity Privacy Management Accountability Framework***. Toronto, Canadá. 2014).

II CONSIDERACIONES PRELIMINARES

A. ¿Qué es la Responsabilidad Demostrada o *Accountability*?

En septiembre de 2013 la OCDE publicó la versión revisada de las Guías sobre Protección de la Privacidad y los Flujos Transfronterizos de Información que originalmente habían sido publicadas en 1980. Las guías de la OCDE recogen un principio fundamental conocido como responsabilidad demostrada (*accountability* en inglés), según el cual una entidad que recoge y hace tratamiento de datos personales debe ser responsable del cumplimiento efectivo de las medidas que implementen los principios de privacidad y protección de datos[4] .

La versión de 2013 de las guías, que en lo sustancial no hizo cambios a los principios que allí se habían incluido desde 1980, sí estableció un nuevo aparte sobre implementación del principio de responsabilidad demostrada. En ese sentido, y según lo dispuesto por las guías, 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 uno de los apartes más relevantes del Decreto 1377 de 2013, en el artículo 26, el regulador introdujo en el sistema colombiano de protección de datos el criterio de la responsabilidad demostrada como una obligación en cabeza de los Responsables del Tratamiento. Igualmente, dispuso que los Responsables 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.

4 Múltiples instrumentos nacionales e internacionales han incluido el concepto de responsabilidad demostrada. Ver entre otros: Ley de Protección de la Información Personal y Documentos Electrónicos de Canadá (***Personal Information Protection and Electronic Documents Act – PIPEDA***), Directiva 95/46/CE, Reglas de Privacidad Transfronterizas (***Cross Border Privacy Rules - CBPR***) de APEC, procedimiento de ***"Puerto Seguro"*** o ***"Safe Harbor"*** acordado entre los Estados Unidos y la Unión Europea y Estándares de Madrid de 2009.

II CONSIDERACIONES PRELIMINARES

Quizá uno de los contenidos más novedosos de la norma reglamentaria, es la estipulación según la cual la Superintendencia de Industria y Comercio, en su calidad de autoridad nacional de protección de datos, debe tener en cuenta la existencia de medidas y políticas adecuadas en el momento de evaluar la imposición de una sanción.

La norma establece de manera específica que estas medidas se deben adoptar teniendo en cuenta diversos factores que son propios de cada organización entre los que se encuentran su tamaño y naturaleza jurídica, la naturaleza de los datos tratados, el tipo de tratamiento al que se someta la información y los riesgos que implique para los titulares la recolección y posterior uso o circulación de esos datos.

Así mismo, el artículo 27 del Decreto 1377 de 2013 dispuso que las políticas internas efectivas que se implementen deberán garantizar (i) que en la organización exista una estructura administrativa proporcional a la estructura del responsable para implementarlas, (ii) que se adopten 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.

Tal y como sucede con el modelo recogido en el decreto, y en los mismos términos en que la Superintendencia de Industria y Comercio ha venido diseñando su sistema de supervisión[5], el énfasis de la comunidad dedicada a la protección de la información personal tiende a volcarse hacia un modelo que privilegia la gestión del riesgo y la asignación de responsabilidades en cabeza del Responsable del Tratamiento.

5 El Sistema Integral de Supervisión Inteligente que estará ligado al Registro Nacional de Bases de Datos.

II CONSIDERACIONES PRELIMINARES

B. Beneficios que representa la implementación de la Responsabilidad Demostrada frente al Tratamiento de Datos Personales

La apuesta que hace una organización por implementar estándares elevados de protección de datos personales en su organización, y desarrollar un Programa Integral de Gestión de Datos Personales, genera beneficios para la organización y se traduce en una mayor protección de los individuos.

De manera muy novedosa, y como reconocimiento a aquellas organizaciones que se comprometen de manera decidida por la protección de la información personal que recolectan, el inciso final del artículo 27 del Decreto 1377 de 2013 prevé expresamente que la "verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente decreto".

