COLOMBIA POTENCIA DE LA VIDA

Industria y Comercio
SUPERINTENDENCIA

GUÍA OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

DELEGATURA PARA LA PROTECCIÓN DE DATOS PERSONALES

Superintendencia de Industria y Comercio

CONTENIDO

INTRODUCCIÓN

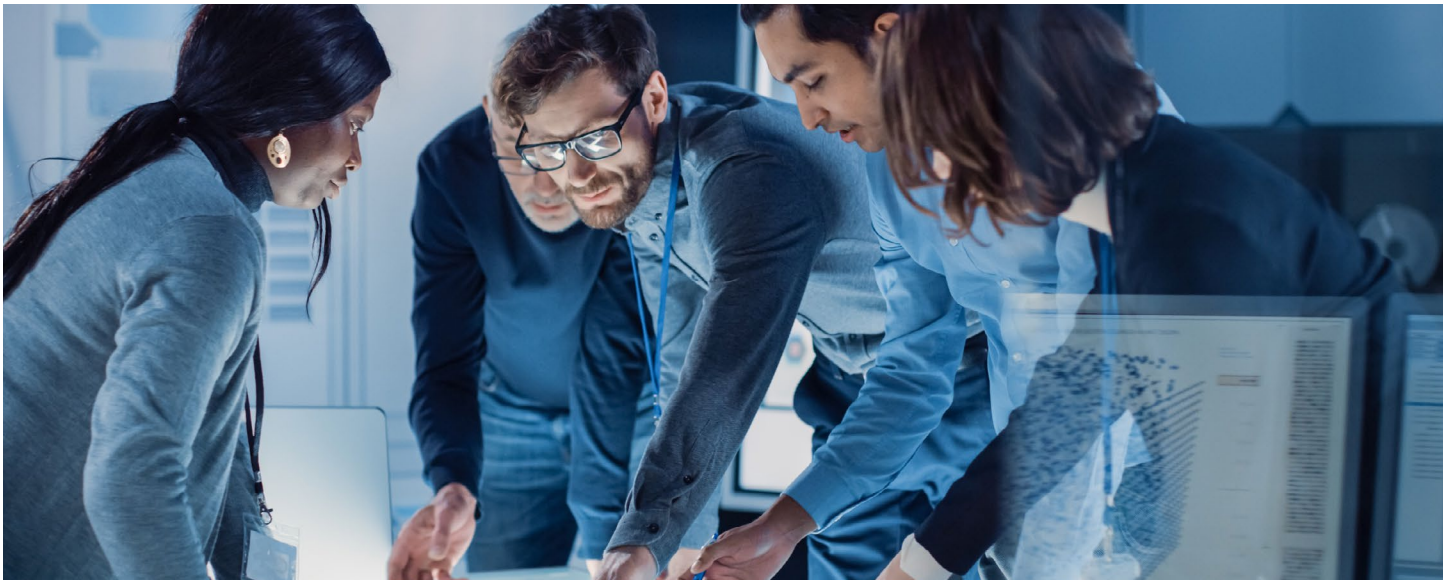
El Régimen General de Protección de Datos Personales –Ley Estatutaria 1581 de 2012 y sus decretos reglamentarios– así como la normativa sectorial en la materia –Ley Estatutaria 1266 de 2008 y sus decretos reglamentarios-, proporcionan un marco basado en la rendición de cuentas para la protección de los Datos Personales en la República de Colombia.

Precisamente, la regulación les exige a los sujetos obligados ser capaces de demostrar que han implementado medidas apropiadas, efectivas y verificables para cumplir con las obligaciones establecidas en la normativa. Bajo aquel entendido, la Superintendencia de Industria y Comercio publicó el 28 de mayo del 2015 la **"Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability)"[1].**

De acuerdo con el artículo 2.2.2.25.4.4. del Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, todo Responsable y Encargado del Tratamiento está en el deber de "(...) 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 decreto"[2]. De lo anterior, se evidencia la necesidad de contar con una persona Responsable de dar respuesta a las consultas y reclamos presentados por los titulares de la información. Sin embargo, la figura del Oficial de Protección de Datos Personales no existe en nuestra legislación.

Con esto presente, a través de esta Guía se pone en consideración de los Responsables y Encargados del tratamiento de datos personales, algunas recomendaciones relevantes que pueden ser útiles para efectos del nombramiento y definición de funciones de un Oficial de Protección de Datos Personales, como mecanismo idóneo que ayudara al cumplimiento del Principio de Responsabilidad Demostrada.

1 Ver documento completo en: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf
2 Artículo 26 del Decreto 1377 de 2013 (Incorporado en el Decreto Reglamentario 1074 de 2015).



OBJETIVOS Y PRECISIONES

Esta guía[3] tiene como propósito presentar algunas sugerencias a las organizaciones que pretendan designar un Oficial de Protección de Datos Personales (en adelante OPD), con el fin de orientarlos para que implementen medidas de Responsabilidad Demostrada con miras a dar cumplimiento a la regulación colombiana.

Este documento no es un concepto legal, ni constituye asesoría jurídica. Tampoco pretende ser un listado exhaustivo de recomendaciones específicas sobre todos los temas que involucran el nombramiento y las funciones de un OPD, pues ello es un asunto interno que define cada organización a la luz de sus particularidades.

Las orientaciones contenidas en este texto solo comprenden algunos de los temas más relevantes sobre el nombramiento y las funciones de un OPD. Por consiguiente, el lector debe tener claro que este documento no incluye todos los deberes legales sobre la materia y que la omisión de algunos de ellos en esta guía no lo exime de cumplir todos los requerimientos legales.

