POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION ISO/IEC 27001:2022.

GOBERNACIÓN DE BOLÍVAR

DIRECCIÓN DE CONECTIVIDAD E INFRAESTRUCTURA TECNOLÓGICA

2026

TABLA DE CONTENIDO

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

La Gobernación de Bolívar reconoce que los datos y activos digitales son recursos estratégicos para garantizar la transparencia, la eficiencia administrativa y la confianza ciudadana. En un contexto de transformación digital y de creciente exposición a riesgos tecnológicos, la seguridad y privacidad de la información se consolidan como pilares fundamentales para el cumplimiento de la misión institucional.

La presente Política de Seguridad y Privacidad de la Información establece los lineamientos que orientan la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), en armonía con el Modelo de Seguridad y Privacidad de la Información (MSPI), la norma ISO/IEC 27001:2022 y el marco normativo nacional vigente, entre ellos la Ley 1581 de 2012 sobre protección de datos personales, la Ley 1712 de 2014 de transparencia y la Ley 527 de 1999 en materia de transacciones y comercio electrónico.

Este marco busca no solo preservar la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información, sino también impulsar la innovación digital segura, asegurar la continuidad del servicio público y fortalecer la cultura organizacional en torno a la seguridad digital.

OBJETIVO

Establecer los lineamientos estratégicos definidos por la Alta Dirección de la Gobernación de Bolívar para garantizar la Seguridad y Privacidad de la Información, mediante la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) alineado al Modelo de Seguridad y Privacidad de la Información (MSPI), las políticas de Seguridad Digital y Gobierno Digital, así como los requisitos legales aplicables y las necesidades de las partes interesadas.

DEFINICIONES/GLOSARIO

A continuación, se presentan los términos y definiciones que servirán de referencia para el desarrollo de la gestión de riesgos de Seguridad de la Información:

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).

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).

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).

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).

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).

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).

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Gobernación de Bolívar, reconociendo la relevancia de los activos de información para el cumplimiento de su misión y visión institucional, establece una Estrategia de Seguridad Digital y adopta el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones. En este marco, implementa, mantiene y mejora de manera continua un Sistema de

Gestión de Seguridad de la Información (SGSI), con el propósito de fortalecer la confianza ciudadana en el ejercicio de la función pública.

De esta manera, la Entidad no solo protege la confidencialidad, integridad y disponibilidad de los activos de información, sino que también garantiza la transparencia, el acceso oportuno y el uso responsable de la información pública, en cumplimiento de la Ley 1712 de 2014 y en coherencia con los lineamientos de la Política de Gobierno Abierto

Para la Gobernación de Bolívar resulta indispensable la protección sistemática de la información, mediante la gestión de riesgos derivados de amenazas internas y externas, mitigando sus impactos sobre los activos y manteniendo niveles de exposición aceptables que permitan cumplir la misión y visión institucional, en coherencia con las necesidades de los diferentes grupos de interés.

La Gobernación de Bolívar en su propósito de dar cumplimiento con la política de seguridad y privacidad de la información, establece los siguientes objetivos:

OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Fortalecer la cultura de seguridad y privacidad de la información en la Entidad, mediante procesos de sensibilización y capacitaciones que promuevan buenas prácticas, el cumplimiento de las políticas institucionales y la prevención de incidentes de seguridad de la información.
2. Establecer y actualizar políticas, procedimientos e instructivos de seguridad y privacidad de la información que garanticen el cumplimiento normativo y la gestión efectiva del SGSI.
3. Minimizar los riesgos de seguridad y privacidad de la información mediante la implementación y seguimiento de los controles definidos en el plan de tratamiento de riesgos.
4. Fortalecer la mejora continua del SGSI mediante el seguimiento periódico de la Matriz de Seguridad y Privacidad de la Información, evaluando la eficacia de los controles y promoviendo acciones de mejora.
5. Implementar y mantener controles tecnológicos básicos y eficaces que garanticen la protección de los activos de información institucional, la continuidad de los servicios digitales y la seguridad de los datos personales.