Esta disposición es especialmente relevante porque implica el reconocimiento expreso que debe hacer la autoridad de vigilancia frente a organizaciones que estén en capacidad de demostrarle que una eventual falla en el tratamiento de la información de un titular corresponde a una situación aislada dentro de un Programa Integral de Gestión de Datos Personales. Teniendo en cuenta que los recursos de vigilancia de la autoridad de protección de datos personales son limitados, su práctica supervisora debe enfocarse hacia aquellas entidades subestándar, con mayores niveles de riesgo, donde el tratamiento de la información genera un riesgo sistémico con la potencialidad de afectar de manera grave a los titulares. La verificación de la implementación de un programa que involucre los

II CONSIDERACIONES PRELIMINARES

elementos esenciales de la responsabilidad demostrada genera una situación de beneficio mutuo entre organizaciones y autoridad de supervisión. Esto por supuesto no implica que la autoridad de vigilancia renuncie a su capacidad investigativa, pero sí determina la manera en que se evalúa una infracción según la entidad sujeta a escrutinio, lo cual solamente podrá determinarse caso a caso.

III FUNDAMENTOS BÁSICOS

DESARROLLO DE UN PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

El ordenamiento jurídico colombiano exige que los sujetos obligados adopten políticas internas efectivas, por disposición expresa del artículo 27 del Decreto 1377 de 2013. Estas políticas internas efectivas no pueden limitarse a reproducir los textos legales ni son meras declaraciones de principios. Por el contrario, la adopción de políticas internas efectivas parte del desarrollo de un Programa Integral de Gestión de Datos Personales, que debe ser el resultado de un proceso de debida diligencia al interior de la organización que permita formularlo. Un programa efectivo de protección de datos debe incorporar políticas que (**I**) respondan a los ciclos internos de gestión de datos de la organización y (**II**) generen resultados medibles que le permitan probar ese grado de diligencia especial.

III FUNDAMENTOS BÁSICOS
DESARROLLO DE UN PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

De manera concreta, el artículo 27 del Decreto 1377 de 2013 exige que esas políticas garanticen:

(I) La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del Responsable para la adopción e implementación de políticas consistentes con la ley.

(II) La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación, y

(III) La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del Tratamiento.

En las secciones siguientes se desarrollan algunos de los elementos esenciales que deben ser incorporados a la organización para el desarrollo, implementación y seguimiento de un **Programa Integral de Gestión de Datos Personales**.

1. COMPROMISO DE LA ORGANIZACIÓN

Para que una organización efectivamente implemente un **Programa Integral de Gestión de Datos Personales**, no es suficiente demostrar la adopción de políticas y procedimientos tendientes a cumplir las normas sobre protección de datos personales. Un programa basado en este estándar debe buscar la implementación de esas políticas y procedimientos, para lo cual, como primera medida, se requiere contar con el compromiso de los sujetos obligados, derivado de una cultura de respeto a la protección de los datos personales que recoge o trata. En este sentido, la organización, atendiendo a su tamaño y estructura, así como al tipo de información personal a la que le realiza tratamiento, debe comprometer recursos económicos y de personal una vez que decide emprender el camino hacia la implementación de un **Programa Integral de Gestión de Datos Personales**.

III FUNDAMENTOS BÁSICOS
DESARROLLO DE UN PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

1.1 DESDE LA ALTA DIRECCIÓN

El primer paso que debe dar una organización para implementar prácticas responsables de protección de datos es lograr que ese compromiso provenga de la alta dirección y/o la gerencia. El apoyo y compromiso de la alta dirección es fundamental para generar una cultura organizacional de respeto a la protección de los datos personales y es un paso que asegura que el programa de gestión de datos personales se implemente exitosamente en todas las áreas.

Para lograr estos objetivos, la alta dirección debe (i) designar a la persona o al área que asumirá la función de protección de datos dentro de la organización, (ii) aprobar y monitorear el Programa Integral de Gestión de Datos Personales, y (iii) informar de manera periódica a los órganos directivos sobre su ejecución. Desde la Dirección también deben destinarse recursos suficientes que le permitan, al área o persona encargada, diseñar e implementar un programa que se ajuste a la realidad de la organización. Por último, y a través de esa persona o área, se deberán establecer responsabilidades específicas para otras áreas de la organización respecto de la recolección, almacenamiento, uso, circulación y eliminación o disposición final de los datos personales que se tratan.