SOBRE EL OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

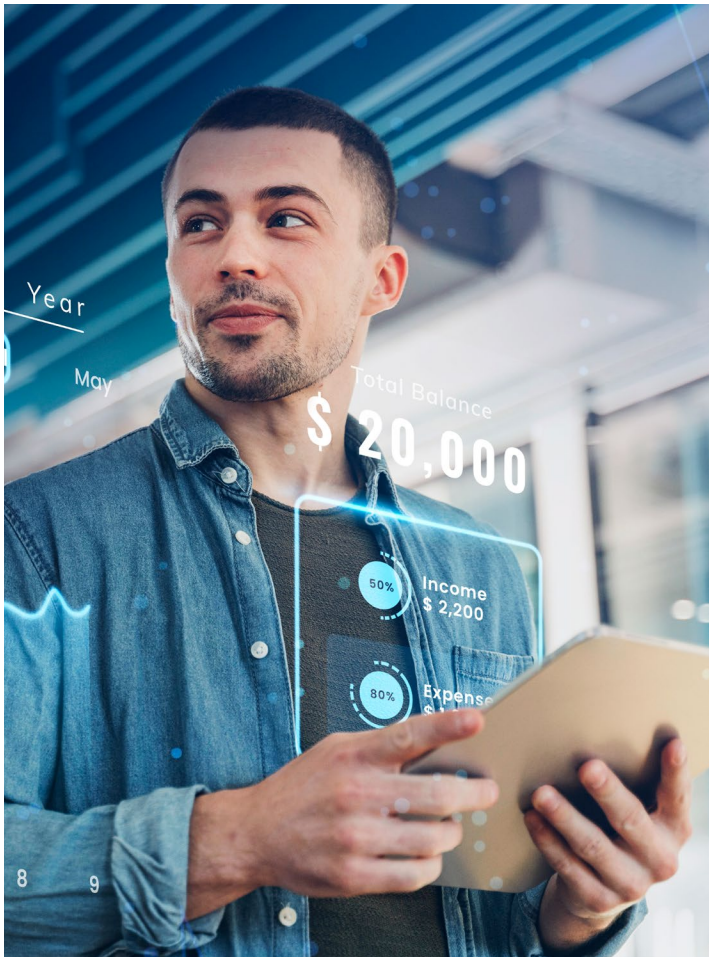
La Superintendencia de Industria y Comercio –Autoridad Nacional de Protección de Datos Personales– reconoce que el concepto de OPD no es nuevo. Por el contrario, tanto en el Derecho Comparado[4] como en la práctica se ha desarrollado en las últimas décadas el nombramiento y las funciones que le asisten a un OPD.

Por ejemplo, en la Unión Europea, el Grupo de Trabajo del Artículo 29 argumentó que el OPD es la piedra angular de la rendición de cuentas y que el nombramiento de un OPD puede facilitar el cumplimiento y, además, convertirse en una ventaja competitiva para las empresas[5]. Además de facilitar el cumplimiento mediante la aplicación de instrumentos de Responsabilidad Demostrada (tales como facilitar o llevar a cabo evaluaciones de impacto y auditorías de protección de datos), los OPD actúan como intermediarios entre las partes interesadas correspondientes (p. ej. la autoridad, los titulares y las unidades de negocio dentro de una organización).

3 Para la elaboración de esta guía se siguió el formato y se usaron los contenidos de las "Directrices sobre los delegados de protección de datos (DPD)" elaborado Grupo de Trabajo sobre Protección de Datos del Artículo 29.

4 Algunas regulaciones de otros Estados ya exigen el Oficial de Protección de Datos. Lo anterior, por ejemplo, es el caso de el Reglamento (UE) 2016/679del Parlamento Europeo y del Consejo o la Ley de Protección de Datos de Brasil (LGPD).

5 Véase http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf



Empero, los OPD no responden en caso de incumplimiento del Régimen de Protección de Datos Personales de Colombia. Son los Responsables y Encargados del Tratamiento quienes están obligados a garantizar y ser capaces de demostrar que el Tratamiento se realiza de conformidad con la regulación nacional. Es decir, el cumplimiento de las normas sobre protección de datos es responsabilidad del Responsable y del Encargado del Tratamiento.

La función del OPD en la organización es la de velar por la implementación efectiva de las políticas y procedimientos adoptados por ésta para cumplir el Régimen de Protección de Datos Personales de Colombia. Adicionalmente, es la de velar por la implementación de buenas prácticas de gestión de datos personales dentro de la empresa.

De esta manera, el OPD tendrá a su cargo la función 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.

RECOMENDACIONES SOBRE LA DESIGNACIÓN DE UN OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

La organización –el Responsable o el Encargado del Tratamiento– tiene un papel fundamental a la hora de posibilitar el desempeño efectivo de las labores asignadas al OPD. El nombramiento de un OPD es un primer paso, pero se recomienda que el OPD cuente además con la autonomía y los recursos suficientes para desarrollar su labor de forma efectiva y eficiente.

De esta manera, la Superintendencia de Industria y Comercio en su rol de Autoridad Nacional de Protección de Datos se permite realizar las siguientes recomendaciones.

La designación de un Oficial de Protección de Datos Personales por parte del Responsable del Tratamiento no implica que el Encargado del Tratamiento también debe designar uno.

La designación de un OPD por parte del Responsable del Tratamiento no implica que su Encargado del Tratamiento también tenga que designar uno. Lo anterior, sin perjuicio de las obligaciones contractuales que entre las partes surjan del contrato de transmisión de datos personales.