CONTEXTO DE LA ORGANIZACIÓN Y PARTES INTERESADAS.

En cumplimiento con la norma ISO/IEC 27001:2022, la Gobernación del Departamento de Bolívar identifica y evalúa el contexto interno y externo que afecta la seguridad de la información. Asimismo, se reconocen las partes interesadas (ciudadanía, servidores públicos, contratistas, proveedores tecnológicos y entes de control), garantizando que sus necesidades y expectativas sean consideradas en el marco del Sistema de Gestión de Seguridad de la Información (SGSI).

GESTIÓN DE RIESGOS Y OPORTUNIDADES

El SGSI no solo gestiona riesgos asociados a la seguridad de la información, sino también identifica y aprovecha oportunidades que fortalezcan la transformación digital, la innovación tecnológica y la confianza ciudadana. Este enfoque asegura el cumplimiento de los objetivos estratégicos y misionales de la entidad.

COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de la Gobernación de Bolívar mediante la Resolución 261 de 2023 "*Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar*" en su Artículo 13 se compromete a "*Establecer un Sistema de Gestión de Seguridad de la Información (SGSI) y adóptese el Modelo de Seguridad y Privacidad de la Información (MSPI) como lineamiento de la Estrategia de Seguridad Digital*", así mismo, mediante el Plan de Seguridad y Privacidad de la Información se compromete a revisar el avance de la implementación del SGSI de manera periódica y garantizará los recursos para implementar y mantener el sistema, así mismo, incluirá dentro de las decisiones estratégicas la seguridad de la información.

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La presente Política de Seguridad y Privacidad de la Información de la Gobernación de Bolívar aplica a todos los procesos, dependencias, sistemas de información, servicios y activos de información, tanto en formato físico como digital, que se generan, reciben, procesan, transmiten, almacenan o gestionan en el marco de la función pública.

Este alcance comprende:

- Procesos institucionales: estratégicos, misionales, de apoyo y de evaluación.
- Activos de información: datos, documentos, registros, sistemas, aplicaciones, infraestructura tecnológica y servicios digitales.
- Grupos de interés: ciudadanía, servidores públicos, contratistas, proveedores tecnológicos y entes de control.

De esta forma, la política se articula con el Sistema de Gestión de Seguridad de la Información (SGSI) y con el Manual de Administración de Riesgos de la Gobernación de Bolívar, garantizando la gestión integral de los riesgos de seguridad digital, de gestión y demás concernientes con el fin de apoyar el cumplimiento de la misión institucional.

APLICABILIDAD

La presente política, junto con sus objetivos, lineamientos, manuales, procedimientos e instructivos derivados, es de obligatorio cumplimiento para todas las personas y actores que, de manera directa o indirecta, gestionen o tengan acceso a la información de la Gobernación de Bolívar.

En particular, aplica a:

- Servidores públicos de planta y de libre nombramiento y remoción.
- Contratistas, practicantes y consultores, en el marco de sus actividades y obligaciones contractuales o académicas.
- Proveedores tecnológicos y terceros aliados, que suministren bienes, servicios o soluciones que impliquen el uso o tratamiento de la información de la entidad.
- Ciudadanía y grupos de interés, en la medida en que interactúen con los sistemas de información, trámites y servicios digitales de la Gobernación.

Todos los actores mencionados deben garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información bajo su responsabilidad, actuando en coherencia con las Políticas de Gobierno Digital y Seguridad Digital, el SGSI y la normativa legal vigente.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES).