1.2 OFICIAL DE PROTECCIÓN DE DATOS

Como prevé el artículo 23 del Decreto 1377 de 2013, todo Responsable y Encargado debe designar a una persona o área que "asuma la función de protección de datos personales" y 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 decreto".

La función del oficial de protección de datos o del área encargada de protección de datos en la organización es la de velar por la implementación efectiva de las políticas y procedimientos adoptados por ésta para cumplir las normas, así como la

III FUNDAMENTOS BÁSICOS
DESARROLLO DE UN PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

implementación de buenas prácticas de gestión de datos personales dentro de la empresa. El oficial de privacidad tendrá la labor de estructurar, diseñar y administrar el programa que permita a la organización cumplir las normas sobre protección de datos personales, así como establecer los controles de ese programa, su evaluación y revisión permanente. Dentro de sus actividades se encuentran entre otras las siguientes[6] :

- Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales.
- Coordinar la definición e implementación de los controles del Programa Integral de Gestión de Datos Personales.
- Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales.
- Impulsar una cultura de protección de datos dentro de la organización.
- Mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo.
- Registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la SIC.
- Obtener las declaraciones de conformidad de la SIC cuando sea requerido.
- Revisar los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con Encargados no residentes en Colombia.

6 Las actividades específicas del Oficial de Privacidad según se describen en: NYMITY. ***A privacy office guide to demonstrating accountability.*** Toronto, Canadá. 2014. p. 66.

III FUNDAMENTOS BÁSICOS

DESARROLLO DE UN PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

• Analizar las responsabilidades de cada cargo de la organización, para diseñar un programa de entrenamiento en protección de datos personales específico para cada uno de ellos

• Realizar un entrenamiento general en protección de datos personales para todos los empleados de la compañía.

• Realizar el entrenamiento necesario a los nuevos empleados, que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización.

• Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización (talento humano, seguridad, call centers y gestión de proveedores, etc.).

• Medir la participación, y calificar el desempeño, en los entrenamientos de protección de datos.

• Requerir que dentro de los análisis de desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre protección de datos personales.

• Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de sus políticas de tratamiento de la información personal.

• Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la Superintendencia de Industria y Comercio.

• Realizar seguimiento al Programa Integral de Gestión de Datos Personales.

III FUNDAMENTOS BÁSICOS
DESARROLLO DE UN PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

1.3 PRESENTACIÓN DE INFORMES

Los sujetos obligados deben establecer mecanismos de información internos para reportar dentro de la organización acerca del seguimiento y la ejecución del Programa. Igualmente, deben implementar planes de auditoría interna para verificar el cumplimiento de sus políticas de tratamiento de datos personales y señalar el procedimiento a seguir en caso de que se presenten violaciones a sus códigos de seguridad o detecten riesgos en la administración de la información de los Titulares.

La producción del material que sustente la implementación de un **Programa Integral de Gestión de Datos Personales** en la compañía, debe incluirse dentro de la información que es enviada a los accionistas o socios, con el fin de mantenerlos plenamente informados. Se resaltan en este punto los siguientes elementos clave sobre presentación de informes internos[7]:

(I) Definir de manera clara la estructura de la generación de reportes. Esto implica saber qué empleado genera qué tipo de reporte, para asignar responsabilidades claras en el evento de una queja o de una violación a los códigos de seguridad.

(II) Documentar el proceso de generación de reportes como parte del Programa Integral de Gestión de Datos Personales.

(III) Generar reportes para los accionistas o socios de manera periódica, e informar en estos el estado del programa de protección de datos personales.

2. CONTROLES DEL PROGRAMA

Un segundo paso que deben dar las organizaciones una vez han adelantado el proceso de debida diligencia interna que les ha servido para comprometerse con la implementación de un esquema basado en estándares de responsabilidad

7 Ver. ***Getting accountability right with a privacy management program*** (https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.pdf) Pp. 8 y 9. y NYMITY: A privacy office guide to demonstrating accountability. Toronto, Canadá. 2014.

III FUNDAMENTOS BÁSICOS
DESARROLLO DE UN PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

demostrada, es el desarrollo y puesta en marcha de controles que le permitirán al oficial de protección de datos o al área encargada desarrollar un **Programa Integral de Gestión de Datos Personales**. Los controles ayudan a asegurar que las políticas adoptadas se implementen al interior de cada sujeto obligado.

