1. **NOMBRE DEL INSTRUCTIVO:** Relacionamiento con Terceros Protección de Datos Personales
2. **PROCESO AL QUE PERTENECE:** Oficina de Seguridad de la Información
3. **UBICACIÓN Y COBERTURA DEL PROCEDIMIENTO:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NIVEL** |  |  | **COBERTURA** |  |
| Estratégico |  |  | Central |  |
| Misional |  |  | Nacional | **X** |
| Apoyo | **X** |  | Seccional |  |

1. **OBJETIVO**

Establecer las acciones para la debida diligencia en el relacionamiento con terceros encargados del tratamiento de datos personales de la Rama Judicial.

1. **MARCO NORMATIVO**
* Ley 270 de 1996 – Ley Estatutaria de la Administración de Justicia
* Ley 872 de 2003 – Creó el Sistema de Gestión de la Calidad en la Rama Ejecutiva y en otras entidades prestadoras de servicios
* Ley 1581 de 2012 – Por el cual se dictan disposiciones generales para la protección de datos personales.
* NTC-ISO-IEC 27001:2013 – Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos
* ACUERDO No. PSAA14-10161 (junio 12 de 2014) - “Por el cual se actualiza el Sistema Integrado de Gestión y Control de la Calidad creado mediante Acuerdo PSAA07-3926 de 2007 y se establece el Sistema Integrado de Gestión y Control de la Calidad y el Medio Ambiente – SIGCMA -”
* ACUERDO No. PSAA14-10279 (diciembre 22 de 2014) - “Por el cual se aprueban las políticas y procedimientos de Seguridad de la Información para la Rama Judicial”
1. **ALCANCE**

Este instructivo hace parte del manual de protección de datos personales y contiene la descripción de las actividades y lineamientos para el relacionamiento con terceros encargados del tratamiento en el marco de la acreditación de la diligencia demostrada. Para ello se han definido unos criterios de clasificación de los terceros según su nivel de criticidad respecto al volumen y naturaleza de los datos personales objeto de tratamiento. A partir de esta clasificación, se consagran las acciones sugeridas para la verificación de la existencia de un nivel adecuado de cumplimiento por parte del tercero encargado antes de realizar el proceso de formalización o perfeccionamiento del vínculo contractual.

1. **LIDER DEL PROCEDIMIENTO**

|  |  |
| --- | --- |
| **CARGO**  | **DEPENDENCIA**  |
| Oficial de Protección de Datos Personales | GPET – Oficina de Seguridad de la Información |

1. **RESPONSABLES DEL PROCEDIMIENTO**

|  |  |
| --- | --- |
| **CARGO**  | **DEPENDENCIA**  |
| Oficial de Protección de Datos Personales | GPET – Oficina de Seguridad de la Información |
| Profesional área jurídica |  |
| Profesionales de áreas requirentes de relacionamiento con terceros | Dependencia requirente de relacionamiento con terceros |

1. **PROVEEDORES E INSUMOS**

|  |  |
| --- | --- |
| **PROVEEDORES**  | **ENTRADA/INSUMOS EXTERNOS**  |
| Superintendencia de Industria y Comercio | Requerimientos para la responsabilidad demostrada |
| Profesionales de áreas requirentes de relacionamiento con terceros | Requerimiento de controles para la protección de datos personales durante el relacionamiento con un tercero.  |

1. **CONTROLES DEL PROCEDIMIENTO**

| **NOMBRE DEL CONTROL**  | **DESCRIPCIÓN DEL CONTROL**  |
| --- | --- |
| Manual de Políticas de Seguridad de la Información  | Objetivo de Control A18 – Cumplimiento |
| Manual de Protección de Datos Personales | Numeral 12. Relacionamiento con terceros |
| Lista de chequeo para verificar elementos mínimos de seguridad | Lista de chequeo que permite verificar al Oficial de Protección de Datos Personales los elementos mínimos de cumplimiento por parte del tercero, relacionados a la seguridad y protección de los datos personales.  |

1. **DESCRIPCIÓN DEL INSTRUCTIVO**

**PASO 1: Impartir directrices para el relacionamiento con tercero.** Como coordinador de todas las actividades relacionadas con la protección de datos personales al interior de la Rama Judicial, el Oficial de Protección de Datos Personales deberá impartir directrices para el relacionamiento con terceros cuyas actividades involucren el tratamiento de datos personales, para lo cual tomará en consideración los siguientes aspectos:

1. *Determinación de la tipología del tratamiento:* Las actividades de debida diligencia para el relacionamiento con terceros cuyas actividades impliquen tratamiento de información personal, dependerán de la tipología o clasificación del tratamiento que se realice en cada caso en particular en función de la sensibilidad o criticidad del tratamiento de datos involucrado, para lo cual, se tomarán en cuenta los siguientes criterios:
* Volumen de información: El volumen de información personal involucrada en la actividad de relacionamiento con un tercero será calificado.
* Naturaleza de la información: El tipo o naturaleza de información personal objeto de tratamiento será uno de los criterios de clasificación de los terceros cuyo relacionamiento involucre tratamiento de información personal. Para ello, se tomará en consideración las distintas tipologías o categorías descritas en el Sistema del Registro Nacional de Bases de Datos Personales, según se describe a continuación:
1. Datos generales.
2. Datos de identificación.
3. Datos de ubicación.
4. Datos de contenido socioeconómicos.
5. Datos Sensibles.
6. Otro tipo de datos.

Las actividades que involucren exclusivamente datos asociados a las tipologías (i) y (ii) de información, serán consideradas como actividades de ***tratamiento bajo***.

Las actividades que involucren tratamiento de cualquiera de las categorías previamente descritas a excepción de datos sensibles serán consideradas como actividades de ***tratamiento moderado***.

Las actividades que involucren tratamiento de algún tipo de dato personal considerado sensible o especial, así como aquellos relacionados con información de niños, niñas y adolescentes, serán consideradas como actividades de ***tratamiento intensivo***.

1. *Verificación previa del nivel de cumplimiento por parte del tercero:* Estos criterios de verificación deben aplicarse durante la etapa precontractual como condición para la selección y perfeccionamiento de una relación contractual o convencional con un proveedor o aliado cuyas actividades involucren tratamiento de datos personales. El Oficial de Protección de Datos Personales fijará los estándares mínimos que tendrán que cumplir los terceros cuyas actividades involucren una o varias actividades de tratamiento, para ser puestos a conocimiento de todas las áreas de la Rama Judicial.

El propósito de la lista de chequeo es el de listar los factores clave para la debida diligencia en la verificación de los requisitos mínimos de cumplimiento del tercero en función del nivel de criticidad y tipología del tratamiento. Por tanto, el Oficial de Protección de Datos Personales será el encargado de realizar la verificación formal o sustancial de los requisitos de cumplimiento del tercero de acuerdo a su clasificación, cuyas conclusiones deberán ser soportadas y documentadas en términos de viabilidad del relacionamiento o de forma excepcional; con la concertación, seguimiento y cierre de los planes de cumplimiento con el tercero que no alcance niveles mínimos para el cumplimiento adecuado de la ley de protección de datos personales.

1. *Definición de coberturas jurídicas:* El área jurídica de la Rama Judicial determinará con base en los lineamientos del Oficial de Protección de Datos Personales, las cláusulas, garantías y demás coberturas que deberán quedar plasmadas en el acuerdo para la formalización del relacionamiento con un tercero cuya actividad involucre tratamiento de información personal. Estos lineamientos serán definidos por el Oficial de Protección de Datos Personales a partir del mejor entendimiento y análisis del impacto a la privacidad que se realizará de forman conjunta con el área requirente y demás áreas de Rama Judicial.
2. *Supervisión del contrato:* La supervisión contractual es una labor de inspección e intervención oportuna de la ejecución del contrato, que, en el caso particular del tratamiento de los datos personales, está llamada a evitar y/o corregir infracciones a las obligaciones consagradas en la Ley 1581 de 2012, el Decreto Único 1074 de 2015 y las políticas internas de la Rama Judicial. Al tiempo que permite mitigar la exposición al riesgo sancionatorio o reputacional.

Por ende, el Oficial de Protección de Datos Personales definirá los parámetros para la supervisión del contrato que involucre una actividad de tratamiento de la información personal. El objetivo de la directriz interna que se imparta para la supervisión de los proveedores o aliados que presenten un servicio asociado con una actividad de tratamiento de la información, es el de monitorear el cumplimiento de las disposiciones legales y contractuales que obligan a estos sujetos.

1. *Disposición y/o devolución de la información personal al terminar el contrato*: El Oficial de Protección de Datos Personales de acuerdo con la naturaleza de la información personal, señalará los términos en los que deberá realizarse la devolución y/o disposición de los datos personales.

De acuerdo con la instrucción interna que imparta el Oficial de Protección de Datos Personales, quedará plasmado en el contrato como una obligación a cargo del tercero cumplir con cada uno de los requisitos técnicos de disposición y devolución de la información personal.

**PASO 2: Identificación de la necesidad de relacionamiento con tercero.** Cada área de Rama Judicial, de acuerdo con sus requerimientos particulares, definirá si la eventual necesidad de relacionamiento con un tercero ya sea mediante la selección o contratación de un proveedor, o mediante la suscripción de un convenio con un aliado, conlleva actividades que involucren tratamiento de datos personales, entendiendo por la realización de todas o alguna de las siguientes actividades:

|  |  |  |
| --- | --- | --- |
| Recolección | Imagen que contiene objeto, monitor, frente, firmar  Descripción generada automáticamente | Implica un contacto directo entre el tercero y el titular de la información personal, con el propósito de recolectar la información que la Rama Judicial requiera para fines judiciales, contractuales u otros. |
| Uso | Icono  Descripción generada automáticamente | Implica que el tercero utilizará la información personal según las finalidades dispuestas por la Rama Judicial. |
| Almacenamiento | Base de datos con relleno sólido | Implica que el tercero almacenará la información personal mediante sus propios medios técnicos o mediante infraestructura a cargo de otro tercero, tanto a nivel nacional como internacional. |
| Actualización |  | Implica que el tercero entre en contacto directo con el titular con el fin de actualizar la información previamente recolectada, o a modificar los datos almacenados según la información que le reporte la Rama Judicial. |
| Supresión o eliminación |  | Implica que el tercero asuma la responsabilidad de eliminar la información que sobre uno o varios titulares repose en una base de datos, según las indicaciones de la Rama Judicial.  |

**PASO 3: Definición del tipo de encargado del tratamiento de la información personal.** Una vez el área requirente identifique la necesidad de relacionamiento con un tercero cuya actividad involucre tratamiento de datos personales, el Oficial de Protección de Datos Personales procederá a clasificar el tipo o categoría de tratamiento con base en los criterios de volumen y naturaleza de información personal que será objeto de tratamiento por el tercero conforme a los lineamientos previamente descritos.

La clasificación de la tipología del tratamiento según la naturaleza y volumen de información personal obedece a una estrategia de relacionamiento que le permitirá a la Rama Judicial definir estándares mínimos de verificación para la mitigación de riesgos de incumplimiento en forma proporcional y razonable según el nivel de criticidad del relacionamiento teniendo en cuenta las siguientes tipologías:

|  |  |  |
| --- | --- | --- |
|  | Encargado con tratamiento intensivo de información | Manejan un gran volumen de información o datos de naturaleza sensible.  |
|  | Encargado con tratamiento moderado de información | Manejan un volumen moderado de información personal o cualquier tipo de información personal exceptuando datos sensibles. |
|  | Encargado con tratamiento bajo de información | Maneja un bajo volumen de información o datos personales exclusivamente asociado a información general o de identificación.  |

**PASO 4: Aplicación de la lista de chequeo como requisito previo para la contratación.** De acuerdo con la directriz que imparta el Oficial de Protección de Datos Personales sobre la materia, el encargado de cada área de relacionamiento con el tercero o en su defecto, el área encargada de las labores de compras o adquisiciones deberá solicitar al tercero la información y/o soportes necesarios que le permitan el cabal diligenciamiento de una lista de chequeo de verificación de elementos mínimos del cumplimiento de la ley de protección de datos personales.

El diligenciamiento de la lista de chequeo le permitirá a la Rama Judicial exigirle al tercero, cumplir con un mínimo de requisitos que aseguran un nivel adecuado de protección de la información personal tratada. Así mismo, determinar las coberturas jurídicas que deberán quedar pactadas en el contrato.

**PASO 5. Concertación de plan de cumplimiento:** Una vez realizado el proceso de calificación del tipo de tratamiento a cargo del tercero y aplicado el respectivo listado de chequeo de verificación de requisitos mínimos de cumplimiento de la ley, el Oficial de Protección de Datos Personales determinará la viabilidad o procedencia del relacionamiento con el tercero. No obstante, en el evento en que el tercero analizado no alcance niveles adecuados del cumplimiento de la ley de protección de datos personales, se podrá de forma excepcional concertar planes de cumplimiento específicos, a fin de garantizar la continuidad de la operación. Todo plan de cumplimiento debe ser documentado y concertado con el tercero, especificando los aspectos puntuales requeridos para alcanzar los niveles adecuados de cumplimiento, así como el término máximo otorgado para verificar su efectiva implementación.