La Gobernación de Bolívar, define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados (Manuales, Procedimientos, Formatos etc.…):

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN
Alta Dirección (Gobernador, Consejo de Gobierno)	Proporcionar los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información (Recursos económicos, formación y recursos tecnológicos).
Comité Institucional de Gestión y Desempeño	*Conforme a las funciones asignadas en el **Decreto 169 de 2018**:* ***"ARTÍCULO 9o.- FUNCIONES DEL COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO**: El Comité Institucional de Gestión y Desempeño, cumplirá las siguientes funciones:* ***6.** Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información."* *Modificadas parcialmente por el **Decreto 489 de 2018**:* *"**Artículo 2**".- MODIFIQUESE el artículo 5 de las funciones del Comité Institucional de Gestión y Desempeño, el cual en lo sucesivo quedará así:* *…**En materia de Antitrámites y de Gobierno Digital:*** ***…II. En materia de Gobierno Digital:*** 1. *Ser la instancia responsable del liderazgo, planeación e impulso de la Estrategia de Gobierno Digital en la entidad y canal de comunicación con la institución responsable de coordinar la Estrategia de Gobierno Digital, con la Comisión Interinstitucional de Políticas y de Gestión de la Información para la Administración Pública (COINFO) y de los demás grupos de trabajo relacionados con la transformación y modernización de la administración pública, apoyados en el aprovechamiento de la tecnología.* 2. *Definir los mecanismos para dar cumplimiento a la normatividad relacionada con el Gobierno Digital.* 3. *Liderar, bajo los lineamientos de la Estrategia de Gobierno Digital, la elaboración del diagnóstico y la elaboración y seguimiento al plan de acción de Gobierno Digital de la entidad.* 4. *coordinar y articular la Estrategia de Gobierno Digital en el departamento de Bolívar.* 5. *Incorporar el aprovechamiento de las TIC en las acciones de racionalización de trámites, atención efectiva al ciudadano y acompañar a los demás grupos conformados al interior de la entidad, tales como calidad y control interno.* 6. *identificar las barreras normativas para la provisión de trámites y servicios en línea y propender por levantar dichos obstáculos, de manera que puedan ser prestados por medios electrónicos.* 7. *Definir los lineamientos para la implementación efectiva de políticas y estándares asociados, como la política de actualización del sitio Web (donde deberán estar involucradas las diversas áreas, direcciones y/o programas de la entidad), política de uso aceptable de los servicios de Red y de internet, política de servicio por medios electrónicos, política de privacidad y condiciones de uso y política de seguridad del sitio Web, entre otros.* 8. *Definir e implementar el esquema de vinculación de la entidad a la Intranet Gubernamental y cada uno de sus componentes.* 9. *Definir y generar incentivos y/o estímulos para el uso de los servicios de Gobierno Digital por parte de los ciudadanos, las empresas y la entidad misma.* 10. *Adelantar investigaciones, de tipo cualitativo y cuantitativo, que permitan identificar necesidades, expectativas, uso, calidad e impacto de los servicios y trámites de Gobierno Digital de la entidad.*

<table>
<tr><th>ROL / INSTANCIA / DEPENDENCIA</th><th>RESPONSABILIDADES RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN</th></tr>
<tr><td></td><td>11. Garantizar la participación de funcionarios de la entidad en procesos de generación de capacidades (sensibilización, capacitación y formación) que se desarrollen bajo el liderazgo de la institución responsable de coordinarla implementación de la Estratégica de Gobierno Digital.

PARAGRAFO 1.2.: Para efectos del desarrollo y cumplimiento de tales funciones, el Comité Institucional de Gestión y Desempeño se apoyará en los Equipos de Trabajo Temáticos correspondiente a las Políticas de Racionalización de Trámites, Política de Gobierno Digital y Seguridad Digital, establecidos en el Artículo 7 del presente decreto.”</td></tr>
<tr><td>Comité de Seguridad de la Información</td><td>Conforme a las funciones asignadas en la Resolución 261 de 2023:

“Por la cual se conforma el Comité de Seguridad de la Información, se definen sus funciones y se adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar”

ARTÍCULO TERCERO: Funciones del Comité. El Comité de Seguridad de la Información de la Gobernación de Bolívar tendrá dentro de sus funciones las siguientes:

• Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.
• Revisar los diagnósticos del estado de la seguridad de la información en la Gobernación de Bolívar.
• Acompañar e impulsar el desarrollo de proyectos de seguridad.
• Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la Gobernación de Bolívar.
• Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
• Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
• Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
• Realizar revisiones periódicas del SGSI y según los resultados de esta revisión definir las acciones pertinentes.
• Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
• Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.
• Las demás funciones inherentes a la naturaleza del Comité. ”</td></tr>
<tr><td>Secretaría de las Tecnologías de la Información y de las Comunicaciones</td><td>Conforme a las funciones asignadas en el Decreto 169 de 2018:

ARTÍCULO 11°. - EQUIPOS DE TRABAJO TEMÁTICOS:
Para la ejecución de las Dimensiones de Gestión y Desempeño Institucional previstas en el Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG y las políticas enlistadas en el Decreto 1499 de 2017, se conformarán los siguientes equipos temáticos, los cuales serán los responsables de presentar propuestas y estrategias de operación para la implementación y sostenibilidad de las políticas y los componentes y requisitos del modelo.

Modificadas parcialmente por el Decreto 489 de 2018.

“ARTÍCULO 3°.- MODIFIQUESE el artículo 7 de los Equipos de Trabajo Temáticos que conforman el Comité Institucional de Gestión y Desempeño, el cual en lo sucesivo quedará así:

<table>
<tr><th>DIMENSIONES DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL /</th><th>POLÍTICAS</th><th>RESPONSABLES</th><th>COMPONENTES Y REQUISITOS</th></tr>
</table>
</td></tr>
</table>

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN

EQUIPOS DE TRABAJO TEMÁTICOS			
GESTIÓN PARA EL RESULTADO CON VALORES	Política de Gobierno Digital	Dirección de Conectividad e Infraestructura Tecnologica	• Adopción y formulación de la estrategia de tecnologías de la información. • Implementación de mecanismos para alcanzar niveles óptimos de calidad, seguridad y confiabilidad de la información. • Promoción del uso y apropiación de las tecnologías de la información. • Diagnóstico de capacidades institucionales. • Gestión de la Seguridad Informática.
	Política de Seguridad Digital	Dirección de Conectividad e Infraestructura Tecnológica	• Gestión de la Seguridad de la Información. • Rendición de cuentas al coordinador nacional de seguridad nacional sobre la implementación de la política. • Articulación de esfuerzos, recursos, metodologías y estrategias en la entidad.

Modificadas parcialmente por el **Decreto 222 de 2022**:

"***ARTICULO: 11°: -EQUIPOS DE TRABAJO TEMÁTICOS****: Para la ejecución de las Dimensiones de Gestión y Desempeño Institucional previstas en el Manual Operativo del Modelo integrado de Planeación y Gestión MIPG y las políticas enlistadas en el Decreto 1499 de 2017, así como las actualizaciones contenidas en el Manual Operativo del Modelo Integrado de Planeación y Gestión –MIPG versión 4, se conformarán los siguientes equipos temáticos, los cuales serán los responsables de presentar propuestas y estrategias de operación para la implementación y sostenibilidad de las políticas y los competentes y requisitos del modelo.*

IMENSIONES DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL/ EQUIPOS DE TRABAJO TEMÁTICOS	POLITICAS	INTEGRACION DEL EQUIPO TEMATICO	COORDINADOR / LÍDER EQUIPO DE TRABAJO TEMATICO
GESTIÓN CON VALORES PARA RESULTADOS	Política de Gobierno Digital	• Comunicaciones y Prensa • Dirección de Logística	• Dirección de Conectividad e Infraestructura Tecnológica
	Política de la Seguridad Digital	• Oficina de Comunicaciones y Prensa. • Dirección Logística.	• Dirección de Conectividad e Infraestructura Tecnológica