2.1 PROCEDIMIENTOS OPERACIONALES

La empresa que aspire a implementar un programa basado en esquemas de responsabilidad demostrada, debe desarrollar e implementar procedimientos administrativos consistentes con las políticas generales de protección de datos y con las disposiciones legales vigentes de forma que pueda manejar adecuadamente los riesgos inherentes al tratamiento de información personal dentro de las actividades de gestión operacional[8].

2.2 INVENTARIO DE LAS BASES DE DATOS CON INFORMACIÓN PERSONAL

Los sujetos obligados deben conocer qué datos personales almacenan, cómo los utilizan y si realmente los necesitan, teniendo en cuenta la finalidad para la cual los recolectan.

Es importante que identifiquen en qué parte del procedimiento o actividad se obtienen los datos, si deben solicitar la autorización del Titular y, de ser así, si están conservando prueba de la misma para su posterior consulta.

En los casos en los que recolecten datos personales sensibles o datos de niños, niñas y adolescentes, es necesario (i) implementar las medidas adecuadas para garantizar una protección reforzada de dicha información y (ii) asegurarse de que se esté informando al titular o a quien corresponda (cuando se trate de datos de menores) que no existe obligación de suministrar tales datos. Es importante tener en cuenta

8 Ver por ejemplo los procedimientos y actividades específicas que pueden ser incoporados al Programa Integral de Gestión de Datos Personales en el Privacy Management Accountability Framework incluido en NYMITY, ***A privacy office guide to demonstrating accountability***. Toronto, Canadá. 2014. P. 65

III FUNDAMENTOS BÁSICOS
DESARROLLO DE UN PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

que una clasificación de la información recopilada por la compañía, como por ejemplo, en sensible, confidencial y pública, según el caso, ayuda a tener un inventario efectivo de los datos tratados por la empresa.

2.3 POLÍTICAS

Los sujetos obligados deben generar políticas internas que dispongan obligaciones en virtud de la ley y dárselas a conocer a los empleados.

Estas políticas deben implementar los principios que rigen el Tratamiento de datos personales (artículo 4 Ley 1581 de 2012) y estar documentadas. Igualmente, se deben documentar los procedimientos para la recolección o recopilación, el mantenimiento, uso y eliminación o disposición final de los datos personales (artículo 11 del Decreto 1377 de 2013).

En particular, la empresa debe incorporar políticas de tratamiento de la información, de obligatorio cumplimiento, que establezcan reglas sobre los siguientes puntos, entre otros:

- La recolección, almacenamiento, uso, circulación y supresión o disposición final de la información personal, incluyendo los requisitos para obtener la autorización de los Titulares.
- El acceso y corrección de datos personales.
- La conservación y eliminación de información personal.
- El uso responsable de la información, incluyendo controles de seguridad administrativos, físicos y tecnológicos.
- Inclusión en todos los medios contractuales de la empresa de una cláusula de confidencialidad y de manejo de información, donde se afirme que se conoce a suficiencia la política de la empresa, se acepta, y se permite a la compañía utilizar dicha información de forma responsable.
- Presentación de quejas, denuncias y reclamos.

III FUNDAMENTOS BÁSICOS
DESARROLLO DE UN PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

Los sujetos obligados deben igualmente incluir en otras políticas de la organización (vgr. talento humano, contratos, transparencia, etc.) elementos que permitan cumplir las normas sobre protección de datos personales.

2.4 SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES

Un aspecto fundamental que deben tener en cuenta las organizaciones está relacionado con la identificación y manejo de los riesgos asociados al tratamiento de datos personales. Por ello, es importante que desarrollen un sistema de administración de riesgos, acorde con su estructura organizacional, sus procesos y procedimientos internos asociados al tratamiento de datos personales, la cantidad de base datos y tipos de datos personales tratados por la empresa. Este sistema le permitirá a la empresa identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales.

