CUESTIONARIO DE DIAGNÓSTICO PARA EL CUMPLIMIENTO DE LA LEY 1581 DE 2012 EN LAS MIPYMES

50 años 1968-2018
Industria y Comercio
SUPERINTENDENCIA

GOBIERNO DE COLOMBIA

LISTADOS DE COMPROBACIÓN

La presente cartilla ha sido preparada por la Superintendencia de Industria y Comercio como complemento de la cartilla de "***Formatos modelo para el cumplimiento de obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios***", para orientar a los Responsables y Encargados del Tratamiento de datos personales sobre el cumplimiento de sus obligaciones frente al manejo de información personal y para que aquellos que emprendieron la tarea de implementar un Programa Integral de Gestión de Datos Personales puedan verificar el avance de su organización en algunos de los aspectos incluidos en la "*Guía para la implementación del Principio de Responsabilidad Demostrada*".

En esta ocasión, se pone a disposición de los sujetos obligados en la presente cartilla, dos listados de comprobación. El primero, será útil para verificar el cumplimiento de los principios y deberes establecidos en la Ley 1581 de 2012 por parte de sus organizaciones y, el segundo, les permitirá conocer el nivel de avance de la organización en la implementación del principio de responsabilidad demostrada acorde con los lineamientos establecidos en la guía publicada por esta Superintendencia en el año 2016.

Es importante señalar que estos documentos solo les permiten a los interesados realizar la comprobación de aspectos relativos al cumplimiento de las obligaciones legales de Responsables y Encargados a manera de autoevaluación y no constituyen prueba ante la Superintendencia de la observancia o no de sus obligaciones ni reemplazan la obligatoriedad de contar con toda la documentación requerida por la Ley de Protección de Datos personales y sus normas reglamentarias.

También es necesario precisar que, en lo que respecta a la implementación del principio de responsabilidad demostrada, las organizaciones que desarrollen un Programa Integral de Gestión de Datos Personales deben estar en capacidad de demostrar dicha implementación por lo que el diligenciamiento del listado de comprobación no reemplaza el cumplimiento de sus obligaciones.

Adicionalmente, se aclara que el uso de estas herramientas no implica pronunciamiento alguno por parte de esta entidad respecto del cumplimiento de la Ley 1581 de 2012 y sus decretos reglamentarios por parte de los sujetos obligados, como tampoco inhibe el ejercicio de las funciones de inspección, vigilancia y control a cargo de la Superintendencia de Industria y Comercio.

GLOSARIO[1]

▪ ***Dato personal***: Se trata de cualquier información vinculada a personas naturales que tenga carácter privado, es decir, que esté ligada con su intimidad, su información personal, entre otros.

▪ ***Dato público***: Es uno de los tipos de datos personales existentes. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

▪ ***Dato semiprivado***: Son los datos que no tienen naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo al TTitular sino a cierto sector o a la sociedad en general. Los datos financieros y crediticios de la actividad comercial o de servicios, son algunos ejemplos.

▪ ***Dato privado***: Es el dato que por su naturaleza íntima o reservada solo es relevante para el Titular. El nivel de escolaridad, por ejemplo, corresponde a un dato privado.

▪ ***Datos sensibles***: Son aquellos que afectan la intimidad del Titular, es decir, aquellos que revelan su origen racial o étnico, su orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

▪ ***Autorización***: Es el consentimiento que da cualquier persona para que las empresas o personas Responsables del Tratamiento de la información, puedan utilizar sus datos personales.

▪ ***Aviso de privacidad***: Es una de las opciones de comunicación verbal o escrita que brinda la ley para darle a conocer a los Titulares de la información, la existencia y las formas de acceder a las políticas de Tratamiento de la información y el objetivo de su recolección y uso.

▪ ***Encargado del Tratamiento***: Es la persona natural o jurídica que realiza el Tratamiento de datos personales, a partir de una delegación que le hace el Responsable, recibiendo instrucciones acerca de la forma en la que deberán ser administrados los datos.

1 Estas definiciones están contenidas en la Ley 1266 de 2008, en la Ley 1581 de 2012, en el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo y en la Circular Única de la Superintendencia de Industria y Comercio.

▪ ***Responsable del Tratamiento***: Es la persona natural o jurídica, pública o privada, que decide sobre la finalidad de las bases de datos y/o el Tratamiento de los mismos.

▪ ***Titular***: Es la persona natural cuyos datos personales son objeto de Tratamiento.

▪ ***Base de Datos***: Conjunto organizado de datos personales que son objeto de Tratamiento.

▪ ***Tratamiento***: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

▪ ***Transferencia***: Se trata de la operación que realiza el Responsable o el encargado del Tratamiento de los datos personales, cuando envía la información a otro receptor, que, a su vez, se convierte en Responsable del Tratamiento de esos datos.

▪ ***Transmisión***: Comunicación de los datos dentro o fuera del territorio nacional a un Encargado para que realice el Tratamiento indicado por el Responsable.

▪ ***Incidente de seguridad***: Se refiere a la violación a los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el Responsable del Tratamiento o por su Encargado.

LISTADO DE COMPROBACIÓN RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES

PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES	S/N
Se recolecta información personal para finalidades legítimas y se informa al Titular esas finalidades.	
Se cuenta con el consentimiento previo, expreso e informado para el Tratamiento de datos de los Titulares de los cuales se recolecta información personal.	
Si hay casos en los que se recolecta información personal sin el consentimiento de los Titulares, existe un mandato legal o judicial que habilite a la organización para hacerlo.	
Se conserva información personal veraz, completa, exacta, actualizada, comprobable y comprensible.	
Se cuenta con medidas técnicas para controlar y brindar un conocimiento restringido de la información personal solo a los Titulares o a terceros autorizados conforme a la ley.	
Se cuenta con medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a la información personal para evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.	
Se garantiza la confidencialidad de la información por las personas de la organización que intervienen en el Tratamiento de datos personales, incluso después de que han finalizado su relación con alguna de las labores desempeñadas.	

TRATAMIENTO DE DATOS SENSIBLES Y DE MENORES DE EDAD	S/N
Se cuenta con autorización explícita de los Titulares para el Tratamiento de sus datos sensibles.	
Se informa al Titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.	
Se informa al Titular cuáles de los datos que serán objeto de Tratamiento en su organización son sensibles y para qué finalidad(es) se utilizarán.	
Se efectúa Tratamiento de datos personales de menores de edad únicamente para actividades que responden y respetan el interés superior de los menores.	
En el Tratamiento de datos personales de menores de edad se asegura el respeto de sus derechos fundamentales.	
Se cuenta con la autorización del representante legal del menor de edad para el Tratamiento de sus datos.	

DERECHOS DE LOS TITULARES DE INFORMACIÓN	S/N
Se permite el ejercicio del derecho de los Titulares a conocer, actualizar y rectificar los datos personales que recolecta.	
Se da respuesta a las solicitudes presentadas por los Titulares dentro de la oportunidad prevista en la ley general de protección de datos personales.	
Se entrega a los Titulares copia de la autorización otorgada por ellos para el Tratamiento de sus datos personales cuando así lo solicitan estos.	
Se informa a los Titulares qué uso le ha dado la organización a sus datos personales cuando así lo solicitan estos.	
Se permite a los Titulares el acceso gratuito a los datos personales que han sido objeto de Tratamiento al menos una vez cada mes calendario y cada vez que se hagan modificaciones sustanciales a las Políticas de Tratamiento de la Información.	

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES	S/N
Se cuenta con la autorización de los Titulares de los datos contenidos en las bases de datos que tiene la organización para el Tratamiento de los mismos.	
Se conocen los casos en los que no es necesario contar con autorización de los Titulares para el Tratamiento de su información personal.	
Se cuenta con procedimientos efectivos y eficientes para solicitar, a más tardar en el momento de la recolección de los datos personales, las autorizaciones de los Titulares para el Tratamiento de los mismos.	
Se informa a los Titulares qué datos personales serán recolectados y todas las finalidades específicas del Tratamiento para las cuales la organización obtiene el consentimiento.	
Se obtienen nuevas autorizaciones de los Titulares, cuando la organización realiza cambios sustanciales en las políticas de Tratamiento de información personal.	
Se establecen mecanismos que garantizan la consulta posterior de la autorización otorgada por los Titulares para el Tratamiento de sus datos personales.	
Se pone a disposición de los Titulares mecanismos gratuitos y de fácil acceso para presentar solicitudes de supresión de datos o la revocatoria de la autorización otorgada.	

INFORMACIÓN MÍNIMA A LOS TITULARES	S/N
Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, el Tratamiento al cual serán sometidos los mismos y la finalidad.	
Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, el carácter facultativo de la respuesta a las preguntas que se hacen, cuando se relacionan con datos sensibles o datos de niñas, niños y adolescentes.	
Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, los derechos que les asisten.	
Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, la identificación, dirección física y electrónica y teléfono del Responsable del Tratamiento.	
Se conserva prueba de haber informado a los Titulares lo mencionado anteriormente.	

SUMINISTRO DE LA INFORMACIÓN PERSONAL	S/N
La información personal que se suministra al Titular o a quien éste autorice es de fácil lectura, sin barreras técnicas que impidan su acceso y corresponde en un todo a aquella que reposa en la base de datos.	
Se suministra únicamente información personal a los Titulares, sus causahabientes o sus representantes legales, a las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial y a los terceros autorizados por el Titular o por la ley.	

ATENCIÓN DE CONSULTAS Y RECLAMOS DE LOS TITULARES	S/N
Se cuenta con canales o mecanismos sencillos y ágiles y que estén permanentemente habilitados para la atención de las consultas y reclamos de los Titulares o sus causahabientes.	
Se dan a conocer a los Titulares e interesados los canales habilitados para la atención de consultas y reclamos en la política de Tratamiento de datos personales dispuesta por la organización.	
Se atiende, dentro de los diez (10) días hábiles contados a partir de su recibo, las consultas de información personal presentadas por los Titulares, sus causahabientes y las personas autorizadas.	
Se informa a los peticionarios el motivo de la no atención oportuna a su consulta de información personal y se señala la fecha de respuesta de la solicitud, sin exceder el término de cinco (5) días adicionales a los diez (10) días iniciales para contestar.	
Se atiende, dentro de los quince (15) días hábiles contados a partir de su recibo, las reclamaciones presentadas por los Titulares o sus causahabientes que consideran que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley.	
Se informa a los peticionarios el motivo de la no atención oportuna a su reclamo y se señala la fecha de respuesta de la solicitud, sin exceder el término de ocho (8) días adicionales a los quince (15) días iniciales para contestar.	
Se adoptan medidas para asegurar que los datos personales que reposan en las bases de datos sean precisos y suficientes y, cuando así lo solicite el Titular o cuando haya podido advertirlo, sean actualizados, rectificados o suprimidos, de tal manera que satisfagan los propósitos del Tratamiento.	
Se ha designado a una persona o área para que asuma la función de protección de datos personales y dé trámite a las solicitudes de los Titulares para el ejercicio de sus derechos.	

ATENCIÓN DE CONSULTAS Y RECLAMOS DE LOS TITULARES	S/N
Se da a conocer a los Titulares los procedimientos dispuestos por la organización para el acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización, y los mismos son fácilmente accesibles.	
Se incluye dentro de la política de Tratamiento de datos personales los procedimientos dispuestos para garantizar el acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización.	
Se cuenta con un manual interno de políticas y procedimientos para garantizar la atención de consultas y reclamos presentados por los Titulares y para garantizar, en general, el adecuado cumplimiento de la ley.	
Se han adoptado procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del Tratamiento de sus datos personales.	

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES	S/N
Se cuenta con una política para el Tratamiento de los datos personales.	
La política para el Tratamiento de datos personales consta en medio físico o electrónico, en un lenguaje claro y sencillo, y es puesta en conocimiento de los Titulares.	
Se cuenta con una política para el Tratamiento de datos personales que incluye el nombre o razón social, domicilio, dirección, correo electrónico y teléfono de la organización.	
La política para el Tratamiento de datos adoptada por la organización incluye información sobre el Tratamiento al cual serán sometidos los datos personales y la finalidad del mismo.	
Incluye la política para el Tratamiento de datos personales información sobre los derechos que le asisten a los Titulares respecto de su información personal.	

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES	S/N
Se informa en la política para el Tratamiento de datos personales sobre la persona o área Responsable de la atención de peticiones, consultas y reclamos ante la cual el Titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.	
Se indica en la política para el Tratamiento de datos personales cuál o cuáles son los procedimientos para que los Titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.	
En la política para el Tratamiento de datos personales está incluida la fecha de entrada en vigencia y el período de vigencia de la o las bases de datos que tiene la organización.	

AVISO DE PRIVACIDAD[2]	S/N
Se informa a los Titulares la existencia de políticas para el Tratamiento de datos personales por medio de un aviso de privacidad.	
El aviso de privacidad publicado por la organización incluye el nombre o razón social y los datos de contacto de la misma.	
En el aviso de privacidad publicado se incluye la descripción del Tratamiento al cual serán sometidos los datos personales recolectados y la finalidad de tal recolección.	
El aviso de privacidad incluye un listado de los derechos que tienen los Titulares cuya información es recolectada por la organización.	
Se informa a los Titulares en el aviso de privacidad publicado, cómo acceder o consultar la política de Tratamiento de datos personales dispuesta por la organización.	
En el aviso de privacidad publicado se señala expresamente la facultad que tienen los Titulares de contestar o no las preguntas que versen sobre datos personales sensibles o sobre los datos de niños, niñas y adolescentes.	
Se conserva el modelo de aviso de privacidad utilizado para cumplir con la obligación legal de dar a conocer las políticas de Tratamiento de la información personal.	

2 La publicación de un aviso de privacidad es obligatoria únicamente si la política de Tratamiento de datos personales implementada por la organización no se pone a disposición de los Titulares e interesados de manera directa.

REPORTE DE VIOLACIONES A LOS CÓDIGOS DE SEGURIDAD	S/N
Informa a la Superintendencia cuando se presentan violaciones a los códigos de seguridad que generen riesgos en la administración de la información de los Titulares.	

GESTIÓN DE ENCARGADOS DEL TRATAMIENTO	S/N
Se han establecido procedimientos internos para asegurar que los Encargados del Tratamiento garanticen la protección de los datos personales que le son entregados y que su Tratamiento se haga acorde con los principios y deberes establecidos en la ley.	
Se suscriben contratos con los Encargados que incluyan expresamente el Tratamiento que éste podrá realizar a los datos personales.	
Se suscriben contratos con los Encargados que incluyan cláusulas de confidencialidad de la información entregada.	
Se exige a los Encargados tener y mantener políticas de seguridad de la información y de Tratamiento de datos personales antes de entregar las bases de datos.	
Se informa al Encargado de forma oportuna todas las novedades respecto de los datos que previamente le fueron suministradas.	
Se cuenta con medidas necesarias para que la información suministrada al Encargado se mantenga actualizada.	
Se comunica al Encargado cuando se ha rectificado la información incorrecta.	
Se comunica al Encargado si determinada información se encuentra en discusión por parte del Titular, una vez éste presenta una reclamación y no ha finalizado el trámite respectivo.	
Se verifica que el Encargado actualice y rectifique la información personal en los términos legales.	

TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES	S/N
Se transfieren datos personales a países que garantizan niveles adecuados de protección de datos, según lo establecido en el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única de la Superintendencia de Industria y Comercio.	
Se han implementado medidas apropiadas y efectivas para garantizar el adecuado Tratamiento de los datos personales que se transfieren a otro país y para otorgar seguridad a los registros al momento de efectuar dicha transferencia.	
Se transfieren datos personales fuera del territorio colombiano con base en alguna de las causales de excepción establecidas en el artículo 26 de la Ley 1581 de 2012.	
Se transfieren datos personales fuera del territorio colombiano con base en una declaración de conformidad emitida por esta Superintendencia.	
Se han suscrito contratos con los Responsables del Tratamiento destinatarios de los datos personales a transferir fuera del territorio colombiano o se implementan otros instrumentos jurídicos en los que se señalen las condiciones que regirán la transferencia internacional de datos personales, mediante las cuales se garantizará el cumplimiento de los principios que rigen el Tratamiento, así como de las obligaciones que tienen a cargo.	
Se transmiten datos personales fuera del territorio colombiano a un encargado para que realice el Tratamiento indicado por la organización como Responsable del Tratamiento y para ello se han suscrito contratos de transmisión de datos personales en los que se señalen los alcances del Tratamiento, las actividades que el encargado realizará y las obligaciones de este respecto de los Titulares y el Responsable.	
Se incluyen en el contrato de transmisión internacional de datos personales celebrado con el Encargado cláusulas mediante las cuales este se compromete a dar aplicación a las obligaciones del Responsable bajo su política de Tratamiento de la información y a realizar el Tratamiento de datos de acuerdo con la finalidad que los Titulares han autorizado y con las leyes aplicables.	

TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES	S/N
Se incluye en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación de dar Tratamiento, a nombre del Responsable, a los datos personales conforme a los principios establecidos en la ley general de protección de datos personales.	
Se incluye en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación para este de salvaguardar la seguridad de las bases de datos que contengan datos personales.	
Se incluye en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación para este de guardar confidencialidad respecto del Tratamiento de los datos personales.	

RESPONSABILIDAD DEMOSTRADA	S/N
Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto Único 1074 de 2015 de manera proporcional a la naturaleza jurídica de la organización y su tamaño empresarial.	
Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto Único 1074 de 2015 de manera proporcional a la naturaleza de los datos personales objeto del Tratamiento.	
Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto Único 1074 de 2015 de manera proporcional al tipo de Tratamiento que realice con los datos personales.	
Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto Único 1074 de 2015 de manera proporcional a los riesgos potenciales que el Tratamiento podría causar sobre los derechos de los Titulares.	

RESPONSABILIDAD DEMOSTRADA	S/N
Se conserva evidencia sobre la implementación efectiva de medidas de seguridad apropiadas para el cumplimiento del régimen de protección de datos personales.	
Se han adoptado mecanismos internos para poner en práctica las políticas establecidas en los que se incluyan herramientas de implementación, entrenamiento y programas de educación en materia de protección de datos personales.	

REGISTRO NACIONAL DE BASES DE DATOS	S/N
Se han registrado las bases de datos con información personal de la organización en el Registro Nacional de Bases de Datos (RNBD), administrado por la Superintendencia de Industria y Comercio[3].	

3 Esto aplica solamente para las sociedades y entidades sin ánimo de lucro que tienen más de 100.000 Unidades de Valor Tributario (UVT), así como para las personas jurídicas de naturaleza pública – Ver Decreto 090 de 2018.

LISTA DE VERIFICACIÓN PARA MEDIR EL AVANCE EN LA IMPLEMENTACIÓN DEL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA EN LA ORGANIZACIÓN

COMPROMISO DE LA ORGANIZACIÓN

DESDE LA ALTA DIRECCIÓN	S/N
Se cuenta con el compromiso de la organización para la implementación de un Programa Integral de Gestión de Datos Personales.	
Existe en la organización una cultura de respeto a la protección de los datos personales que se recogen o tratan.	
Se han comprometido recursos económicos y de personal en la organización, acorde a su tamaño y estructura, así como al tipo de información a la que se le realiza Tratamiento, para la implementación del Programa Integral de Gestión de Datos Personales.	
Se cuenta con el apoyo y compromiso de la Alta Dirección para generar una cultura organizacional de respeto a la protección de datos personales.	
La Alta Dirección de la organización designó a la persona o área que asumirá la función de protección de datos dentro de la organización.	
La Alta Dirección de la organización aprobó el Programa Integral de Gestión de Datos Personales.	
La Alta Dirección de la organización realiza un monitoreo del Programa Integral de Gestión de Datos Personales.	
La Alta Dirección de la organización informa de manera periódica a los órganos directivos sobre la ejecución del Programa Integral de Gestión de Datos Personales.	
La Alta Dirección de la organización destina recursos suficientes al área o persona encargada de diseñar e implementar el Programa Integral de Gestión de Datos Personales para desempeñar sus funciones.	
A través del área o persona encargada de diseñar e implementar el Programa Integral de Gestión de Datos Personales se establecen las 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.	

OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	S/N
Se cuenta con una persona o área que asume la función de protección de datos personales y que da trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el Decreto Único Reglamentario 1074 de 2015.	
Se cuenta con una persona o área que vele por la implementación efectiva de las políticas y procedimientos adoptados por la organización para cumplir las normas de protección de datos personales.	
Se cuenta con una persona o área que establezca los controles del Programa Integral de Gestión de Datos Personales así como la evaluación y revisión permanente de dichos controles.	
La persona o área que asume la función de protección de datos personales ha promovido la elaboración e implementación de un sistema que permita administrar los riesgos del Tratamiento de datos personales.	
La persona o área que asume la función de protección de datos personales sirve de enlace y coordina las demás áreas de la organización para asegurar la implementación transversal del Programa Integral de Gestión de Datos Personales.	
La persona o área que asume la función de protección de datos personales impulsa dentro de la organización una cultura de protección de datos.	
La persona o área que asume la función de protección de datos personales mantiene un inventario de las bases de datos personales en poder de la organización y las clasifica de acuerdo a su tipo.	
La persona o área que asume la función de protección de datos personales registró o ha registrado las bases de datos de la organización en el Registro Nacional de Bases de Datos y ha actualizado tal registro[4].	
La persona o área que asume la función de protección de datos personales ha solicitado la declaración de conformidad de las operaciones de transferencia internacional de información personal ante la Superintendencia, cuando ha sido requerida, de conformidad con las instrucciones impartidas por esa entidad.	

4 Esto aplica solamente para las sociedades y entidades sin ánimo de lucro que tienen más de 100.000 Unidades de Valor Tributario (UVT), así como para las personas jurídicas de naturaleza pública – Ver Decreto 090 de 2018.

OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	S/N
La persona o área que asume la función de protección de datos personales revisa los contenidos de los contratos de transmisiones internacionales de datos, suscritos por la organización con los Encargados del Tratamiento no residentes en Colombia.	
La persona o área que asume la función de protección de datos personales ha diseñado un programa de entrenamiento en protección de datos personales acorde con las responsabilidades de cada cargo de la organización.	
La persona o área que asume la función de protección de datos personales realiza un entrenamiento general a todos los empleados y colaboradores de la compañía en protección de datos personales.	
La persona o área que asume la función de protección de datos personales realiza un entrenamiento a los nuevos empleados o colaboradores de la organización que, por las condiciones de su empleo, tengan acceso a los datos personales que se gestionan al interior de la misma.	
La persona o área que asume la función de protección de datos personales integra las políticas de protección de datos personales dentro de las actividades de las demás áreas de la organización.	
La persona o área que asume la función de protección de datos personales mide la participación de los empleados y colaboradores en los entrenamientos en protección de datos y califica su desempeño.	
La persona o área que asume la función de protección de datos personales requiere que se complete satisfactoriamente el entrenamiento en protección de datos personales para realizar el análisis del desempeño de los empleados y colaboradores.	
La persona o área que asume la función de protección de datos personales vela por la implementación de planes de auditoría interna para verificar el cumplimiento de las políticas de Tratamiento de datos personales.	
La persona o área que asume la función de protección de datos personales acompaña y asiste a la organización en la atención de las visitas y requerimientos realizados por la Superintendencia de Industria y Comercio.	

ATENCIÓN DE CONSULTAS Y RECLAMOS DE LOS TITULARES	S/N
La persona o área que asume la función de protección de datos personales realiza seguimiento al Programa Integral de Gestión de Datos Personales.	

PRESENTACIÓN DE INFORMES	S/N
Se cuenta con mecanismos de información internos para reportar el seguimiento y la ejecución del Programa Integral de Gestión de Datos Personales.	
Se cuenta con planes de auditoría interna para verificar el cumplimiento de las políticas de Tratamiento de datos personales y señalar el procedimiento a seguir en caso de que se presenten violaciones a los códigos de seguridad o se detecten riesgos en la administración de la información personal de los Titulares.	
Se remite a los accionistas o socios de la organización el material que sustenta la implementación del Programa Integral de Gestión de Datos Personales.	
Se define la estructura de la generación de reportes en la que se establezca qué empleado o persona genera qué tipo de reporte y se asignan responsabilidades claras ante una queja de los Titulares o una violación a los códigos de seguridad.	
Se documenta el proceso de generación de reportes como parte del Programa Integral de Gestión de Datos Personales.	
Se generan reportes para los accionistas o socios de manera periódica y se informa a estos el estado del Programa Integral de Gestión de Datos Personales.	

CONTROLES DEL PROGRAMA

PROCEDIMIENTOS OPERACIONALES	S/N
Se cuenta con procedimientos administrativos consistentes con las políticas generales de protección de datos personales y con las disposiciones legales vigentes, para manejar adecuadamente los riesgos inherentes al Tratamiento de datos personales dentro de la gestión operacional.	

INVENTARIO DE BASES DE DATOS CON INFORMACIÓN PERSONAL	S/N
Se tienen identificadas e inventariadas las bases de datos dentro de la organización.	
Se tiene claridad sobre el medio en el que se conservan las bases de datos al interior de la organización (manual o automatizado). Se tiene claridad de cuántos Titulares o personas naturales existen en cada base de datos.	
Se tiene identificado qué tipo de datos personales reposan en cada base de datos (datos de identificación, datos de ubicación, datos sensibles, datos de contenido socioeconómico, etc.)	
Se tiene establecido claramente para qué se utiliza cada base de datos y si realmente los datos que allí reposan son necesarios, teniendo en cuenta la finalidad para la que se recolectan.	
Se ha identificado cómo se obtienen los datos personales en la organización, si se debe solicitar la autorización de los Titulares para obtener esos datos y, de ser así, si se conserva prueba de tal autorización para su posterior consulta.	
Se informa a los Titulares la finalidad de la recolección de sus datos personales y el Tratamiento al que tales datos serán sometidos, así como los derechos que tienen como Titulares.	
Se protege la calidad de la información personal al momento de su recolección.	
Si se recolectan datos de menores de edad, se han implementado medidas adecuadas para garantizar una protección reforzada de dicha información.	
Si se recolectan datos de menores de edad, la organización informa al Titular o a quien corresponda (tutores o representantes de los menores), que no existe obligación de suministrar tales datos.	
Se ha identificado qué áreas de la organización utilizan los datos personales y de qué forma los utilizan.	
Se han implementado medidas de seguridad para tratar y conservar los datos personales recolectados. Se han implementado procedimientos para actualizar, rectificar y depurar los datos personales en las bases de datos.	

INVENTARIO DE BASES DE DATOS CON INFORMACIÓN PERSONAL	S/N
Se entregan o comparten las bases de datos con información personal a terceros ubicados dentro o fuera del país.	
Se ha identificado para qué se entregan o comparten las bases de datos con información personal con terceros dentro o fuera del territorio nacional.	
Se ha identificado por cuánto tiempo se conservan los datos personales y qué medios se utilizan para su disposición final (archivo físico, digitalización, eliminación, etc).	
Se cuenta con medidas técnicas que garanticen la seguridad de los datos personales una vez se ha definido cuál será su disposición final.	

POLÍTICAS	S/N
Se cuenta con políticas internas debidamente documentadas e implementadas que incluyan las obligaciones señaladas en la Ley de Protección de Datos Personales y se dan a conocer a los empleados o colaboradores.	
Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para la recolección o recopilación, el mantenimiento, uso y eliminación o disposición final de los datos personales.	
Se cuenta con procedimientos debidamente documentados e implementados que establezcan los requisitos para obtener la autorización de los Titulares.	
Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para el acceso y corrección de datos personales.	
Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para la conservación y eliminación de información personal.	
Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para el uso Responsable de la información, incluyendo controles administrativos, físicos y tecnológicos que garanticen la seguridad de la información.	

POLÍTICAS	S/N
Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para la 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 la política de la empresa, se acepta, y se permite a la compañía utilizar dicha información de forma Responsable.	
Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para la presentación de quejas, denuncias y reclamos por parte de los Titulares y la forma de tramitarlas y atenderlas de manera adecuada, congruente y oportuna.	
Se incluye en las políticas de la organización, diferentes a la de protección de datos personales (talento humano, contratos, transparencia, etc.), elementos que permitan cumplir las normas sobre protección de datos.	

SISTEMA DE ADMINISTRACIÓN DE RIESGOS	S/N
Cuenta con un sistema de administración de riesgos, acorde con la estructura organizacional, los procesos y procedimientos internos asociados al Tratamiento de datos personales, la cantidad de bases de datos y los tipos de datos personales tratados por la empresa, que le permita identificar, medir, controlar y monitorear aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos los datos personales.	
Se ha identificado a qué riesgos se ven expuestos los datos personales a los que se realiza Tratamiento al interior de la organización (ej.: riesgo de pérdida o fuga de información, riesgo de mantener información desactualizada o no veraz, riesgo de accesos indebidos a la información, etc.).	
Se ha determinado la posibilidad de ocurrencia de los riesgos identificados y el impacto que podría ocasionar la materialización de los mismos, tanto para los Titulares como para la organización.	

SISTEMA DE ADMINISTRACIÓN DE RIESGOS	S/N
Se ha establecido qué acciones se deben tomar para controlar y/o mitigar los riesgos identificados, con el fin de disminuir la posibilidad y/o el impacto de la materialización de dichos riesgos.	
Los controles establecidos son suficientes, efectivos y oportunos para disminuir la posibilidad y/o el impacto de la materialización de los riesgos.	
Se realiza seguimiento constante para velar porque las medidas adoptadas sean efectivas.	
Se realiza una evaluación de riesgos constante en la organización y desde el diseño en cada nuevo proyecto en el que se involucre el Tratamiento de datos personales.	

FORMACIÓN Y EDUCACIÓN	S/N
Se tiene implementado un programa de capacitación para los empleados y contratistas de la organización en materia de protección de datos personales.	
Se realizan jornadas de capacitación al personal en materia de protección de datos personales, con periodicidad.	
Las capacitaciones realizadas a los empleados, contratistas y colaboradores en general de la organización involucrados directamente en las actividades de Tratamiento de datos personales se adaptan específicamente a las funciones, obligaciones y tareas que tienen a cargo.	
Existen dentro de los contratos suscritos por los empleados de la organización acuerdos de cumplimiento de las políticas internas desarrolladas por esta para el adecuado Tratamiento de los datos de las personas.	

PROTOCOLOS DE RESPUESTA EN EL MANEJO DE VIOLACIONES E INCIDENTES DE SEGURIDAD	S/N
Se cuenta con un procedimiento documentado e implementado y una persona o área encargada de manejar los incidentes o violaciones a los sistemas de información donde se gestionan datos personales y a los archivos físicos.	
Los empleados y contratistas de la organización tienen conocimiento sobre qué hacer antes, durante y después de que se presente un incidente de seguridad.	
Dentro del protocolo de incidentes de seguridad adoptado por la organización está previsto reportar a la Superintendencia de Industria y Comercio la ocurrencia de tales incidentes.	
Se cuenta con mecanismos, herramientas o procedimientos para la elaboración de informes internos y para informar tanto a los Titulares como a la Superintendencia de Industria y Comercio cuando se presenten incidentes de seguridad que involucren datos personales.	
Se cuenta con mecanismos, herramientas o procedimientos que permitan, además de informar a los Titulares la ocurrencia de un incidente de seguridad con sus datos personales y las posibles consecuencias, dar a conocer opciones o alternativas a dichos Titulares para minimizar el daño potencial o el daño causado.	
Se cuenta con mecanismos o procedimientos que permitan informar a la Superintendencia el tipo de incidente ocurrido, la fecha en la que ocurrió y la fecha en la que se tuvo conocimiento del mismo, la causal del incidente, el tipo de datos personales comprometidos y la cantidad de Titulares afectados.	

GESTIÓN DE LOS ENCARGADOS DEL TRATAMIENTO EN LAS TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES	S/N
Se han implementado medidas para asegurar la protección de los datos personales cuyo Tratamiento es realizado por los Encargados.	
Los contratos suscritos con los Encargados del Tratamiento incluyen requisitos para que estos cumplan las normas colombianas de protección de datos y las políticas de Tratamiento de la información adoptadas por la organización.	
Se cuenta con mecanismos para que los Encargados reporten a la organización los incidentes de seguridad de la información que se presentan.	
Se verifica si los Encargados del Tratamiento de la información personal cuentan con política de Tratamiento de datos personales y programas de formación o educación en temas de protección de datos para sus empleados.	
Se exige la realización de auditorías internas y/o externas a las actividades desarrolladas por el Encargado del Tratamiento.	
Existen acuerdos con los Encargados y sus empleados o colaboradores aceptando que cumplirán con las políticas y protocolos de Tratamiento de datos de su organización.	
Se exige a los Encargados que utilizan subcontratistas que se establezcan obligaciones para éstos de adherencia a las políticas de Tratamiento de la organización.	

COMUNICACIÓN EXTERNA	S/N
Se han implementados procedimientos para informar a los Titulares sus derechos.	
Se dirigen comunicaciones claras y comprensibles a los Titulares.	
Se cuenta con un área o persona encargada de la atención de las quejas y reclamos relacionados con el ejercicio del derecho de hábeas data.	
Se informa a los Titulares cuáles son los canales de atención que la organización tiene dispuestos para la presentación de sus reclamaciones o consultas.	

EVALUACIÓN Y REVISIÓN CONTINUA

PLAN DE SUPERVISIÓN Y REVISIÓN	S/N
Se ha desarrollado dentro de la organización un plan de supervisión y revisión anual del Programa Integral de Gestión de Datos Personales.	
El plan de supervisión y revisión implementado establece las medidas de desempeño e incluye un calendario para las revisiones de las políticas y los controles del Programa Integral de Gestión de Datos Personales, por lo menos una vez al año.	

EVALUACIÓN Y REVISIÓN DE LOS CONTROLES DEL PROGRAMA	S/N
Se revisan y evalúan periódicamente los controles establecidos para minimizar o evitar la materialización de los riesgos en el Tratamiento de datos personales.	
Los controles establecidos tienen en cuenta las nuevas amenazas, los motivos de las quejas más recientes presentadas por los Titulares, los hallazgos en las auditorías o las orientaciones de la autoridad de protección de datos.	
Se hace seguimiento a los servicios prestados por la organización que involucran recolección, uso, divulgación y, en general, cualquier Tratamiento de información personal para determinar que estén cumpliendo las políticas y procedimientos adoptados.	
Se realizan capacitaciones idóneas y acordes con las políticas y procedimientos dispuestos por la organización.	
La persona o área que asume la función de protección de datos personales controla y actualiza el inventario de información personal continuamente para identificar y evaluar nuevas recolecciones, usos y divulgaciones.	
La persona o área que asume la función de protección de datos personales revisa las políticas de acuerdo a los resultados de las evaluaciones o auditorías.	
La persona o área que asume la función de protección de datos personales mantiene como documentos históricos las evaluaciones de impacto y las de amenazas a la seguridad y riesgos.	

EVALUACIÓN Y REVISIÓN DE LOS CONTROLES DEL PROGRAMA	S/N
La persona o área que asume la función de protección de datos personales revisa y actualiza, en forma periódica, los programas de formación y educación para todos los empleados de la organización como resultado de evaluaciones continuas.	
La persona o área que asume la función de protección de datos personales revisa y adapta los protocolos de respuesta al manejo de violaciones e incidentes de seguridad e implementa las mejores prácticas y recomendaciones de las revisiones que se efectúan posterior a la ocurrencia de esos incidentes.	
La persona o área que asume la función de protección de datos personales revisa y, si es el caso, modifica los requisitos establecidos en los contratos suscritos por la organización con los Encargados del Tratamiento.	
La persona o área que asume la función de protección de datos personales actualiza y aclara las comunicaciones externas para explicar las políticas de Tratamiento de datos.	
La persona o área que asume la función de protección de datos personales reporta 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 Integral de Gestión de Datos Personales.	