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN
	Además, conforme al **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*" *"**ARTÍCULO 3. SEGURIDAD DE LA INFORMACIÓN**: Con el propósito de cumplir con el principio de seguridad de la información que conforma los registros individuales constitutivos de los bancos de datos, se atenderán los lineamientos de esta Política, cuyo responsable es la Dirección de Tecnologías de la Información y las Comunicaciones -TIC- de la entidad.* ***ARTÍCULO 4. CONTROL**: La Dirección de Tecnologías de la Información y las Comunicaciones - TIC- será la encargada de velar por el cumplimiento de las políticas de protección de datos personales adoptadas a través del presente decreto, y realizará conjuntamente con la Secretaría de Planeación, las actuaciones necesarias para implementar la Política Pública de Protección de Datos Personales de la Gobernación de Bolívar."* Finalmente, el **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*" ***"Artículo 278**. Creación y naturaleza de la Secretaría de las Tecnologías de la Información y de las Comunicaciones. Créase la Secretaría de Tecnologías de la Información y de las Comunicaciones- TIC, como un organismo del sector central, de la administración del Departamento de Bolívar, con carácter misional."* ***"Artículo 282.** Funciones principales de la Secretaría de las Tecnologías de la Información y de las Comunicaciones- TIC. La Secretaría de las Tecnologías de la Información y de las Comunicaciones- TIC, tendrá las siguientes funciones:* *4. Ejecutar las funciones de acuerdo con los planes y estrategias institucionales, acordes con el modelo integrado de planeación y gestión de la entidad y los lineamientos, guías y estándares definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones.* *5. Desarrollar las políticas de administración, seguridad y control necesarias para garantizar la eficacia, eficiencia y confiabilidad de los recursos informáticos de la administración departamental.* *7. Garantizar la seguridad informática y de los sistemas de información del sector central y entidades del sector descentralizado de la administración departamental.* *9. Coordinar, supervisar y hacer el seguimiento de la implementación y ejecución de las políticas de seguridad tecnológica en el departamento;"* *"**Artículo 284**. Funciones principales del Despacho de la Secretaría de las Tecnologías de la Información y de las Comunicaciones- TIC. Las funciones del Despacho de la Secretaría de las Tecnologías de la Información y de las Comunicaciones- TIC, son las siguientes:* *3. Formular las políticas de custodia, administración, backup y seguridad de la información de la Administración departamental.* *7. Formular las políticas de administración, seguridad y control necesarias para garantizar la eficacia, eficiencia y confiabilidad de los recursos informáticos de la Administración departamental.* *9. Establecer y verificar el cumplimiento de políticas de seguridad para la administración de la tecnología (servidores, software de base, aplicaciones, servicios informáticos de valor agregado y estaciones de trabajo, entre otros).* *17. Garantizar la seguridad informática y de los sistemas de información del sector central y entidades del sector descentralizado de la administración departamental."* ***"Artículo 285.** Objetivo de la Dirección de Conectividad e Infraestructura Tecnológica. Dirigir e implementar la infraestructura tecnológica que aseguren la conectividad y que provean en forma oportuna, eficiente y transparente la información necesaria para el cumplimiento de los fines misionales del sector central."*

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN
	"Artículo 286. *Funciones principales de la Dirección de Conectividad e Infraestructura Tecnológica. Las funciones de la Dirección de Conectividad e Infraestructura Tecnológica, son las siguientes:* *3. Implementar estándares y buenas prácticas de tecnología en la Gobernación de Bolívar y acompañar los procesos de desarrollo tecnológico de las dependencias.* *5. Implementar políticas públicas para el uso, acceso y administración de la infraestructura tecnológica que soporta la información de la Entidad, de manera alineada con la estrategia gubernamental nacional y sectorial; así como la seguridad, privacidad y la interoperabilidad de los sistemas.* *6. Definir la arquitectura tecnológica de los sistemas de información de la Entidad, incluyendo estándares de interoperabilidad, de privacidad, de seguridad y de construcción o parametrización de aplicaciones.* *8. Evaluar y comunicar el valor y desempeño de la infraestructura tecnológica y administrar riesgos.* *9. Desarrollar estrategias de continuidad y tolerancia a fallas de la Infraestructura Tecnológica.* *10. Coordinar y administrar las acciones destinadas a prevenir, mitigar o superar los Incidentes, así como la recuperación de información ante los eventos que se presenten.* *11. Establecer políticas de uso para los recursos tecnológicos e investigar y formular iniciativas estratégicas y nuevos servicios de infraestructura TIC enfocados a los requerimientos del Departamento."*
Secretaría General	• Miembro del Comité de Seguridad de la Información.
Secretaría de Planeación	• Miembro del Comité de Seguridad de la Información.
Secretaría Jurídica	• Miembro del Comité de Seguridad de la Información.
Dirección de Atención al Ciudadano y Gestión Documental	• Miembro del Comité de Seguridad de la Información.
Oficina de Comunicaciones y Prensa	• Miembro del equipo temático de la Política de Gobierno Digital. • Miembro del equipo temático de la Política de Seguridad Digital.
Dirección Logística	• Miembro del equipo temático de la Política de Gobierno Digital. • Miembro del equipo temático de la Política de Seguridad Digital.
Control Interno	• Podrá asistir con voz y sin votos a las reuniones del Comité de Seguridad de la Información. • Las funciones que le otorgue la ley.
Líderes de Proceso	• Responsables de gestionar los riesgos y hacer seguimiento en 1ª línea. (Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6). • Conforme lo indica la 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*" *3.4. Acciones a desarrollar: Los líderes de proceso serán responsables de aplicar la metodología para el desarrollo de la identificación, análisis y valoración de los riesgos de gestión por cada uno de los procesos, sobre todo, para aquellos procesos más vulnerables. De igual forma cada líder de proceso propondrá y ejecutará las acciones necesarias para mitigar sus riesgos y el equipo auditor de la oficina de Control Interno hará seguimiento al cumplimiento de las acciones formuladas.*
Todos los funcionarios y contratistas	• Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados. • Responsables de ejecutar controles operativos en el día a día. (Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6).

SANCIONES

El incumplimiento de la Política de Seguridad y Privacidad de la Información de la Gobernación de Bolívar dará lugar a la aplicación de las medidas disciplinarias, administrativas, contractuales y legales que correspondan, de acuerdo con la normativa interna de la entidad y con las disposiciones del ordenamiento jurídico nacional. Estas medidas podrán incluir llamados de atención, sanciones disciplinarias conforme al Código Disciplinario Único, la imposición de cláusulas contractuales e incluso la terminación anticipada de contratos en el caso de contratistas y proveedores.

El respeto a esta política constituye no solo una obligación legal y contractual, sino también un compromiso institucional orientado a fortalecer la cultura de seguridad de la información, prevenir riesgos y salvaguardar los derechos e intereses de la ciudadanía en el marco de la gestión pública.

El ejercicio de las competencias de control interno garantizará la verificación permanente del cumplimiento de esta política, mediante actividades de seguimiento, auditoría y evaluación de los procesos relacionados con la seguridad y privacidad de la información. En los casos en que se evidencien incumplimientos, se dará traslado a los entes de control competentes para la aplicación de las medidas que correspondan, en estricto cumplimiento del marco normativo vigente.

El estricto cumplimiento de esta política constituye un deber institucional y una responsabilidad compartida entre servidores públicos, contratistas, terceros y proveedores que acceden, administran o gestionan información de la Gobernación de Bolívar. Este compromiso busca proteger la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información, fortalecer la confianza ciudadana en la gestión pública y garantizar que la entidad cumpla de manera transparente, eficiente y segura con su misión y objetivos estratégicos

SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

La Gobernación del Departamento de Bolívar realizará revisiones anuales al Sistema de Gestión de Seguridad de la Información establecido mediante 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". Dichas revisiones estarán enfocadas en los siguientes aspectos:

