LINEAMIENTOS PARA EL CUMPLIMIENTO DE LA CIRCULAR EXTERNA 003 DE 2024 DE LA SIC
INSTRUCCIONES PARA LOS ADMINISTRADORES SOCIETARIOS
EN EL TRATAMIENTO DE DATOS PERSONALES

La mayoría de los lineamientos relacionados provienen de la Guía de Responsabilidad Demostrada de la SIC y sirven como orientación para cumplir con las instrucciones establecidas en la circular externa 003 de 2024. Sin embargo, estos no son los únicos. Enmarcados en el principio de responsabilidad demostrada, los responsables deben identificar controles y medidas adicionales, de carácter preventivo y proactivo, que se ajusten a las particularidades de cada organización, con el fin de proteger el derecho de los titulares a la protección de sus datos personales.

1. **Los administradores están obligados al cumplimiento de los establecido por la regulación relativa a la protección de datos personales.**

DIMENSIÓN GUÍA DE RESPONSABILIDAD DEMOSTRADA	ACTIVIDAD	CUMPLE	
		SI	NO
1.1 DESDE LA ALTA DIRECCIÓN	Aprobar y monitorear el Programa Integral de Gestión de Datos Personales		

2. **Las Políticas Internas Efectivas que establezcan los administradores para garantizar el debido Tratamiento de Datos personales en la actividad económica deben ser objeto de monitoreo y control para garantizar su cumplimiento.**

DIMENSIÓN GUÍA DE RESPONSABILIDAD DEMOSTRADA	ACTIVIDAD	CUMPLE	
		SI	NO
1.1 DESDE LA ALTA DIRECCIÓN	Definir responsabilidades específicas para otras áreas de la organización respecto de la recolección, almacenamiento, uso, circulación y eliminación o disposiciones final de los datos personales que se tratan		

DIMENSIÓN GUÍA DE RESPONSABILIDAD DEMOSTRADA	ACTIVIDAD	CUMPLE	
		SI	NO
2.3 POLÍTICAS	Las políticas deben implementar los principios que rigen el Tratamiento de Datos Personales y estar documentadas. Igualmente se deben documentar los procedimientos para la recolección o recopilación, el mantemiento, uso y eliminación o disposicion final de los datos personales.		
2.3 POLÍTICAS	La recolección, almacenamiento, uso, circulación y supresión o disposición final de la informacion personal, incluyendo requisitos para obtener la autorización		
2.3 POLÍTICAS	La conservación y eliminación de la información personal		
2.3 POLÍTICAS	El uso responsable de la información, incluyendo controles de seguridad administrativos, físicos y tecnológicos		
2.3 POLÍTICAS	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 informacion de forma responsable		
2.3 POLÍTICAS	Procedimiento de quejas y reclamos		
2.3 POLÍTICAS	Si hay otras políticas de la organización (en talento humano, contratos, transparencia) elementos que permitan cumplir con las normas de protección de datos personales		
2.2 INVENTARIO DE LAS BASES DE DATOS CON INFORMACIÓN PERSONAL	Conocer los datos que almacenan, cómo los utilizan y si realmente los necesitan, teniendo en cuenta la finalidad para la cual los recolectan		
2.2 INVENTARIO DE LAS BASES DE DATOS CON INFORMACIÓN PERSONAL	Identificar en que parte del procedimiento o actividad se obtienen los datos, si deben solciitar la autorización del Titular y, de ser así, si están conservando prueba de la misma para su posterior consulta		
2.2 INVENTARIO DE LAS BASES DE DATOS CON INFORMACIÓN PERSONAL	En caso de manejo de datos de NNA implementar medidas adecuadas para garantizar la protección reforzada de dicha información		
2.2 INVENTARIO DE LAS BASES DE DATOS CON INFORMACIÓN PERSONAL	Asegurarse de que se esté informando al titular o a quien corresponda (datos de menores) que no existe obligación de suministar tales datos. La clasificación de la información recopilada por la compañía, por ejemplo, en sensible, confidencial, pública, según el caso, ayuda a tener un inventario efectivo de los datos tratados por la empresa		