El sistema de administración de riesgos que adopte la empresa debe tener en cuenta las siguientes etapas:

III FUNDAMENTOS BÁSICOS
DESARROLLO DE UN PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

2.4.1 Identificación

La identificación consiste en establecer los riesgos a que se ven expuestos los datos personales en desarrollo de su tratamiento. Para realizar dicha identificación es necesario: (I) documentar los procesos y procedimientos que se implementen dentro del ciclo de vida de los datos personales[9], (II) definir la metodología de identificación de los riesgos asociados al tratamiento de información personal y (III) identificar los riesgos e incidentes ocurridos, respecto de este tipo de información, en los casos que aplique.

2.4.2 Medición

La medición tiene por objeto determinar la posibilidad de ocurrencia de los riesgos relacionados con el tratamiento de datos personales y su impacto en caso de materializarse.

2.4.3 Control

El control se relaciona con las acciones que se deben tomar para controlar y/o mitigar los riesgos a que se ven expuestos los datos personales, con el fin de disminuir la posibilidad y/o las consecuencias de la materialización de los mismos. Para analizar los controles es preciso establecer, al menos, si son suficientes, efectivos y oportunos, como también identificar el tipo de control, esto es, si son manuales, automáticos, discrecionales, obligatorios, preventivos, o correctivos.

2.4.4 Monitoreo

El monitoreo consiste en realizar un seguimiento constante para velar porque las medidas que se hayan establecido sean efectivas.

9 Hace referencia a reconocer cómo se produce el flujo de información en los procesos de gestión en los que se realice tratamiento de la información personal, es decir, poder identificar el tratamiento de datos personales realizado en cada uno de tales procesos (recolección, mantenimiento y uso, supresión y disposición final de los datos personales) con el objeto de adoptar las medidas técnicas, físicas, jurídicas, organizativas y de seguridad que demanda una gestión eficaz orientada a la protección de los datos personales.

III FUNDAMENTOS BÁSICOS
DESARROLLO DE UN PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

Para el efecto, es importante llevar a cabo las siguientes acciones:

(I) Contemplar un proceso de seguimiento efectivo que facilite la rápida detección y corrección de las deficiencias en la administración de los riesgos identificados.

(II) Establecer indicadores que evidencien la efectividad del sistema de administración de riesgos adoptado.

(III) Asegurar que los controles estén funcionando en forma oportuna, efectiva y eficiente.

(IV) Asegurar que los riesgos residuales se encuentren en los niveles de aceptación establecidos.

(V) Llevar un registro de incidentes que contemple: Base de datos y datos comprometidos, titulares, fecha del incidente y de descubrimiento, acciones correctivas realizadas y responsables.

Los sujetos obligados deben evaluar sus riesgos periódicamente e implementar estas evaluaciones en toda la organización dentro de cada nuevo proyecto que involucre datos personales

Es necesario desarrollar procedimientos para efectuar dichas evaluaciones y tener un proceso de revisión y aprobación que involucre tratamiento a la persona o área que tiene a cargo la función de protección de datos personales en el diseño de nuevas iniciativas, servicios o programas.

2.5 REQUISITOS DE FORMACIÓN Y EDUCACIÓN

Un componente fundamental para implementar un Programa Integral de Gestión de Datos Personales está en la formación y educación de todos los empleados de la organización. Serán en vano los esfuerzos de una empresa que, habiendo diseñado

III FUNDAMENTOS BÁSICOS
DESARROLLO DE UN PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

unas políticas robustas de protección de datos desde la alta gerencia, falle en su deber de capacitar al personal que, en el día a día, trata datos personales como parte de sus funciones.

Las organizaciones deben impartir una formación de carácter general sobre la materia y, para el personal que maneje datos personales directamente, deberá existir una capacitación complementaria, adaptada específicamente a sus funciones. Esta formación y educación debe ser permanente, por ello es importante que exista una actualización periódica del contenido del programa.

Dentro de los contratos que suscriban los empleados, es importante incluir acuerdos de cumplimiento de las políticas internas adoptadas por los sujetos obligados.