- Revisión de las políticas, procedimientos, instructivos, manuales, guías, formatos, reportes, informes y demás documentos que conforman el Sistema de Gestión de Seguridad de la Información de la Gobernación del Departamento de Bolívar.
- Revisión de indicadores definidos para el Sistema de Gestión de Seguridad de la Información en la resolución indicada.
- Revisión de avance en la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC según el Plan de Seguridad y Privacidad de la Información aprobado para la vigencia.
- Revisión de avance de la Política de Seguridad Digital de acuerdo con lo solicitado por FURAG con el objetivo de realimentar y mejorar el mismo sistema.

MEJORA CONTINUA Y ACCIONES CORRECTIVAS

La Gobernación del Departamento de Bolívar se compromete a implementar procesos de mejora continua en la gestión de la seguridad y privacidad de la información, en concordancia con el ciclo PHVA (Planear – Hacer – Verificar – Actuar) y con los principios de la norma ISO/IEC 27001:2022.

En este marco, la entidad garantizará:

- La identificación y análisis de no conformidades, incidentes de seguridad y desviaciones frente a lo establecido en la política, procedimientos y controles.
- La implementación de acciones correctivas y preventivas que eliminen las causas raíz de los incidentes y eviten su recurrencia.
- El seguimiento de recomendaciones provenientes de evaluaciones de control interno y revisiones realizadas por la Alta Dirección.
- La incorporación de lecciones aprendidas derivadas de incidentes, buenas prácticas y experiencias de mejora institucional.
- La revisión periódica de la eficacia de las medidas adoptadas, asegurando la adaptación del SGSI a cambios tecnológicos, normativos y organizacionales.

De esta manera, la mejora continua se consolida como un pilar fundamental para fortalecer la confianza ciudadana, garantizar la protección de los activos de información y asegurar que la Gobernación de Bolívar cumpla de manera eficiente, segura y transparente con su misión institucional

RESPONSABLES

1. Comité Institucional de Gestión y Desempeño - Aprobación
2. Comité de Seguridad de la Información – Seguimiento
3. Dirección de Conectividad e Infraestructura Tecnológica - Diseño, Implementación y Acompañamiento
4. Dependencias - Implementación

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.

La obligación descrita está bajo la responsabilidad del Líder de Seguridad de la Información y por el Comité Institucional de Gestión y Desempeño.

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección, el comité de gestión y desempeño institucional 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 Institucional de Gestión y Desempeño y por parte del Comité de Seguridad digital de la Gobernacion 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

VERSIÓN	FECHA	AUTOR	CAMBIOS
1.0	30 de noviembre 2020	Tairo Mendoza Piedrahita- Profesional Especializado Dirección TIC	Versión Inicial

2.0	Octubre de 2021	Tairo Mendoza Piedrahita- Profesional Especializado DIRECCION TIC	Lineamientos de Política de Seguridad y Privacidad de la Información MSPI
3.0	Septiembre 10 de 2025	Robinson Domínguez Reyes. Profesional Especializado Lizeth Gómez Padilla Asesora Externa	• Actualización a los lineamientos del nuevo modelo de Seguridad y Privacidad de la Información 2025 • Incorporación del marco ISO/IEC 27001:2022.

ELABORÓ	**REVISÓ**	**APROBÓ**
Nombre: Robisnson Domínguez Reyes **Cargo:** Profesional Especializado **Nombre:** Lizeth Gómez Padilla **Cargo:** Asesora externa **Fecha:** 10/09/-2025	**Nombre**: Laura Abuchar Camacho. **Cargo:** Directora de Conectividad e Infraestructura Tecnológica **Fecha**: 02/10/2025	**Nombre**: Comité Institucional de Gestión y Desempeño. Comité de Seguridad digital de la Gobernacion de Bolívar **Fecha**:


AB ORDINE
LIBERTAS
GOBERNACIÓN
DE BOLÍVAR