Precisamente, de acuerdo con el artículo 2.2.2.25.5.2. del Decreto 1074 del 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, aquel contrato señalará los alcances del Tratamiento, las actividades que el Encargado realizará por cuenta del Responsable para el Tratamiento de los datos personales y las obligaciones del Encargado para con el Titular y el Responsable. Adicionalmente, aquel contrato podría establecer la necesidad de que el Encargado del Tratamiento cuente también con un OPD, si así se estima conveniente.

Es posible realizar la designación de un Oficial de Protección de Datos Personales único para varias organizaciones

Es posible la designación de un OPD único para varias organizaciones. Por ejemplo, un Grupo Empresarial[6] puede tener un único OPD que asista a todos los miembros del grupo en el ejercicio de sus funciones. En estos casos, lo importante es garantizar la accesibilidad del OPD a cada miembro del Grupo Empresarial.

De igual forma, es posible que una organización externa preste los servicios de OPD a más de un Responsable y/o Encargado del Tratamiento. Es decir, es factible tercerizar las labores de OPD a una organización (ej. Firma de abogados o empresa que preste servicios profesionales en la materia) experta en la materia. Vale considerar que, con el objetivo de garantizar la claridad jurídica y la adecuada ejecución de las labores, se recomienda asignar claramente las tareas dentro del equipo del OPD externo y designar una única persona como contacto y persona "a cargo" de cada cliente. También sería útil, en general, especificar estos puntos en el contrato celebrado con la organización que realizará las funciones de OPD.

En ese mismo orden de ideas, la función del OPD también puede ejercerse en el marco de un contrato suscrito con una persona natural ajena a la organización del Responsable o del Encargado del Tratamiento. De esta manera, es posible tercerizar a una persona natural experta en la materia que preste dichos servicios profesionales de manera independiente.

6 Según el artículo 28 de la Ley 222 de 1995: "*Habrá grupo empresarial cuando además del vínculo de subordinación, exista entre las entidades unidad de propósito y dirección.*

Se entenderá que existe unidad de propósito y dirección cuando la existencia y actividades de todas las entidades persigan la consecución de un objetivo determinado por la matriz o controlante en virtud de la dirección que ejerce sobre el conjunto, sin perjuicio del desarrollo individual del objeto social o actividad de cada una de ellas.

Corresponderá a la Superintendencia de Sociedades, o en su caso a la de Valores o Bancaria, determinar la existencia del grupo empresarial cuando exista discrepancia sobre los supuestos que lo originan".

Garantice que el Oficial de Protección de Datos Personales sea accesible y fácil de ubicar

Para la satisfactoria ejecución de las labores asignadas al OPD, es indispensable que los diferentes sujetos interesados en su labor puedan contactarlo sin tener que comunicarse con otra dependencia de la organización. De esta manera, se recomienda la publicación y divulgación de los datos de contacto del OPD. Adicionalmente, se aconseja informarle a la Dirección de Investigación de Protección de Datos Personales aquella información.

Con lo anterior, se pretende garantizar que los diferentes sujetos interesados -tanto internos como externos a la organización- y la Autoridad Nacional de Protección de Datos Personales puedan contactar de forma fácil y directa al OPD.

Ante la pregunta, ¿Qué datos del OPD se recomiendan poner a disposición del público? es necesario considerar lo siguiente. La información de contacto del OPD debería incluir información que permita a los interesados y

a la Superintendencia de Industria y Comercio comunicarse con este de forma sencilla. Por ejemplo, entre otros, se recomienda informar:

- Dirección física de atención al público.
- Número telefónico de la oficina.
- Dirección de correo electrónico específico previsto para el desarrollo del oficio.

Cuando corresponda, a efectos de comunicación con el público, podrían proporcionarse otros medios de comunicación, por ejemplo:

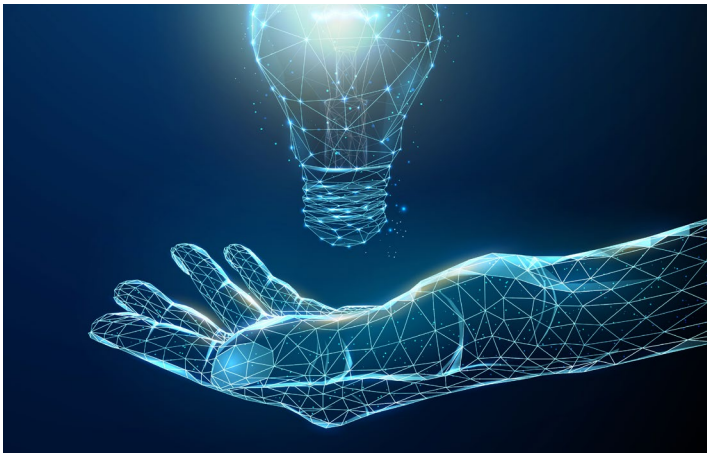
- Una línea directa específica.
- Un formulario de contacto específico dirigido al OPD en el sitio web de la organización.

Ahora bien, puede que no toda organización considere necesario informarle al público el nombre del OPD (persona natural). Aunque hacerlo podría ser una práctica recomendable. De ahí que, corresponde al Responsable o al Encargado del Tratamiento y al OPD decidir si es necesario o útil en cada circunstancia concreta.

No obstante, la comunicación del nombre del OPD a la Autoridad Nacional de Protección de Datos Personales es fundamental, con el fin de que el OPD actúe como punto de contacto entre la organización y aquella entidad.

Como una buena práctica, se recomienda que las organizaciones informen a sus empleados y proveedores del nombre y datos de contacto del OPD. Por ejemplo, el nombre y los datos de contacto del OPD podrían publicarse internamente en la intranet de la organización, en el directorio telefónico interno y en el organigrama.

Por último, garantice la debida confidencialidad de las comunicaciones que sostenga el OPD. La confidencialidad en las comunicaciones que sostenga el OPD es importante. Por ejemplo, los empleados de la organización pueden ser reacios a presentar quejas al OPD si la confidencialidad de sus comunicaciones no está garantizada. De ahí que, el OPD tendrá el deber de mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones.



Verifique y garantice el conocimiento especializado del Oficial de Protección de Datos Personales

Es importante que la organización, al momento de seleccionar su OPD, tenga en consideración el nivel de conocimientos. De esta manera, aquel nivel de conocimiento debe, por lo menos, ser acorde con la sensibilidad, complejidad y cantidad de datos que la organización trata. Por ejemplo, cuando la actividad de Tratamiento de los datos es especialmente compleja o cuando implica una gran cantidad de datos sensibles, el OPD podría necesitar un nivel mayor de conocimientos y apoyo.

Existe también una diferencia dependiendo de si la organización transfiere sistemáticamente Datos personales a países que no cuentan con un nivel adecuado de protección de datos[7] o si dichas transferencias son ocasionales. Por tanto, el OPD debe seleccionarse con cuidado, teniendo debidamente en cuenta las particularidades relativas al Tratamiento de datos personales de cada organización.

Sin duda, un factor importante es que este tenga conocimientos sobre el Régimen General de Protección de Datos Personales de Colombia y las prácticas nacionales en la materia. Más aún, el conocimiento, por parte del OPD, de legislaciones internacionales le permitirán a la organización ser más competitiva en el cumplimiento de las normas donde ofrezca bienes o servicios.

De igual forma, el conocimiento del sector empresarial y de la organización del Responsable del

7 Revisar Circular Externa N° 5 del 10 de agosto del 2017 de la Superintendencia de Industria y Comercio.

Tratamiento es también útil. Asimismo, el OPD debe tener un buen conocimiento de las operaciones específicas de Tratamiento que se llevan a cabo, así como de los sistemas de información y de las necesidades de seguridad[8] y protección de datos de la organización.

Para el caso de un OPD de una entidad estatal, es recomendable que aquel posea un conocimiento sólido de las normas que regulan el sector.

Procure la participación del Oficial de Protección de Datos Personales en todas las cuestiones relativas a la Protección de Datos Personales

La privacidad desde el diseño y por defecto (*Privacy by Design and by Default*), es considerada una medida proactiva para, entre otras, cumplir con el Principio de Responsabilidad Demostrada (*Accountability*). Al introducir la privacidad desde el diseño, se busca garantizar el correcto Tratamiento de los datos utilizados en los proyectos que involucren recolección, uso o Tratamiento de datos personales. Así las cosas, el debido Tratamiento de la información debe ser un componente esencial del diseño y puesta en marcha de todos los proyectos de cada organización.

De ahí que, es fundamental que el OPD y/o su equipo, participen desde la etapa más temprana posible en todos los productos, servicios o proyectos de la organización. Por ejemplo, desde las evaluaciones de impacto relativas a la protección de datos, se recomienda el asesoramiento del OPD.

Precisamente, garantizar que se informe y consulte al OPD desde el principio, facilitará el cumplimiento del Régimen General de Protección de Datos Personales, fomentará un enfoque de privacidad desde el diseño y, por lo tanto, debería ser un procedimiento estándar en la gobernanza de la organización.

Asimismo, es importante que el OPD sea considerado como un interlocutor dentro de la organización y que forme parte de los correspondientes grupos de trabajo que se ocupan de las actividades relacionadas con el Tratamiento de datos dentro de la organización.

En consecuencia, se le recomienda a la organización, por ejemplo, que:

- Se invite al OPD a participar con regularidad en reuniones con los directivos de la organización.
- El OPD esté presente cuando se tomen decisiones con implicaciones para la protección de datos personales. Toda la información pertinente debería de transmitírsele al OPD y a su debido tiempo con el fin de que pueda prestar una asesoría adecuada.
- La opinión del OPD sea debidamente tenida en cuenta. En caso de desacuerdo, se recomienda, como buena práctica, documentar los motivos por los que no

8 Se recomienda tener en consideración la Guía para la Gestión de Incidentes de Seguridad en el Tratamiento de Datos Personales: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf

se sigue el consejo del OPD por parte de la organización – Responsable/Encargado del Tratamiento –.

- Se consulte al OPD con prontitud una vez que se haya producido una brecha a los códigos de seguridad de la organización o cualquier incidente que afecte la información.

Cuando sea pertinente, el Responsable o el Encargado del Tratamiento podría elaborar directrices o programas internos sobre la protección de datos que determinen cuándo debe consultarse al OPD.

No olvide la importancia de que el Oficial de Protección de Datos Personales cuente con los recursos necesarios para el cumplimiento de las funciones

El OPD debe contar con los recursos necesarios para el adecuado cumplimiento de las funciones asignadas. Por tanto, es indispensable que la organización respalde a su OPD facilitando los recursos necesarios para el desempeño de sus funciones y el acceso a los datos personales y a las operaciones de Tratamiento que aquella realice.

De igual forma, se requiere apoyo adecuado en cuanto a recursos financieros, infraestructura (locales, instalaciones, equipos) y personal,

según se requiera. El acceso a otras áreas de la organización. Las labores del OPD son transversales al día a día de la organización, por ello, es necesario que aquella persona tenga acceso a otros servicios, como:

- **El área de recursos humanos.**
- **La Oficina Jurídica.**
- **El área de tecnología y seguridad.**

De modo que los OPD puedan recibir apoyo esencial e información de aquellas otras dependencias.

Adicionalmente, es recomendable que se garanticen los mecanismos idóneos para el mantenimiento de sus conocimientos especializados. Es decir, garantizar una formación continua. Debe darse a los OPD la oportunidad de mantenerse al día con respecto a los avances que se den en el ámbito de la protección de datos. El objetivo debe ser mejorar constantemente el

nivel de conocimientos del OPD y se les debe animar a participar en cursos de formación sobre protección de datos y otras formas de desarrollo profesional, como la participación en foros privados, talleres, etc.

Tenga en cuenta que, cuanto más complejas o sensibles sean las operaciones de Tratamiento, más recursos deberán destinarse al OPD. La función de protección de datos debe desempeñarse con eficacia y dotarse con los recursos suficientes para que el Tratamiento que se esté realizando sea adecuado.

El respeto a la autonomía e independencia del Oficial de Protección de Datos Personales será esencial para el satisfactorio cumplimiento de sus funciones

Se recomienda establecer dentro de la organización algunas garantías básicas que contribuyan a asegurar que los OPD puedan realizar sus tareas con el suficiente grado de autonomía.

En particular, los Responsables o Encargados del Tratamiento deberían garantizar que el OPD no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. Los OPD sean o no empleados del Responsable o Encargado del Tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente.

Esto significa que, en el desempeño de sus tareas, no debe instruirse a los OPD sobre cómo abordar un asunto. Por ejemplo, qué resultado debería lograrse, cómo investigar una queja o si se debe consultar a la autoridad de protección de datos personales. Asimismo, no se les debería instruir para que adopten una determinada postura con respecto a un asunto relacionado con la regulación, por ejemplo, una interpretación concreta de la ley.

Ahora bien, la autonomía de los OPD no significa que tengan poder para adoptar decisiones más allá de sus funciones, definidas con arreglo a su contrato o manual de funciones. Como se ha mencionado, el Responsable o el Encargado

del Tratamiento sigue siendo Responsable del cumplimiento de la normativa de protección de datos y debe ser capaz de demostrar dicho cumplimiento.

Cuando la organización (Responsable o Encargado del Tratamiento) tome una decisión que vaya en contra de la regulación, el OPD debería contar con los canales adecuados para expresar sus inquietudes.

Por último, el OPD idealmente debería rendir cuentas directamente al más alto nivel jerárquico de la organización. Dicha situación ayuda a garantizar que la alta dirección (p. ej. junta directiva) está informada de los consejos y recomendaciones del OPD. Ya que, como parte de la misión del OPD está la de informar y asesorar al Responsable o al Encargado del Tratamiento. Por supuesto, aquella rendición de cuentas debería acompañarse con un escrito que permita dejar trazabilidad de las labores y recomendaciones.

Evite los conflictos de intereses cuando el Oficial de Protección de Protección de Datos Personales realice otras funciones en la organización.

No sería extraño que el OPD desempeñara otras funciones y cometidos dentro de la organización. Sin embargo, especialmente en aquellas situaciones, se requiere que la organización garantice que dichas funciones y cometidos no den lugar a conflicto de intereses.

La ausencia de conflicto de intereses está

estrechamente relacionada con la necesidad de un actuar independiente y autónomo por parte del OPD. Aunque el OPD puede tener otras funciones, solamente deberían confiársele otras tareas y cometidos si estas no dan lugar a conflictos de intereses. Esto supone, en especial, que el OPD no debería ocupar un cargo en la organización que le lleve a determinar los fines y medios del Tratamiento de datos personales.

Debido a la estructura organizativa específica de cada organización, esto deberá considerarse caso por caso.

Como norma general, los cargos en conflicto dentro de una organización pueden incluir los puestos de alta dirección. A modo de ejemplo:

- **Director general.**
- **Director de operaciones.**
- **Director financiero.**
- **Jefe del área de mercadotecnia.**
- **Jefe de recursos humanos.**
- **Director del área de TI.**

De todas formas, otros cargos inferiores en la estructura organizativa también podrían generar un conflicto de intereses si tales cargos llevan a la determinación de los fines y medios del Tratamiento.

Asimismo, también puede surgir un conflicto de intereses, por ejemplo, si se pide a un OPD que represente al Responsable o al Encargado del Tratamiento ante instancias jurisdiccionales en casos relacionados con la protección de datos.

Por eso, dependiendo de las actividades, tamaño y estructura de la organización, puede ser una práctica recomendable que los Responsables y Encargados del Tratamiento:

- Determinen los puestos que podrían ser incompatibles con la función de OPD.
- Elaboren normas internas a tal efecto con el fin de evitar conflictos de intereses.
- Incluyan una explicación más general sobre los conflictos de intereses.

- Declaren que su OPD no tiene ningún conflicto de intereses con respecto a sus funciones.

Una manera como la organización puede crear consciencia en dicho sentido sería:

- Incluyendo las salvaguardas en los manuales internos de la organización.
- Garantizar que en el anuncio de convocatoria para el puesto de OPD o el contrato de servicios sea lo suficientemente preciso y detallado para evitar un conflicto de intereses.

En este contexto, debe tenerse en cuenta también que los conflictos de intereses pueden adoptar diversas formas en función de si el OPD es un empleado de la organización o es un servicio tercerizado.

RECOMENDACIONES SOBRE LAS FUNCIONES DEL OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

Luego de haber desarrollado algunas recomendaciones relativas a los procesos de designación de un OPD, se abordarán algunas recomendaciones centradas en las funciones que realiza el OPD en la organización.

Supervisión de la observancia del Régimen de Protección de Datos Personales

Como función esencial de un OPD en la organización se encuentra la de supervisar el cumplimiento del Régimen General de Protección de Datos Personales. Precisamente, la importancia de que los Responsables y Encargados del Tratamiento cuenten con la colaboración de un OPD.

Para lograr dicho cometido, es importante que el OPD conozca las obligaciones específicas que deberá cumplir. Entre otras que puedan surgir, luego de analizar las particularidades de cada organización, las obligaciones específicas de supervisión del **Régimen General de Protección de Datos Personales están las siguientes:**

- **Recabar** información para determinar las actividades de Tratamiento.
- **Analizar y comprobar** la conformidad con la normativa de las actividades de Tratamiento.
- **Informar, asesorar y emitir** recomendaciones al Responsable o al Encargado del Tratamiento.
- **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 ara asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales.

- **Impulsar** una cultura de protección de Datos personales en poder de la organización y su debida clasificación según su naturaleza.
- **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 Superintendencia de Industria y Comercio.
- **Obtener** las declaraciones de conformidad de la Superintendencia de Industria y Comercio cuando sea requerido.
- **Obtener** la certificación de las Normas Corporativas Vinculantes por parte de la Superintendencia de Industria y Comercio cuando sea requerido.
- **Revisar** los contenidos de los contratos de transferencias internacionales de Datos personales que se suscriban con otros Responsables del Tratamiento, ubicados o no en territorio colombiano[9].
- **Revisar** los contenidos de los contratos de transmisión internacional de Datos personales que se suscriban con Encargados del Tratamiento, ubicados o no en territorio colombiano.
- **Analizar** la responsabilidad 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.

- **Realizar** el entrenamiento necesario a los nuevos colaboradores, que tengan acceso por las condiciones de sus contratos, 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*, gestión de proveedores, etc.)[10].
- **Medir** la participación, y calificar el desempeño, en los entrenamientos de protección de datos Personales.
- **Requerir** que, dentro de los análisis de desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre Datos personales.
- **Velar** por la implementación de planes de auditoría interna para verificar el cumplimiento de sus políticas de

9 Se recomienda revisar la Guía para la implementación del Principio de Responsabilidad Demostrada en las Transferencias Internacionales de Datos Personales: https://www.sic.gov.co/sites/default/files/files/2021/2021%20Gu%C3%ADas%20para%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%202021.pdf

10 Se recomienda revisar la Guía sobre el Tratamiento de Datos Personales para fines de marketing y publicidad: https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20marketing%2C%20publicidad%20y%20tratamiento%20de%20datos%202019.pdf

Tratamiento de 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.

Como se mencionó al inicio, supervisar la observancia no significa que el OPD sea personalmente Responsable de cualquier caso de inobservancia al Régimen General de Protección de Datos Personales.

Las Leyes Estatutarias 1266 de 2008 y 1581 de 2012 establecen claramente los sujetos obligados ante la ley y quienes están obligados a "*ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado las medias apropiadas y efectivas para cumplir con las obligaciones establecidas*". Por eso, el cumplimiento de las normas en materia de protección de datos es responsabilidad del Responsable/Encargado del Tratamiento, no del OPD.

El trabajo del Oficial de Protección de Datos Personales en una evaluación de impacto relativa a la protección de Datos Personales

En reiteradas ocasiones, la Superintendencia de Industria y Comercio ha sugerido efectuar una evaluación de impacto en la privacidad (Privacy Impact Assessment - PIA por sus siglas en inglés), con el fin de poner en funcionamiento un sistema efectivo de manejo de riesgos y controles internos para garantizar que los datos se traten debidamente y conforme con la regulación existente. Aquella labor se encuentra en cabeza del Responsable del Tratamiento y no del OPD.

No obstante, a la luz de la privacidad desde el diseño y por defecto se recomienda que el Responsable del Tratamiento acuda al OPD cuando realice una evaluación de impacto relativa a la protección de datos. Más aún, se recomienda a los Responsables del Tratamiento para que acudan a la asesoría del OPD, entre otras, para los siguientes asuntos:

- Si debe llevarse a cabo o no una evaluación de impacto relativa a la protección de Datos personales.
- Qué metodología debe seguirse al llevar a cabo una evaluación de impacto.
- Si debe realizarse la evaluación de impacto por la propia organización o subcontratarse.
- Qué medidas (incluidas aquellas técnicas, organizacionales y administrativas) deben aplicarse para mitigar cualquier riesgo para los derechos e intereses de los Titulares de la información.
- Si la evaluación de impacto relativa a la protección de datos se ha llevado a cabo correctamente o no y si sus conclusiones (si seguir adelante o no con el Tratamiento y qué medidas aplicar) son conformes con la regulación colombiana en la materia.

Si el Responsable no está de acuerdo con la asesoría ofrecida por el OPD, se recomienda que la documentación de la evaluación de impacto justifique específicamente por escrito por qué no se ha tenido en cuenta el/los consejo(s).

Por último, se recomienda, además, que el Responsable del Tratamiento describa con claridad, en el contrato del OPD las funciones exactas del OPD y su alcance, en particular con respecto a la realización de evaluaciones de impacto relativas a la protección de datos.

El Oficial de Protección de Datos Personales como un canal de cooperación con la autoridad de control y actuación como punto de contacto

Una manera de garantizar el adecuado Tratamiento que realiza la organización y la constante actualización del OPD, es precisamente que aquel coopere con la Autoridad Nacional de Protección de Datos y actúe como punto de contacto para cuestiones relativas al Tratamiento de la información.

Estas labores materializan el papel de facilitador del OPD. El OPD actúa como punto de contacto para facilitar el acceso de la Autoridad Nacional de Protección de Datos a los documentos y la información necesarias para la realización de sus funciones, así como para el ejercicio de sus poderes de investigación y control.

Como ya se ha señalado, el OPD debería mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones. No obstante, aquella necesidad de mantener el secreto o la confidencialidad no excluye la posibilidad y conveniencia de que el OPD se contacte con la Autoridad Nacional de Protección de Datos y acuda a su asesoramiento. Precisamente, es recomendable que el OPD realice consultas a la Autoridad Nacional de Protección de Datos sobre cualquier asunto en el marco de sus funciones.

Se recomienda que las labores del Oficial de Protección de Datos Personales se realicen con un enfoque basado en el riesgo

El OPD debería desempeñar sus funciones prestando la debida atención a los riesgos asociados a las operaciones de Tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del Tratamiento.

En esencia, se recomienda que los OPD establezcan prioridades en lo que respecta a sus actividades y centren sus esfuerzos en las cuestiones que presenten mayores riesgos para la protección de datos. Esto no significa que deban desatender la supervisión de la observancia de las normas en las operaciones de Tratamiento de datos que tengan comparativamente menos riesgos, sino que deben centrarse en los ámbitos de mayor riesgo.

Aquel enfoque selectivo y pragmático debe ayudar al OPD a asesorar al Responsable del Tratamiento sobre qué metodología usar cuando se realice una evaluación de impacto relativa a la protección de datos, qué ámbitos deben ser objeto de una auditoria de protección de datos interna o externa, qué actividades de formación internas proporcionar al personal o a los directivos Encargados de las actividades de protección de datos y a qué operaciones de Tratamiento dedicar más tiempo y recursos.

El Oficial de Protección de Datos Personales es una persona idónea en la organización para realizar el registro en el Registro Nacional de Bases de Datos

En virtud del artículo 25 de la Ley Estatutaria 1581 de 2012, la Superintendencia de Industria y Comercio es la encargada de administrar el Registro Nacional de Bases de Datos. A su vez, para realizar el registro de bases de datos, los Responsables del Tratamiento "*deberán aportar a la Superintendencia de Industria y Comercio las políticas de Tratamiento de la información, las cuales obligarán a los Responsables y Encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes. Las políticas de Tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la presente ley*".

En la práctica, es frecuente que los OPD elaboren inventarios y mantengan un registro de las operaciones de Tratamiento basándose en la información que les proporcionan las diferentes áreas del Responsable del Tratamiento de datos en la organización. Por tanto, es recomendable que el Responsable o el Encargado del Tratamiento asignen al OPD la tarea de realizar y actualizar el registro de la organización en el Registro Nacional de Bases de Datos.

El Registro Nacional de Bases de Datos es una herramienta que materializa la transparencia porque de manera abierta y libre permite que cualquier ciudadano consulte la información sobre todas las Bases de Datos inscritas en el mismo y las Políticas de Tratamiento de la Información de las entidades estatales.

Es sencillo y gratuito realizar el registro y actualizar la información contenida en el mismo. Para el efecto consulte: https://www.sic.gov.co/registro-nacional-de-bases-de-dato.

Dependiendo del tipo de organización y su respectivo tamaño, se recomienda que el Oficial de Protección de Datos Personales presida un comité integrado por las diferentes dependencias de la organización para la adecuada toma de decisiones relativa al Tratamiento de Datos personales

Durante el ciclo de vida de la información en la organización, son varias áreas que realizan Tratamiento sobre ella o, en su caso, deciden qué se realizará con aquella. Por ello, se recomienda que las organizaciones puedan materializar una instancia –comité– con todas aquellas dependencias para que puedan tomar decisiones sobre la información tratada por el Responsable del Tratamiento bajo una perspectiva holística.

Aquel comité, presidido por el OPD, velaría por la adecuada articulación de las políticas organizacionales en materia de información. Por su parte, como miembros del comité, por ejemplo, podrían participar las siguientes áreas:

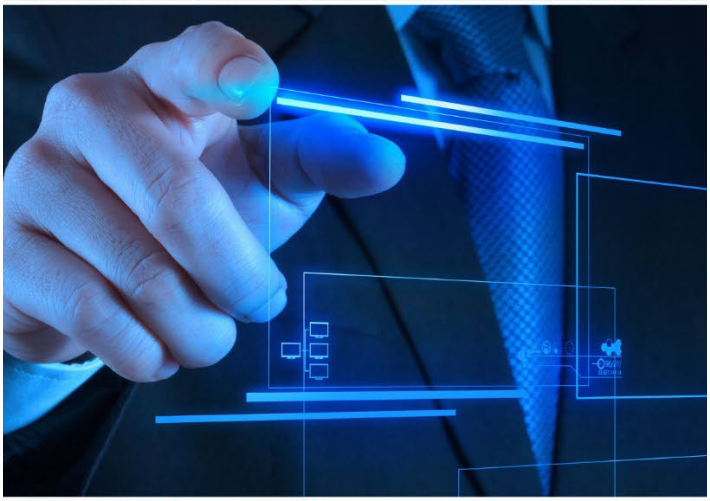
- **Recursos humanos.**
- **Financiera.**
- **Jurídica.**
- **Administrativa.**
- **Informática y tecnología.**
- **Comunicaciones.**

La manera de materializar aquella instancia dependerá de las particularidades de cada organización. Sin embargo, más allá de la metodología o la forma en la que la organización decida su materialización, es necesario entender la importancia que para la organización y los Titulares implica que las decisiones sobre la información se tomen con la participación de todos los actores involucrados en la operación.