2.6 PROTOCOLOS DE RESPUESTA EN EL MANEJO DE VIOLACIONES E INCIDENTES

Las violaciones a los códigos de seguridad de las organizaciones generan un altísimo riesgo para los titulares de la información y son causantes en muchos casos de impactos muy significativos a la reputación corporativa. Por lo anterior, un Programa Integral de Gestión de Datos Personales debe involucrar un componente de gestión de riesgos, internos y externos, que le permita identificar sus vulnerabilidades a tiempo y enfocar sus recursos a la adopción de medidas de mitigación de riesgo que minimicen dicho impacto tanto para la organización como para los titulares de información.

Dentro de esa gestión, es necesario que los sujetos obligados cuenten con un procedimiento y una persona o área responsable de manejar los incidentes o vulneraciones a los sistemas de información donde se gestionan datos personales y a los archivos físicos. Así mismo, es preciso que prevean los mecanismos para rendir informes internos y reportar los incidentes a los Titulares y a esta Superintendencia. De igual manera, es importante que las organizaciones implementen mecanismos

que les permitan comunicarse de manera eficiente con los Titulares afectados para (I) informarles sobre el incidente de seguridad relacionado con sus datos personales y las posibles consecuencias y (II) proporcionar herramientas a dichos Titulares afectados para minimizar el daño potencial o causado.

Los incidentes se refieren a cualquier evento en los sistemas de información o bases de datos manuales o sistematizadas, que atente contra la seguridad de los datos personales en ellos almacenados. La Ley 1581 de 2012 no hace distinción alguna respecto de los incidentes que deben ser reportados a la Superintendencia, por lo que, independientemente de su impacto, deben reportarse a esta entidad todos los incidentes ocurridos. Cómo mínimo, debe informarse el tipo de incidente, la fecha en que ocurrió y la fecha en la que se tuvo conocimiento del mismo, la causal, el tipo de datos personales comprometidos y la cantidad de titulares afectados.

2.7 GESTIÓN DE LOS ENCARGADOS DEL TRATAMIENTO EN LAS TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES

Los sujetos obligados deben tomar las medidas necesarias para asegurar la protección de los datos personales cuyo Tratamiento es realizado por Encargados a través de transmisiones internacionales de datos personales.

Para ello, se deben tener en cuenta, entre otros, los siguientes aspectos:

(I) Disposiciones que incluyan requisitos para que los Encargados cumplan con las normas colombianas de protección de datos, en general, y las políticas de tratamiento del Responsable, en particular. De la misma manera, considerar mecanismos para que el Encargado reporte al Responsable los incidentes de seguridad de la información.

(II) Formación y educación en temas de protección de datos personales para los empleados del Encargado que tienen acceso a la información personal.

III FUNDAMENTOS BÁSICOS
DESARROLLO DE UN PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

(III) Exigencia de adherencia a las políticas de tratamiento si se utilizan subcontratistas.

(IV) Realización de auditorías internas y/o externas.

(V) Acuerdos con los Encargados y sus empleados aceptando que cumplirán con las políticas y protocolos del Responsable del Tratamiento.

2.8 COMUNICACIÓN EXTERNA

Los sujetos obligados deben desarrollar un procedimiento para informar a los Titulares sus derechos, de acuerdo con lo establecido en el artículo 11 de la Ley 1581 de 2012, así como los programas de control que han implementado. Las comunicaciones dirigidas a los Titulares deben ser claras y comprensibles y no limitarse a una simple reiteración de la ley.

El objetivo que deben alcanzar es dar a conocer a los Titulares que tienen derecho a acceder a sus datos personales, actualizarlos, corregirlos y eliminarlos y revocar la autorización que hayan otorgado, cuando no exista un deber legal o contractual de permanecer en la base de datos, e informarles acerca de los mecanismos que han puesto a su disposición para ejercer esos derechos.

IV EVALUACIÓN Y REVISIÓN CONTINUA

Es muy importante desarrollar un **Programa Integral de Gestión de Datos Personales**, pero igual de importante es mantener ese programa para garantizar su eficacia permanente, el cumplimiento y la adherencia a estándares de Responsabilidad Demostrada. Los sujetos obligados deben supervisar, evaluar y revisar su programa para asegurar que siga siendo pertinente y eficaz. Se deben asignar los recursos necesarios para ello y el entrenamiento requerido a cargo de la persona o área que tiene la función de protección de datos personales.