**PASO 6. Definición de coberturas contractuales o convencionales.** El representante o delegado del área legal, procederá con el apoyo del delegado del área requirente y de conformidad con los lineamientos del Oficial de Protección de Datos Personales, a determinar las coberturas requeridas para la formalización del relacionamiento contractual o convencional con el tercero.

**PASO 7. Seguimiento y supervisión del contrato.** De acuerdo con las políticas de internas de la Rama Judicial, se designará una persona o área que realice la supervisión del contrato o convenio suscrito con el tercero que involucre tratamiento de datos personales. El supervisor del contrato será la persona responsable de verificar y acreditar que, durante la ejecución del contrato, el tercero cumple con los términos de la ley, el contrato o convenio y las políticas internas de la Rama Judicial. Por tanto, esta verificación implicará 2 aspectos centrales:

1. *Verificación permanente del cabal cumplimiento por parte del tercero de las obligaciones formales del régimen de protección de datos personales:* En línea con las instrucciones que imparta el Oficial de Protección de Datos Personales para la supervisión de las personas naturales o jurídicas que fungen como terceros que tratan información personal, el supervisor realizará auditorías y/o revisiones periódicas al cumplimiento de las obligaciones y compromisos contractuales o convencionales adquiridos por el tercero. Lo anterior en aras de verificar como mínimo el efectivo y oportuno cumplimiento:
* Las actividades de atención de consultas y reclamos tales como: actualización, eliminación y/o disposición, entre otros.
* De la efectiva gestión de la obtención de la autorización del tratamiento por parte de los titulares de información a través de los avisos de privacidad o solicitudes de autorización.

Al mismo tiempo, el supervisor deberá verificar que el tercero esté utilizando la información personal de acuerdo con las finalidades y parámetros definidos por la Rama Judicial.

1. *Ser el canal para el reporte de incidentes de seguridad y planes de mejora relacionados con la seguridad de la información.* El supervisor deberá informar al Oficial de Protección de Datos Personales todo incidente de seguridad del que tenga conocimiento, con el propósito de identificar el plan de acción a implementar por el tercero que ejecute una actividad de tratamiento de la información.

El supervisor, posterior al plan de acción y/o mejora que dictaminé el Oficial de Protección de Datos Personales, deberá informárselo a la persona natural o jurídica encargada del tratamiento. Así mismo, deberá verificar de manera periódica, según lo definido por el Oficial de Protección de Datos Personales, que las actividades que integran el plan de acción sean realizadas por el tercero en el tiempo y condiciones señaladas por la Rama Judicial.

Si durante el seguimiento se observa que el tercero no cumple con el plan de mejora, el supervisor deberá informar esta situación al Oficial de Protección de Datos Personales para que esté junto con el área jurídica evalúen la continuidad del contrato.

**PASO 8. Terminación del contrato.** Finalizado el contrato con ocasión a la ejecución de su objeto, el cumplimiento del término o el incumplimiento de las obligaciones a cargo del tercero; el supervisor verificará que este realice las labores técnicas y operativas asociadas a la devolución o disposición de la información en los términos acordados al momento de perfeccionar el relacionamiento con el tercero o en su defecto, a través de los mecanismos que defina el Oficial de Protección de Datos Personales.

1. **ANEXOS**

**Anexo I. LISTA DE CHEQUEO DE REFERENCIA PARA LA VERIFICACIÓN DE ELEMENTOS MÍNIMOS DE CUMPLIMIENTO PREVIA FORMALIZACIÓN DEL RELACIOAMIENTO CON TERCEROS**

A continuación, se indican los aspectos que deben contener las listas de chequeo que sean adoptadas por el Oficial de Protección de Datos Personales para la verificación de elementos mínimos de cumplimiento por parte del tercero en etapa previa a la formalización del relacionamiento según clasificación del tipo de tratamiento.

1. **Elementos de la lista de chequeo**
2. **Aspectos técnicos:** Hacen referencia a las herramientas mínimas que debe disponer toda organización para el tratamiento de los datos personales:
* *Política de seguridad de la información.* Directriz que tiene por objetivo la preservación de la confidencialidad, integridad y disponibilidad de la información de una organización. Entendida por información, todo conjunto de datos susceptible de valoración económica. Por ende, la política de información del proveedor que preste un servicio asociado con una actividad de tratamiento de la información personal deberá contener como mínimo los siguientes requisitos:
* Lineamientos generales para la clasificación de activos de la información. Permite la caracterización y clasificación de los activos de la información facilitan el proceso de identificación y control de riesgos asociados a la seguridad de la información.
* Estándares para el uso de los recursos de la información por empleados, contratistas y demás personas. Exige la definición de unos estándares mínimos para la utilización de recursos de la información que permitan la transmisión y/o almacenamiento a de la información por personal empleado o no.
* Lineamientos para la gestión del riesgo asociado con la seguridad de la información. Involucra la identificación, control y monitoreo continuo de los riesgos a los que están expuestos los activos de la información.
* Directrices para el acceso a la información. Comprende la caracterización de los usuarios de la información y los controles de acceso de acuerdo con su rol y función al interior.
* *Política de Protección de Datos Personales.* Adicional a los aspectos enunciados previamente, la política de protección de datos personales debe contener como mínimo los siguientes elementos:
* Caracterización de la información personal que es empleada por la organización y los controles asociados según la naturaleza de los datos personales.
* Lineamientos para el uso de la información personal de acuerdo las finalidades fijadas para cada escenario del tratamiento.
* *Procedimiento para la gestión de usuarios con acceso a la información personal.* Instructivo que define la clase de usuarios que tendrán acceso a la información personal conforme a su naturaleza, junto con las medidas de seguridad según el perfil de relacionamiento con los datos personales.
* *Procedimiento o control para la disposición final de la información personal.* Se entiende por disposición final de los datos personales su supresión, destrucción o archivo. Por tanto, el documento deberá detallar las actividades que deberán seguirse para realizar cualquiera de los fines previamente señalados.
* *Documentación de controles de seguridad de la información personal.* Directriz en la que se indique el conjunto mínimo de medidas de seguridad que deberán ser aplicadas al interior de la organización, dependiendo del nivel de protección que los datos personales requieran – alto, medio, bajo - según su naturaleza.
* *Política y procedimiento para la gestión de incidentes de seguridad de la información personal.* Documento que implemente los controles mínimos para gestión de incidentes de seguridad, presentes y futuros que tengan el potencial de afectar la integridad, confidencialidad y disponibilidad de la información personal. Así mismo, la definición de un procedimiento para el reporte de eventos y debilidades de seguridad a la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio y al Oficial de Protección de Datos Personales.
* *Política de auditorías de seguridad de la información personal.* Lineamientos encaminados a definir los objetivos y metodología para la revisión y evaluación del programa integral de gestión de datos personales.
1. **Aspectos organizacionales**
* *Oficial de Protección de Datos Personales.* Persona o área designada para la gestión de la información personal, encargada de coordinar las actividades que integran y desarrollan el programa integral de datos personales al interior de cada Organización.
* *Canales de atención al titular:* Comprende la habilitación de canales para la atención de consultas o reclamos de titulares de información. Toda organización deberá habilitar por lo menos una dirección de correo electrónico, una dirección física y un número telefónico (fijo o móvil), sin perjuicio de poder desarrollar o habilitar otro tipo de canales adicionales.
1. **Aspectos jurídicos**
* *Avisos de privacidad y/o solicitudes de autorización.* Como condición para el tratamiento de los datos personales, toda Organización debe poner a disposición de los titulares de la información, los avisos de privacidad y/o solicitudes de autorización con el lleno de los requisitos de ley.
* *Acuerdos de confidencialidad.* Toda Organización debe contar con una cláusula jurídica para empleados y/o contratista encaminada a salvaguardar y garantizar la confidencialidad de la información a la que tienen acceso personas naturales por razón a su condición de empleado o contratista*.*
* *Política de tratamiento de datos personales.* Toda Organización debe contar con una Política de tratamiento de datos personales acorde con las exigencias mínimas establecidas en la ley 1581 de 2012.
1. **CONTROL DE REGISTROS**

Ver tabla de retención documental validada por el Comité Nacional del SIGCMA.

1. **TÉRMINOS Y DEFINICIONES**

Los términos y definiciones se pueden observar en el documento *“Glosario del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y protección de Datos Personales”.*