DIMENSIÓN GUÍA DE RESPONSABILIDAD DEMOSTRADA	ACTIVIDAD	CUMPLE	
		SI	NO
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 amenazas y riesgos al tratamiento de datos personales detectados en la organización, los controles del programa estan teniendo en cuenta las nuevas amenazas y reflejadno las qujeas más recientes o los hallazagos de las auditorias, o las orientaciones de la autoridad de proteccion de datos, se estan ofreciendo nuevos servicios que involucran una mayor recolección, uso o divulgación de la informacion personal, se esta llevando a cabo capacitacion eficaz, se estan siguiendo las políticas y procedimientos, y el programa se ecnuetnra actualizado		

3. **La adopción de mecanismos internos para hacer cumplir las Políticas Internas Efectivas, incluyendo herramientas de implementación, entrenamiento y programas de sensibilización, deben ser conocidas y promovidas por los administradores. Para lograr estos objetivos, se puede: i) designar a la persona o al área que asumirá la función de protección de Datos personales dentro de la organización; ii) aprobar y verificar el real y efectivo cumplimiento de un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de las normas; iii) establecer canales de comunicación que le permitan a la persona o al area responsable informar de manera periódica a los administradores sobre la ejecución de las Políticas Internas Efectivas de la organización.**

DIMENSIÓN GUÍA DE RESPONSABILIDAD DEMOSTRADA	ACTIVIDAD	CUMPLE	
		SI	NO
1.1 DESDE LA ALTA DIRECCIÓN	Designar a una persona o área que asumirá la función de protección de datos dentro de la organización		
1.1 DESDE LA ALTA DIRECCIÓN	Informar de manera periódica a los órganos directivos sobre su ejecución		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Estructurar, diseñar y administrar el programa		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Establecer los controles del programa, evaluación y revisión permanente		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Coordinar la definición e implementación de los controles del Programa Integral de Gestión de Datos Personales		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal del Programa		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Impulsar una cultura de protección de datos personales dentro de la organización		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Registrar las bases de datos de la organización en el RNBD y actualizar el reporte atendiendo a reportes de la SIC		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Obtener declaraciones de conformidad		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Revisar los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con Encargados no residentes en Colombia		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Analizar la responsabilidad de cada cargo de la organización, para diseñar un programa de entrenamiento en protección de datos personales especificos para cada uno de ellos		

DIMENSIÓN GUÍA DE RESPONSABILIDAD DEMOSTRADA	ACTIVIDAD	CUMPLE	
		SI	NO
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Realizar un entrenamiento general en protección de datos personales para todos los empleados de la compañía		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Realizar el entrenamiento necesario a los nuevos empleados que tengan acceso por las condiciones de su empleo, a datos personales gestionardos por la organización		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización (talento humano, call centers y gestión de proveedores, etc)		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Medir la participación, y calificar el desempeño, en los entrenamientos de protección de datos		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Requerir que dentro de los análisis de desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre protección de datos persoanles		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Velar por la implementación de los planes de auditoria interna para verificar el cumplimiento de sus políticas de tratamiento de información personal		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Acompañar y asistir a la Organización en la atención de las visitas y los requerimientos que realice la SIC		
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Realizar seguimiento al Programa Integral de Gestión de Datos Personales		
1.3 PRESENTACIÓN DE INFORMES	Definir de manera clara la estructura de 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 violacion a los códigos de seguridad		
1.3 PRESENTACIÓN DE INFORMES	Documentar el proceso de generación de reportes como parte del Programa		
1.3 PRESENTACIÓN DE INFORMES	Generar reportes para los accionistas o socios de manera periódica, e informar en estos el estado del programa de protección de datos personales		
2.5 REQUISITOS DE FORMACIÓN Y EDUCACIÓN	Impartir una formación de carácter general y particular al personal que maneje datos personales y la formación debe ser permanente		
2.5 REQUISITOS DE FORMACIÓN Y EDUCACIÓN	Dentro de los contratos que suscriban los empleados, se deben incluir acuerdos de cumplimiento de las políticas internas adoptados por los sujetos obligados		

DIMENSIÓN GUÍA DE RESPONSABILIDAD DEMOSTRADA	ACTIVIDAD	CUMPLE	
		SI	NO
2.8 COMUNICACIÓN EXTERNA	Procedimiento para informar a los titulares sus derechos, de acuerdo con lo establecido en el artículo 11 de la ley 1581, así como los programas de control que se han implementado. Las comunicaciones dirigidas a los titulares deben ser claras y comprensibles y no limitarse a una simple repetición de la ley		
2.7 GESTIÓN DE LOS ENCARGADOS DEL TRATAMIENTO EN LAS TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES	Disposiciones que incluyan requisitos para que los encargados cumplan con las normas colombianas de proteccion de datos y las politicas de tratamietno		
2.7 GESTIÓN DE LOS ENCARGADOS DEL TRATAMIENTO EN LAS TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES	Mecanismos para que el Encargado reporte al Responsable los incidentes de seguridad de la información		
2.7 GESTIÓN DE LOS ENCARGADOS DEL TRATAMIENTO EN LAS TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES	Formación y educación en temas de protección de datos personales para los empleados del Encargado que tiene acceso a la información personal		
2.7 GESTIÓN DE LOS ENCARGADOS DEL TRATAMIENTO EN LAS TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES	Exigencia de adherencia a las políticas de tratamiento si se utilizan subcontratistas		
2.7 GESTIÓN DE LOS ENCARGADOS DEL TRATAMIENTO EN LAS TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES	Realización de auditorias internas y/o externas		
2.7 GESTIÓN DE LOS ENCARGADOS DEL TRATAMIENTO EN LAS TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES	Acuerdos con los encargados y sus empleados aceptando que cumplirán con las políticas y protocolos del responsable del tratamiento		

4. **Los administradores deben establecer los lineamientos corporativos adecuados para adoptar medidas precautorias o preventivas para proteger los derechos de los titulares de Datos personales, como lo son, por ejemplo, los estudios de impacto de privacidad. Los estudios de impacto de privacidad podrían incluir, como mínimo, lo siguiente:**
   1. Una descripción detallada de las operaciones de Tratamiento de Datos personales.
   2. Una evaluación de los riesgos específicos para los derechos y libertades de los Titulares de los Datos personales. En la evaluación de riesgos se espera, por lo menos, la identificación y clasificación estos.
   3. Las medidas previstas para evitar la materialización de los riesgos, medidas de seguridad, diseño de software, tecnologías y mecanismos que garanticen la protección de Datos personales, teniendo en cuenta los derechos e intereses legítimos de los Titulares de los datos y de otras personas que puedan eventualmente resultar afectadas.

Recomendaciones

1. Se recomienda que la organización adopte una metodología de evaluación de impacto en protección de datos, identificando operaciones de tratamiento susceptibles de aplicar dicha metodología.
2. Existen diferentes guías, buenas prácticas, software de apoyo para realizar evaluaciones de impacto en protección de datos.
3. En Escuela de Privacidad, tenemos experiencia realizando Evaluaciones de Impacto en Protección de Datos, así como implementando esta metodología al interior de las organizaciones para que estas con su equipo de trabajo la apliquen. Compartimos un webinar, donde hablamos de esta metodología: https://www.youtube.com/watch?v=mUzuXyImCSw&t=137s

5. **Los administradores deben establecer los lineamientos para fortalecer continuamente las medidas de seguridad de la información. En especial, el manual interno de políticas debería involucrar un componente de gestión de riesgos que le permita a la empresa identificar sus vulnerabilidades a tiempo y enfocar sus recursos en la adopción de las medidas de mitigación de riesgos, tanto para ellas como para los Titulares de la Información.**

DIMENSIÓN GUÍA DE RESPONSABILIDAD DEMOSTRADA	ACTIVIDAD	CUMPLE	
		SI	NO
1.2 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales		
2.1 PROCEDIMIENTOS OPERACIONALES	Procedimientos administrativos consistentes con las políticas generales de protección de datos, de forma que se pueda manejar adecuadamente los riesgos inherentes al tratamiento de la informacion personal dentro de las actividades de gestión operacional		
2.4 SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES	Identificación y manejo de riesgos asociados al tratamiento de datos personales a través de un sistema de administración de riesgos, acorde con su estructura organizacional, sus procesos y procedimientoss internos asociados al tratamiento de datos personales, la cantidad de bases de datos y tipos de datos personales tratados por la empresa.		
2.4 SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES	Identificación. Establecer los riesgos a que se ven expuestos los datos personales en desarrollo de su tratamiento.		
2.4 SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES	Documentar los procesos y procedimientos que se implementen dentro del ciclo de vida de los datos personales		
2.4 SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES	Definir la metodología de identificación de riesgos asociados al tratamiento de la información personal		
2.4 SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES	Identificar los riesgos e incidentes ocurridos, respecto de este tipo de información, en los casos que aplique		
2.4 SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES	Medición. Tiene por objeto determinar la posibilidad de ocurrencia de los riesgos relacionados con el tratamiento de datos personales y su impacto en el caso de materializarse		
2.4 SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES	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 su materialización de los mismos.		

DIMENSIÓN GUÍA DE RESPONSABILIDAD DEMOSTRADA	ACTIVIDAD	CUMPLE	
		SI	NO
2.4 SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES	Monitoreo. Realizar un seguimiento constante para velar por las medidas que se hayan establecido sean efectivas.		
2.4 SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES	Llevar una registro de incidentes que contemple: base de datos y datos comprometidos, titulares, fecha del incidente, y de descubrimiento, acciones correctivas realizadas y responsables.		
2.4 SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES	Se debe evaluar los riesgos periódicamente e implementar estas evaluaciones en toda la organización dentro de cada nuevo proyecto que involucre datos personales		
2.6 PROTOCOLOS DE RESPUESTA EN EL MANEJO DE VIOLACIONES E INCIDENTES	Gestión de riesgos internos y externos, que le permitan identificar sus vulnerabilidades a tiempo, se debe contar con una persona o área responsable de manejar los incidentes o vulneraciones a los sistemas de informacion o a los archivos fisicos.		
2.6 PROTOCOLOS DE RESPUESTA EN EL MANEJO DE VIOLACIONES E INCIDENTES	Mecanismos para rendir informes internos y reportar los incidentes a los titulares y a la SIC. Se debe implementar mecanismos que les permitan comunicarse de manera eficiente con los titulraes afectados, sobre el incidente de seguridad relacionads con sus datos personales y las posibles consecuencias, y proporcionar herremiantas a dichos titulares afectados para minimizar el daño potencial o causado.		
2.6 PROTOCOLOS DE RESPUESTA EN EL MANEJO DE VIOLACIONES E INCIDENTES	Se debe informar como minimo, 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 pesonales comprometidos y la cantidad de titulares afectados.		

Corresponsabilidad

- Se recomienda que este tema sea discutido en las juntas directivas, para identificar los riesgos asociados con la posibilidad de que un administrador societario sea declarado corresponsable por la Superintendencia de Industria y Comercio (SIC). En tal caso, estaría sujeto al régimen sancionatorio de la Ley 1581 de 2012.

- No obstante, el mensaje que la SIC intenta transmitir es que, si la empresa demuestra que está implementando las medidas adecuadas, no debería aplicarse la figura de corresponsabilidad.

- Aunque nos apartamos de la interpretación que la SIC está realizando al considerar a un administrador societario como corresponsable, ya que en la práctica esto solo sería posible si el administrador incumple la ley y utiliza los datos para su beneficio personal, en cuyo caso actuaría como persona natural y no en calidad de administrador societario.

Heidy Balanta
Directora- Escuela de Privacidad
hb@escueladeprivacidad.com