A. Desarrollar un Plan de Supervisión y Revisión

El Oficial de Protección de Datos debe desarrollar un plan de supervisión y revisión anual. El plan debe establecer las medidas de desempeño e incluir un calendario de cuándo deben ser revisadas las políticas y los controles del programa, por lo menos una vez al año.

B. Evaluar y Revisar los Controles del Programa

El monitoreo es un proceso continuo que debe abordar, por lo menos, las siguientes preguntas:

- ¿Cuáles son las últimas amenazas y riesgos al tratamiento de datos personales detectados en la organización?
- ¿Los controles del programa están teniendo en cuenta las nuevas amenazas y reflejando las quejas más recientes o los hallazgos de las auditorías, o las orientaciones de la autoridad de protección de datos?
- ¿Se están ofreciendo nuevos servicios que involucran una mayor recolección, uso o divulgación de la información personal?
- ¿Se está llevando a cabo capacitación eficaz, se están siguiendo las políticas y procedimientos, y el programa se encuentra actualizado?

IV EVALUACIÓN Y REVISIÓN CONTINUA

Con base en los resultados del proceso de evaluación, el Oficial de Protección de Datos debe considerar si se deben tomar medidas para actualizar y revisar los controles del programa y los cambios deben ser comunicados a los empleados.

En general, el Oficial de Protección de Datos debe llevar a cabo las siguientes acciones:

- Controlar y actualizar el inventario de información personal continuamente para identificar y evaluar nuevas recolecciones, usos y divulgaciones.
- Revisar las políticas siguiendo los resultados de las evaluaciones o auditorías.
- Mantener como documentos históricos las evaluaciones de impacto y las de amenazas a la seguridad y riesgos.
- Revisar y actualizar, en forma periódica, la formación y la educación impartida a todos los empleados de la organización, como resultado de evaluaciones continuas y comunicar los cambios realizados a los controles del programa.
- Revisar y adaptar los protocolos de respuesta en el manejo de violaciones e incidentes de seguridad para implementar las mejores prácticas o recomendaciones y lecciones aprendidas de revisiones posteriores a esos incidentes.
- Revisar y, en su caso, modificar los requisitos establecidos en los contratos suscritos con los Encargados del Tratamiento.
- Actualizar y aclarar las comunicaciones externas para explicar las políticas de tratamiento de datos.
- Reportar semestralmente al representante legal de la empresa la evolución del riesgo, los controles implementados, el monitoreo y, en general, los avances y resultados del programa.

V DEMOSTRAR EL CUMPLIMIENTO

La implementación de las medidas citadas en esta guía, acorde con lo establecido en la Ley 1581 de 2012 y el Decreto 1377 de 2013, permitirá a los sujetos obligados acreditar ante los Titulares y esta Superintendencia que han adoptado un P**rograma Integral de Gestión de Datos Personales**, tendiente a cumplir las normas vigentes. De esta forma, también podrán acreditar la debida diligencia en el Tratamiento de datos personales, de manera que éste sea un factor a tener en cuenta en caso de que la autoridad adelante una actuación administrativa.

Sin embargo, para que la **SIC** pueda tener en cuenta la existencia e implementación de ese Programa y esas políticas en el momento de evaluar la imposición de una sanción, la organización debe estar en capacidad de probar dicha implementación. Ese elemento, incluido en la parte inicial del artículo 26 del Decreto 1377 de 2013, es esencial para asegurar el éxito de un **Programa Integral de Gestión de Datos Personales**.

Aunque la demostración de la implementación del programa es esencial de cara a la determinación de las medidas de supervisión que adelanta la SIC, la demostración no sólo se ejerce frente a la autoridad. De manera igualmente importante, un programa bien estructurado le permitirá a la organización ser transparente con los Titulares cuya información ha recogido, generando así confianza en el mercado.

Industria y Comercio
SUPERINTENDENCIA

Bogotá, D.C.
Carrera 13 N° 27-00
Edificio Bochica

Conmutador:(571) 5 870 000 Ext. 30022
Contact Center: (571) 5 920 400 - Bogotá
Línea Gratuita Nacional: 01 8000 - 910165

www.sic.gov.co @sicsuper Superintendencia de Industria y Comercio

MINCOMERCIO
INDUSTRIA Y TURISMO

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN