POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

DIRECCIÓN DE CONECTIVIDAD E INFRAESTRUCTURA TECNOLÓGICA

2026

Tabla de contenido

POLITICA DE TRATAMIENTO DE DATOS PERSONALES

OBJETIVO

Establecer los lineamientos institucionales para garantizar la protección de los datos personales en la Gobernación del Departamento de Bolívar, en cumplimiento de la Ley 1581 de 2012, sus decretos reglamentarios y el Modelo de Seguridad y Privacidad de la Información (MSPI), mediante la implementación de un enfoque de gestión basado en riesgos, controles de seguridad de la información y mejora continua. Lo anterior, con el fin de asegurar el ejercicio efectivo de los derechos de los titulares de conocer, actualizar, rectificar y suprimir la información y preservar las propiedades de confidencialidad, integridad y disponibilidad de los datos, previniendo su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

ALCANCE

La presente Política de Tratamiento de Datos Personales aplica a todos los datos personales que reposen en bases de datos automatizadas, semiautomatizadas o físicas bajo la responsabilidad de la Gobernación del Departamento de Bolívar, y que sean objeto de cualquier operación de tratamiento conforme a la normativa vigente. Su cumplimiento es obligatorio para todos los funcionarios, contratistas, proveedores, aliados y demás grupos de interés que, en ejercicio de sus funciones, competencias u obligaciones contractuales, participen en la recolección, almacenamiento, uso, circulación o supresión de datos personales dentro de los procesos institucionales.

Acorde a lo anterior, esta política se integra al Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad, en concordancia con el Modelo de Seguridad y Privacidad de la Información (MSPI), adoptando un enfoque basado en riesgos, controles de seguridad y mejora continua. Por consiguiente, el tratamiento de datos personales se somete a la identificación, análisis, evaluación y tratamiento de riesgos de seguridad de la información, así como a la implementación de controles administrativos, técnicos y físicos orientados a preservar la confidencialidad, integridad y disponibilidad de la información.

OBLIGACIONES

La presente Política de Tratamiento de Datos Personales es de obligatorio y estricto cumplimiento por parte de la Gobernación del Departamento de Bolívar, en su calidad de responsable del tratamiento, así como para todos los servidores públicos, contratistas, proveedores y terceros que, en virtud de sus funciones u obligaciones contractuales, intervengan en cualquier fase del tratamiento de datos personales.

DOCUMENTOS DE REFERENCIA

El Plan de Seguridad y Privacidad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Ley No. 1341 de 2009 "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones"
- Decreto 235 de 2010 “por la cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas”
- CONPES No. 3701 del 2011 “Lineamientos de Políticas para la Ciberseguridad y Ciberdefensa”
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”
- Decreto Ley No. 19 de 2012 “Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública”
- Decreto No. 2364 de 2012 “Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones”
- Directiva Presidencial No. 004 de 2012 “Eficiencia Administrativa y lineamientos de la política cero papel en la administración pública”
- Decreto No. 1377 de 2013 “Reglamenta parcialmente la Ley 1581 de 2012”
- Ley No. 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”
- Decreto No. 886 de 2014 “Registro Nacional de Bases de Datos”

- Decreto No. 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"
- CONPES No. 3854 de 2016 “Política Nacional de Seguridad Digital”
- Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability) 2016
- Ley No. 1915 de 2018 “Por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos”
- Ley 1928 de 2018 “Por medio de la cual se aprueba el «Convenio sobre la Ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest”
- Decreto No. 531 de 2018 “Por el cual se adopta el Manual de Políticas y Procedimientos de Protección de Datos de la Gobernación de Bolívar y se dictan otras disposiciones”
- Decreto 612 de 2018, “*Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado*”, donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- Decreto No. 1008 de 2018 “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”
- Conpes No. 3920 de 2018 “Política Nacional de Explotación de Datos (Big Data)”
- Ley No. 1978 de 2019 “Por la cual se moderniza el sector de las tecnologías de la información y las comunicaciones -tic, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones”
- Decreto No. 2106 de 2019 “Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública”
- Conpes No. 3968 de 2019 “Declaración de importancia estratégica del proyecto de desarrollo, masificación y acceso a internet nacional, a través de la fase ii de la iniciativa de incentivos a la demanda de acceso a internet”
- Conpes No. 3975 de 2019 “Política Nacional de Transformación Digital e Inteligencia Artificial”
- CONPES No. 3995 de 2020 “Política Nacional de Confianza y Seguridad Digital”

- Resolución 247 de 2020 "*Por medio de la cual se adopta la actualización del Manual para la Administración del Riesgo de la Gobernación de Bolívar y se dictan otras disposiciones*"
- Resolución No. 1519 de 2020 "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos"
- Resolución No. 2160 de 2020 "Por la cual se expide la Guía de lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de estos"
- Resolución 500 de 2021. "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*".
- Conpes No. 4069 de 2021 "Política Nacional de Ciencia, Tecnología e Innovación 2022-2031"
- Directiva Presidencial No. 03 de 2021 "Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos"
- Decreto 767 de 2022 "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital…" del Ministerio de las Tecnologías de la información y las Comunicaciones.
- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas v6 de 2022
- Decreto No. 222 de 2022 "Por medio del cual se actualiza el Modelo Integral de Planeación y Gestión -MIPG en la Gobernación de Bolívar, establecido en el Decreto No. 169 de 2018 y Decreto 489 de 2018"
- Resolución No. 460 de 2022 "Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación"
- Decreto No. 1263 de 2022 "Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública"
- Resolución 261 de 2023 por medio de la cual "*se conforma el Comité de Seguridad de la Información, define sus Funciones y adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar*"

- Resolución No. 836 de 2023 "Por medio de la cual se modifica el artículo primero de la Resolución No. 261 de 24 de Marzo de 2023"
- Artículo 269ª al 269J del Código Penal Colombiano
- Artículo 270 al 272 del Código Penal Colombiano
- Decreto No. 297 de 2024 "Por medio del cual se establece la estructura de la administración del departamento de Bolívar, se dictan reglas sobre su organización y funcionamiento, se determina la estructura interna y funciones de las dependencias del sector central y se dictan otras disposiciones"
- Resolución 2277 de 2025 “Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia”.

TERMINOS Y DEFINICIONES

Para efectos de entendimiento de la presente política de tratamiento de datos personales, es importante tener en cuenta los siguientes términos y definiciones:

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000) (Ministerio de Tecnologías de la Información y las Comunicaciones, 2015b).

Amenaza: Causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema u organización. (International Organization for Standardization, 2016) **Análisis de riesgo:** Proceso para comprender la naturaleza del riesgo y para determinar su nivel. El análisis de riesgos proporciona la base para la evaluación del riesgo y las decisiones sobre el tratamiento del riesgo. El análisis de riesgo incluye estimación de riesgo. (International Organization for Standardization, 2016).

Ataque: Intento de destruir, exponer, alterar, inhabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo de información. (International Organization for Standardization, 2016).

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales. (Ley 1581 de 2012 Artículo 3°. Definiciones).

Aviso de privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la

existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales. (Decreto 1377 de 2013. Artículo 3°. Definiciones).

Base de datos: Conjunto organizado de datos personales que sea objeto de tratamiento. (Ley 1581 de 2012 Artículo 3°. Definiciones).

Causahabiente: Persona que ha sucedido a otra por causa del fallecimiento de ésta (heredero).

Confidencialidad: Propiedad que la información no esté disponible o sea revelada a personas, entidades o procesos no autorizados. (International Organization for Standardization, 2016)
Contraseña: Una cadena de caracteres (Letras, números y otros símbolos) usadas para identificar y autenticar o verificar autorización de acceso. (NIST, 2017)

Control: Mecanismo que modifica el valor de un riesgo. Los controles incluyen cualquier proceso, política, dispositivo, práctica u otras acciones que modifiquen el riesgo. Los controles no siempre ejercen el efecto modificador previsto o asumido. (International Organization for Standardization, 2016).

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables**.** (Ley 1581 de 2012 Artículo 3°. Definiciones).

Dato público: Es el dato que no sea semiprivado, privado o sensible. 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. (Decreto 1377 de 2013. Artículo 3°. Definiciones).

Datos sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos. (Ley 1581 de 2012 Artículo 3°. Definiciones).

Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen

racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013. Artículo 3°. Definiciones).

Detectar: Descubrir la existencia de algo que no era patente. (Real Academia Española, 2019a)
Disponibilidad: Propiedad de ser accesible y utilizable a petición de una entidad autorizada. (International Organization for Standardization, 2016).

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. (Ley 1581 de 2012 Artículo 3°. Definiciones).

Evaluación del riesgo: Proceso de comparar los resultados del análisis de riesgo con los criterios de riesgo para determinar si es aceptable o tolerable la magnitud del riesgo. La evaluación del riesgo ayuda a la decisión sobre el tratamiento del riesgo. (International Organization for Standardization, 2016).

Evento de seguridad de la información: Acontecimiento identificado en el estado de un sistema, servicio o red que indica una posible violación a la política de seguridad de la información o fallo de los controles o una situación previamente desconocida que puede ser relevante para la seguridad. (International Organization for Standardization, 2016).

Gestión de incidentes de seguridad de la información: Proceso para detectar, informar, evaluar, responder ante los incidentes de seguridad, mitigarlos y aprender de ellos. (International Organization for Standardization, 2016).

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos. (International Organization for Standardization, 2016).

Identificar: Reconocer si una persona o cosa es la misma que se supone o se busca. (Real Academia Española, 2019b).

Identificación del riesgo: Proceso de encontrar, reconocer y describir los riesgos. La identificación del riesgo implica la identificación de fuentes de riesgo, eventos, sus causas y sus potenciales consecuencias. La identificación de riesgos puede incluir datos históricos, análisis teóricos, opiniones informadas y de expertos y necesidades de los interesados. (International Organization for Standardization, 2016).

Incidente de seguridad de la información: Evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer de manera negativa las operaciones de la empresa y amenazar la seguridad de la información. (International Organization for Standardization, 2016).

Integridad: Propiedad de la exactitud y completitud de la información. (International Organization for Standardization, 2016).

Líder: Gobernador, Secretario(a), Director(s), Jefe(a)

MSPI: Modelo Seguridad y Privacidad de la Información.

Monitoreo: Determinación del estado de un sistema, proceso o una actividad. (International Organization for Standardization, 2016).

Política: Intenciones y directrices de una organización expresada formalmente por su alta dirección. (International Organization for Standardization, 2016).

Proceso de gestión del riesgo: Aplicación sistemática de políticas de gestión, procedimientos y prácticas a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión de los riesgos. (International Organization for Standardization, 2016).

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. (Ley 1581 de 2012 Artículo 3°. Definiciones).

Riesgo: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado positiva o negativamente. La incertidumbre es el estado total o parcial de la insuficiencia de la información relacionada con la comprensión o el conocimiento de un evento, su consecuencia o probabilidad. (…). En el contexto de la seguridad de la información, los sistemas de gestión, los riesgos de la seguridad de la información pueden expresarse como efecto de la incertidumbre en los objetivos de la seguridad de la información. El riesgo de seguridad de la información se asocia con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daño a una organización. (International Organization for Standardization, 2016).

Riesgo residual: Riesgo restante después de realizado tratamiento. (International Organization for Standardization, 2016).

Seguridad de la información: Preservación de la confidencialidad, disponibilidad e integridad de la información. (International Organization for Standardization, 2016).

Titular: Persona natural cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012 Artículo 3°. Definiciones).

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. (Decreto 1377 de 2013. Artículo 3°. Definiciones).

Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable. (Decreto 1377 de 2013. Artículo 3°. Definiciones).

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012 Artículo 3°. Definiciones).

Tratamiento de riesgo: Proceso para modificar el valor del riesgo. El tratamiento del riesgo puede incluir lo siguiente:

- Evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo.
- Tomar o aumentar el riesgo para poder aprovechar una oportunidad.
- Eliminación de la fuente de riesgo.
- Cambiar la probabilidad.
- Modificar las consecuencias.
- Compartir el riesgo con otra parte o partes.
- Asumir el riesgo mediante una elección informada.

Los tratamientos de riesgo que se ocupan de las consecuencias negativas se denominan a veces "mitigación del riesgo", "eliminación del riesgo", "prevención del riesgo" y "reducción del riesgo". El tratamiento de riesgos puede crear nuevos riesgos o modificar los riesgos existentes. (International Organization for Standardization, 2016).

Valoración de riesgo: Es el proceso global de la identificación del riesgo, el análisis de riesgo y la evaluación del riesgo. (International Organization for Standardization, 2016). **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (International Organization for Standardization, 2016).

GENERALIDADES

La Ley de Protección de Datos Personales reconoce y garantiza el derecho fundamental de hábeas data, en virtud del cual todas las personas pueden conocer, actualizar, rectificar y, cuando sea procedente, suprimir la información que sobre ellas repose en bases de datos o archivos susceptibles de tratamiento por entidades de naturaleza pública o privada. Este marco normativo establece las condiciones, principios y deberes que deben observar los responsables y encargados del tratamiento para asegurar una gestión legítima, segura y transparente de los datos personales.

En este sentido, la normativa colombiana dispone que el tratamiento de datos personales debe realizarse respetando los derechos de los titulares y aplicando los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. Tal como señala la Ley 1581 de 2012, esta tiene por objeto “desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas” (República de Colombia, 2012, art. 1).

Asimismo, en el ámbito del sector público, la adecuada protección de los datos personales se articula con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y con los sistemas de gestión de seguridad de la información, los cuales promueven un enfoque preventivo basado en la gestión de riesgos y la mejora continua para salvaguardar la confidencialidad, integridad y disponibilidad de la información institucional (MinTIC, 2016).

PRINCIPIOS RECTORES

En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios. (Ley 1581 de 2012 Artículo 4°. Principios para el Tratamiento de datos personales):

a) ***Principio de legalidad en materia de tratamiento de datos****:* El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.
b) ***Principio de finalidad****:* El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

c) ***Principio de libertad**:* El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

d) ***Principio de veracidad o calidad**:* La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

e) ***Principio de transparencia**:* En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

f) ***Principio de acceso y circulación restringida**:* el tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la Ley 1581 de 2012, sus decretos reglamentarios y la constitución. En este sentido, el tratamiento solo podrá hacerse por personas que hayan sido autorizadas por parte del titular, en el caso de menores de edad, por sus representantes y/o por las personas previstas en la presente Ley.

   Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, excepto que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la Ley 1581 de 2012.

g) ***Principio de seguridad**:* la información sujeta a tratamiento por EL RESPONSABLE o encargado del tratamiento a que se refiere la Ley 1581 de 2012 y sus decretos reglamentarios, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

h) ***Principio de confidencialidad**:* todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos, están obligadas a garantizar la reserva de la información, por lo que se comprometen a conservar y mantener de manera estrictamente confidencial y no revelar a terceros, toda la información que llegaren a conocer en la ejecución y ejercicio de sus funciones; salvo cuando se trate de actividades autorizadas expresamente por la Ley de protección de datos. Esta obligación persiste y se mantendrá inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento de datos personales.

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

La Gobernación del Departamento de Bolívar, en su calidad de Responsable del Tratamiento de Datos Personales, adopta la presente Política de Tratamiento de Datos Personales con el propósito de consolidar un marco institucional de confianza ciudadana que garantice el ejercicio efectivo de los derechos de los titulares. En atención a la relevancia de la protección de la información personal, la entidad implementa, mantiene, monitorea, revisa y mejora de manera continua un Programa Integral de Gestión de Datos Personales.

En este sentido, dicho programa se desarrolla bajo un enfoque de responsabilidad demostrada, gestión de riesgos y mejora continua, en estricto cumplimiento de la Ley Estatutaria 1581 de 2012 y sus decretos reglamentarios, así como en armonía con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI). Conforme al marco normativo colombiano, el responsable del tratamiento debe adoptar medidas que permitan “garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data” (República de Colombia, 2012, art. 17).

INFORMACIÓN GENERAL DE LA ENTIDAD – RESPONSABLE

- **Nombre o razón social**: Departamento de Bolívar.
- **NIT**: 890.480.059-1
- **Dirección**: Vía Cartagena – Turbaco, km 3, sector Bajo Miranda, El Cortijo.
- **Municipio**: Turbaco – Bolívar.
- **Teléfono**: (57)-(605) 6549216 Ext. 1202
- **Sitio WEB**: www.bolivar.gov.co
- **Correo electrónico**: contactenos@bolivar.gov.co

DEBERES DEL RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES.

Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad (LEY ESTATUTARIA 1581 DE 2012. Artículo 17. Deberes de los Responsables del Tratamiento):

a) Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

b) Solicitar y conservar, en las condiciones previstas en la ley, copia de la respectiva autorización otorgada por el titular.

c) Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

e) Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

f) Actualizar la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.

h) Suministrar al encargado del tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.

i) Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.

j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.

k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos.

l) Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

m) Informar a solicitud del titular sobre el uso dado a sus datos.

n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

o) Cumplir las instrucciones y requerimientos que imparta la superintendencia de industria y comercio.

DEBERES DE LOS ENCARGADOS DEL TRATAMIENTO

Los encargados del tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad (LEY ESTATUTARIA 1581 DE 2012. Artículo 18. Deberes de los Encargados del Tratamiento):

- **a)** Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- **b)** Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- **c)** Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.
- **d)** Actualizar la información reportada por los responsables del tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
- **e)** Tramitar las consultas y los reclamos formulados por los titulares en los términos señalados en la presente ley.
- **f)** Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los titulares.
- **g)** Registrar en la base de datos la leyenda “reclamo en trámite” en la forma en que se regula en la presente ley.
- **h)** Insertar en la base de datos la leyenda “información en discusión judicial” una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
- **i)** Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la superintendencia de industria y comercio.
- **j)** Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
- **k)** Informar a la superintendencia de industria y comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
- **l)** Cumplir las instrucciones y requerimientos que imparta la superintendencia de industria y comercio.

PARÁGRAFO. En el evento en que concurran las calidades de responsable del tratamiento y encargado del tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno.

DERECHOS DEL TITULAR DE LOS DATOS PERSONALES

El Titular de los datos personales tendrá los siguientes derechos (LEY ESTATUTARIA 1581 DE 2012. Artículo 8. Derechos de los Titulares):

a) Conocer, actualizar y rectificar sus datos personales frente a los responsables del tratamiento o encargados del tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
b) Solicitar prueba de la autorización otorgada al responsable del tratamiento salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley.
c) Ser informado por el responsable del tratamiento o el encargado del tratamiento, previa solicitud, respecto del uso que les ha dado a sus datos personales.
d) Presentar ante la superintendencia de industria y comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen.
e) Revocar la autorización y/o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la superintendencia de industria y comercio haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a esta ley y a la constitución.
f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

TRATAMIENTO DE DATOS PERSONALES

El Tratamiento de los Datos Personales de funcionarios, proveedores, contratistas, ciudadanos y demás interesados por parte del RESPONSABLE, garantizará los derechos a la privacidad, la intimidad, el buen nombre y la autonomía de los titulares y en consecuencia todas sus actuaciones se regirán por los principios rectores.
La recolección, almacenamiento, uso, circulación para:

- Gestionar trámites (solicitudes, quejas, reclamos).
- Ejercicio de las funciones legales y misionales.

TRATAMIENTO DE DATOS SENSIBLES

Se prohíbe el tratamiento de datos sensibles, excepto cuando (LEY ESTATUTARIA 1581 DE 2012. Artículo 6°. Tratamiento de datos sensibles):

a) El titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
b) El tratamiento sea necesario para salvaguardar el interés vital del titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
c) El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del titular.
d) El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
e) El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

Derechos de los niños, niñas y adolescentes (LEY ESTATUTARIA 1581 DE 2012. Artículo 7°. Derechos de los niños, niñas y adolescentes):

En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.
Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.
Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y

adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás. El Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta ley.

En consonancia con la necesidad de establecer medidas de seguridad reforzada, especiales y más robustas respecto de las bases de datos que contengan datos sensibles y menores de edad:

- Las dependencias realizarán los procesos de gestión de la seguridad de la información, identificación de activos, análisis de riesgo, establecimiento de controles de seguridad digital, verificación de efectividad de controles y realizarán los correctivos correspondientes.
- En la identificación de activos para las bases de datos con datos sensibles o que contengan datos de menores de edad se establecerá la criticidad alta.
- En el análisis de riesgo para las bases de datos con datos sensibles o que contengan datos de menores de edad se establecerá el impacto Catastrófico.
- Finalmente, se establecerán controles con base en el análisis de riesgo.

FINALIDAD DEL TRATAMIENTO DE DATOS PERSONALES.

La Gobernación del Departamento de Bolívar manejará los datos personales atendiendo a un estricto cumplimiento de las leyes aplicables para:

- Fines administrativos propios.
- Atender o formalizar trámites o servicios solicitados por parte de los titulares.
- Realizar encuestas, estadísticas, invitaciones o convocatorias diseñadas para la mejora en la prestación de servicios.
- Informar o promocionar servicios y campañas de interés general.
- Recopilar información de los asistentes a capacitaciones y eventos desarrollados por la entidad.
- Cualquier otro tipo de finalidad que se pretenda dar a los datos personales, será informado previamente, en el aviso de privacidad y en la respectiva autorización otorgada por el titular del dato, según sea el caso, y siempre teniendo en cuenta los principios rectores para el tratamiento de los datos personales, establecidos por la Ley, el presente documento y las demás normas que desarrollen la materia.

AUTORIZACIONES TRATAMIENTO DE DATOS PERSONALES

Atendiendo el Artículo 10 de la Ley 1581 del 2012: "*La autorización del titular no será necesaria cuando se trate de:*

- *Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.*
- *Datos de naturaleza pública.*
- *Casos de urgencia médica o sanitaria.*
- *Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.*
- *Datos relacionados con el Registro Civil de las Personas.*
- *Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley."*

ATENCIÓN DE PETICIONES, CONSULTAS Y RECLAMOS.

De acuerdo a lo estipulado en el Decreto 531 de 2018 "*Por la cual se adopta el Manual de Políticas y Procedimientos de Protección de Datos de la Gobernación de Bolívar y se dictan otras disposiciones*", la Secretaría de las Tecnologías de la Información y de las Comunicaciones, es el responsable asignado de la atención de peticiones, consultas, quejas y reclamos por la cual el titular de los datos personales podrá ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y/o revocar la autorización.

A su vez la Secretaría de las Tecnologías de la Información y de las Comunicaciones, como líder de protección de datos, actuará como oficial de protección de datos presto para dar cumplimento a los lineamientos establecidos en la presente política, a través de los siguientes medios habilitados para la presentación de peticiones, consultas y reclamos:

- Oficina de atención al ciudadano: Vía Cartagena – Turbaco, km 3, sector Bajo Miranda, El Cortijo.
- Teléfono: (57)-(605) 6549216 Ext. 1202
- Sitio web: www.bolivar.gov.co
- Correo electrónico protecciondedatos@bolivar.gov.co

PROCEDIMIENTO PARA EJERCER LOS DERECHOS COMO TITULAR DE LOS DATOS PERSONALES

La Gobernación del Departamento de Bolívar, Responsable del Tratamiento en cumplimiento de las normas sobre protección de datos personales presenta el procedimiento y requisitos mínimos para el ejercicio de sus derechos:

Para gestionar y dar respuesta eficiente a su PQRSD es necesario tener los siguientes datos:

- Nombre completo
- número de identificación
- Dirección física y/o electrónica
- Teléfonos de contacto
- Medios para recibir respuesta a su solicitud
- Motivo(s)/hecho(s) que dan lugar al reclamo con una breve descripción del derecho que desea ejercer (conocer, actualizar, rectificar, solicitar prueba de la autorización otorgada, revocarla, suprimir, acceder a la información)
- Firma

El Responsable tiene el deber de responder en los siguientes términos según la Ley Estatutaria 1581 de 2012:

Artículo 14. Consultas. *Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en cualquier base de datos, sea esta del sector público o privado. El Responsable del Tratamiento o Encargado del Tratamiento deberán suministrar a estos toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular.*

La consulta se formulará por el medio habilitado por el Responsable del Tratamiento o Encargado del Tratamiento, siempre y cuando se pueda mantener prueba de esta.

La consulta será atendida en un término máximo de diez (10) días hábiles *contados a partir de la fecha de recibo de esta. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.*

Artículo 15. Reclamos. El Titular o sus causahabientes que consideren 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 esta ley, podrán presentar un reclamo ante el Responsable del Tratamiento o el Encargado del Tratamiento el cual será tramitado bajo las siguientes reglas:

1. El reclamo se formulará mediante solicitud dirigida al Responsable del Tratamiento o al Encargado del Tratamiento, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

2. Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo de este, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

3. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

SEGURIDAD DE LA INFORMACIÓN

En consonancia con lo dispuesto en el Conpes 3854 Política Nacional de Seguridad Digital, cuyo objetivo general es "*que los colombianos y las empresas conozcan e identifiquen los riesgos a los que están expuestos en el entorno digital y aprendan como protegerse, prevenir y reaccionar ante los delitos y ataques cibernéticos.*" En sus dimensiones de confidenciad, integridad y disponibilidad, la Gobernación del Departamento de Bolívar adoptará buenas prácticas de seguridad de la información minimizando los riesgos de adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

La Gobernación del Departamento de Bolívar realizará copias de respaldo de información de todas las bases de datos que contengan datos personales.

Las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los datos personales están basadas en el Plan de Tratamiento de Riesgos de la Información, en el Programa Integral de Gestión de Datos Personales, el Plan de Seguridad y Privacidad de la Información y se encuentran consignadas en las Políticas de Seguridad Informática de la Gobernación de Bolívar.

REGISTRO NACIONAL DE BASES DE DATOS

La Gobernación del Departamento de Bolívar procederá a realizar el registro de sus bases de datos, ante el Registro Nacional de Bases de Datos (RNBD) que es administrado por la Superintendencia de industria y comercio, conforme lo estipulado en el Decreto 886 de 2014 "*Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos*"

RESPONSABLES

1. Gobernador del Departamento de Bolívar - Representante Legal
2. Comité de Seguridad de la Información - Seguimiento y Aprobación de documentos
3. Dirección de Conectividad e Infraestructura Tecnológica - Secretaria TIC. (Diseño e Implementación).
4. Dependencias (Implementación y cumplimiento).

APROBACIÓN Y REVISIONES A LA POLÍTICA

La presente política se revisa anualmente, o antes si existiesen cambios relevantes en el contexto interno y externo que afecten el logro de los objetivos institucionales y de seguridad de la información gestionada por la entidad con el objeto de mantener la política oportuna, eficaz y suficiente.

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección y el comité de seguridad de la información de la Gobernación del Departamento de Bolívar con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

Esta política será efectiva desde su aprobación por el Comité de Seguridad digital de la Gobernación de Bolívar.

La revisión de esta política se hará en las siguientes condiciones:

1. Anualmente se deberá revisar la efectividad de la política y sus objetivos.
2. Extraordinariamente ante cambios estructurales en la Entidad.
3. Extraordinariamente ante incidentes de seguridad de la información que requieran que la política que ameriten cambios de la política vigente.

CONTROL DE CAMBIOS

CONTROL DE CAMBIOS			
Fecha	Autor	Versión	Cambio
Enero 26 de 2024	Tairo Mendoza Piedrahita Profesional Especializado Dirección TIC	1.0	• Versión Inicial
Febrero 26 de 2026	Robinson Domínguez Reyes **Cargo:** Profesional Especializado Lizeth Gómez Padilla **Cargo:** Asesora Externa Dirección TIC	2.0	• Actualización de responsables y contacto. • Integración al nuevo Modelo de Seguridad y Privacidad de la Información-MSPI

ELABORÓ	**REVISÓ**	**APROBÓ**
Robinson Domínguez Reyes **Cargo:** Profesional Especializado Lizeth Gómez Padilla **Cargo:** Asesora Externa **25/02/2026**	Laura Abuchar Camacho **Cargo:** Directora de Conectividad e Infraestructura Tecnológica **26/02/2026**	**Nombre**: Comité de Seguridad digital de la Gobernación de Bolívar **Fecha**: Marzo 10 de 2026


AB ORDINE LIBERTAS
GOBERNACIÓN
DE BOLÍVAR