La adecuada realización de las funciones del Oficial de Protección de Datos Personales incrementa la confianza de los Titulares de la información.

Desde hace algunas décadas se ha sostenido que la confianza es factor crucial para el crecimiento y consolidación de cualquier actividad que involucre el Tratamiento de Datos Personales. Por eso se ha sostenido que "*las actividades continuas de creación de confianza deben ser una de las prioridades estratégicas más importantes para cada organización*"[11].

La confianza se entiende como la expectativa de que "*se puede contar con la palabra del otro*" y de que se emprenderán acciones positivas y beneficiosas entre las partes de manera recíproca. Cuando existe confianza la persona cree que una entidad es fiable, cumple su palabra, es sincera, íntegra y lleva a cabo las acciones prometidas[12].



11Cfr. Edelman Trust Barometrer de 2019. https://www.edelman.com/trust-barometer

12 Cfr. Barrera Duque, Ernesto (2018) Diseño organizacional centrado en el cliente. Teoría y práctica en empresas sociales. Universidad de la Sabana y Ecoe ediciones.

De esta manera, la adecuada realización de las funciones del OPD ayudará a incrementar la confianza de los Titulares en la organización.

Finalmente, es importante recalcar que todas las recomendaciones anteriores sólo están enfocadas a las organizaciones que pretendan designar un Oficial de Protección de Datos Personales con el fin de orientarlos para que implementen medidas de Responsabilidad Demostrada con miras a dar cumplimiento a la regulación colombiana; sin perjuicio de otras medidas que permitan dar correcto cumplimiento a lo dispuesto en el artículo 2.2.2.25.4.4. del Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.

Esta guía tiene carácter especial y complementario a la "*Guía para implementación del Principio de Responsabilidad Demostrada (accountability)*" publicada por la Superintendencia de Industria y Comercio el 28 de mayo del 2015.

GLOSARIO

Para mayor comprensión de algunos términos utilizados en esta guía, a continuación, transcribimos la denominación exacta de cada uno y su definición legal.

AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES: "*La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley*"[13].

BASE DE DATOS: "*Conjunto organizado de datos personales que sea objeto de Tratamiento*"[14].

ENCARGADO DEL TRATAMIENTO: "*Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos Personales por cuenta del responsable del tratamiento*"[15].

RESPONSABLE DEL TRATAMIENTO: "*Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos*"[16].

TITULAR: **"***Persona natural cuyos datos personales sean objeto de Tratamiento*"[17].

TRATAMIENTO: "*Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión*"[18].

TRANSFERENCIA: "*La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país*"[19].

DATO PERSONAL: "*Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables*"[20].

13 Artículo 19 de la Ley Estatutaria 1581 de 2012.
14 Literal b) del artículo 3 de la Ley Estatutaria 1581 de 2012.
15 Literal d) del artículo 3 de la Ley Estatutaria 1581 de 2012.
16 Literal e) del artículo 3 de la Ley Estatutaria 1581 de 2012.
17 Literal f) del artículo 3 de la Ley Estatutaria 1581 de 2012.
18 Literal g) del artículo 3 de la Ley Estatutaria 1581 de 2012.
19 Numeral 4 del artículo 3 del Decreto 1377 de 2013, incorporado en el Decreto Único Reglamentario1074 de 2015. 26 Numeral 5 del artículo 3 del Decreto 1377 de 2013, incorporado en el Decreto Único Reglamentario1074 de 2015.
20 Literal c) del artículo 3 de la Ley Estatutaria 1581 de 2012.

DOCUMENTOS CONSULTADOS

Barrera Duque, Ernesto (2018) Diseño organizacional centrado en el cliente. Teoría y práctica en empresas sociales. Universidad de la Sabana y Ecoe ediciones.

Cavoukia, Ann. Privacidad por Diseño: Los 7 principios fundamentales. Disponible en: http://mediascope.nl/wp-content/uploads/2015/08/privacidad-por-dise%C3%B1o.pdf

Superintendencia de Industria y Comercio (2015) "*Guía para implementación del principio de responsabilidad demostrada (accountability)*". https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

Grupo de Trabajo sobre Protección de Datos del Artículo 29 (2017). Directrices sobre los delegados de protección de datos (DPD).

Superintendencia de Industria y Comercio (2021) "*Guía para la implementación del Principio de Responsabilidad Demostrada en las transferencias Internacionales de Datos Personales*". https://www.sic.gov.co/sites/default/files/files/2021/2021%20Gu%C3%ADas%20para%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%202021.pdf

Superintendencia de Industria y Comercio (2020) "*Guía para la gestión de incidentes de seguridad en el Tratamiento de Datos Personales*". https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf

Superintendencia de Industria y Comercio (2019) "*Guía sobre el Tratamiento de Datos Personales para fines de marketing y publicidad*". https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20marketing%2C%20publicidad%20y%20tratamiento%20de%20datos%202019.pdf

COLOMBIA POTENCIA DE LA VIDA

Industria y Comercio
SUPERINTENDENCIA

@sicsuper

@superintendencia_sic

Superintendencia de Industria y Comercio de Colombia

Superintendencia de Industria y Comercio de Colombia

Conmutador: (601) 5 870 000 - Contact Center: (601) 5 920 400
Línea gratuita nacional desde teléfonos fijos: 01 8000 910 165