PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

DIRECCIÓN DE CONECTIVIDAD E INFRAESTRUCTURA TECNOLÓGICA

2026

TABLA DE CONTENIDO

INTRODUCCIÓN

En el marco de la transformación digital y del fortalecimiento de la gestión pública, la Gobernación de Bolívar reconoce la necesidad de garantizar la seguridad y privacidad de la información como un eje estratégico para el cumplimiento de sus funciones misionales. En este sentido, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se configura como un instrumento esencial para identificar, evaluar, priorizar y aplicar medidas que permitan mitigar, transferir, aceptar o eliminar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información institucionales.

Asimismo, este plan se articula directamente con el Modelo de Seguridad y Privacidad de la Información (MSPI), adoptado en el sector público colombiano como marco rector para la implementación de controles que fortalezcan la gestión de riesgos y aseguren el cumplimiento de principios de transparencia, confianza digital y protección de datos personales. De manera complementaria, se encuentra alineado con la norma ISO/IEC 27001:2022, referente internacional que establece los requisitos para los sistemas de gestión de seguridad de la información, y con la ISO/IEC 27002:2022, que proporciona directrices para la selección e implementación de controles de seguridad.

Por lo anterior, el presente documento constituye una guía metodológica para la Gobernación de Bolívar en la gestión proactiva de riesgos asociados al tratamiento de la información. Su propósito no solo es reducir la probabilidad e impacto de incidentes de seguridad, sino también generar capacidades institucionales para la protección de datos en entornos físicos y digitales, en coherencia con la planeación estratégica y los objetivos organizacionales.

Finalmente, este plan refleja el compromiso de la Alta Dirección con la gestión integral de riesgos, la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) y la consolidación de una cultura organizacional orientada a la protección de los derechos de los ciudadanos y al aseguramiento de los procesos misionales de la Entidad.

OBJETIVO

Establecer un marco sistemático, integral y documentado para la definición, implementación, seguimiento y mejora continua de controles orientados a la gestión efectiva de los riesgos identificados en materia de seguridad y privacidad de la información institucional. Este marco busca preservar la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información, en concordancia con los principios de seguridad digital y protección de datos personales.

OBJETIVOS ESPECÍFICOS:

- Garantizar el cumplimiento normativo vigente en materia de seguridad de la información y protección de datos personales.
- Fortalecer la resiliencia institucional frente a incidentes de seguridad, minimizando impactos operativos, legales y reputacionales.
- Consolidar la confianza de la ciudadanía en los servicios digitales ofrecidos por la Entidad, mediante prácticas transparentes, responsables y alineadas con estándares internacionales.

ALCANCE

El presente plan aplica a todos los procesos, dependencias, activos de información, recursos tecnológicos y servicios de la Gobernación de Bolívar que impliquen el tratamiento, almacenamiento, transmisión o resguardo de información institucional y de datos personales. Su alcance incluye:

- Activos de información críticos, tales como bases de datos, sistemas misionales y expedientes digitales.
- Infraestructura tecnológica, incluyendo redes, servidores, estaciones de trabajo, sistemas en la nube y dispositivos móviles.
- Usuarios internos y externos que accedan, gestionen o administren información de la entidad.
- Procesos y servicios que soportan el cumplimiento de los fines misionales y legales de la Gobernación.

En coherencia con lo anterior, el plan contempla tanto riesgos tecnológicos como riesgos organizacionales, humanos y de terceros, asegurando la alineación con el Modelo de Seguridad y Privacidad de la Información (MSPI) y con los requisitos de la ISO/IEC 27001:2022.

JUSTIFICACIÓN

En primer lugar, desde el **cumplimiento normativo**, este plan responde a las disposiciones establecidas por el **Decreto 620 de 2020**, la **Ley 1581 de 2012** sobre protección de datos personales, la **Ley 1712 de 2014** de transparencia y acceso a la información pública, así como a los lineamientos del **MSPI** emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones. Igualmente, alinea la gestión de riesgos con los estándares internacionales **ISO/IEC 27001:2022** y **ISO/IEC 27002:2022**, lo cual garantiza la adopción de buenas prácticas internacionalmente reconocidas.

En segundo lugar, desde la perspectiva **reputacional**, la Gobernación de Bolívar reconoce que la adecuada protección de la información institucional y de los datos personales es un factor clave para generar confianza entre la ciudadanía, los entes de control y los aliados estratégicos. La materialización de incidentes de seguridad, tales como fugas, accesos no autorizados o pérdida de información crítica, no solo tendría consecuencias legales, sino también un impacto negativo en la credibilidad y legitimidad de la Entidad.

Finalmente, desde un enfoque **estratégico**, este plan constituye una herramienta para fortalecer la gobernanza de la información, incrementar la eficiencia administrativa, reducir vulnerabilidades en los procesos misionales y garantizar la continuidad de los servicios digitales de la Gobernación. De esta manera, se aporta a la consolidación de un ecosistema público confiable, resiliente y alineado con los principios de la seguridad digital nacional, contribuyendo directamente al cumplimiento de los objetivos institucionales y de las políticas gubernamentales en materia de innovación y transformación digital.

PROCESO DE GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION

Basados en la norma ISO 27005, la GOBERNACIÓN DE BOLÍVAR, ejecutará el siguiente modelo de gestión de riesgos de la **Guía de Gestión de Riesgos del MINTIC**, el cual ayudará a garantizar un tratamiento adecuado de los riesgos de seguridad de la información:

- Proceso para la administración del riesgo en seguridad de la información

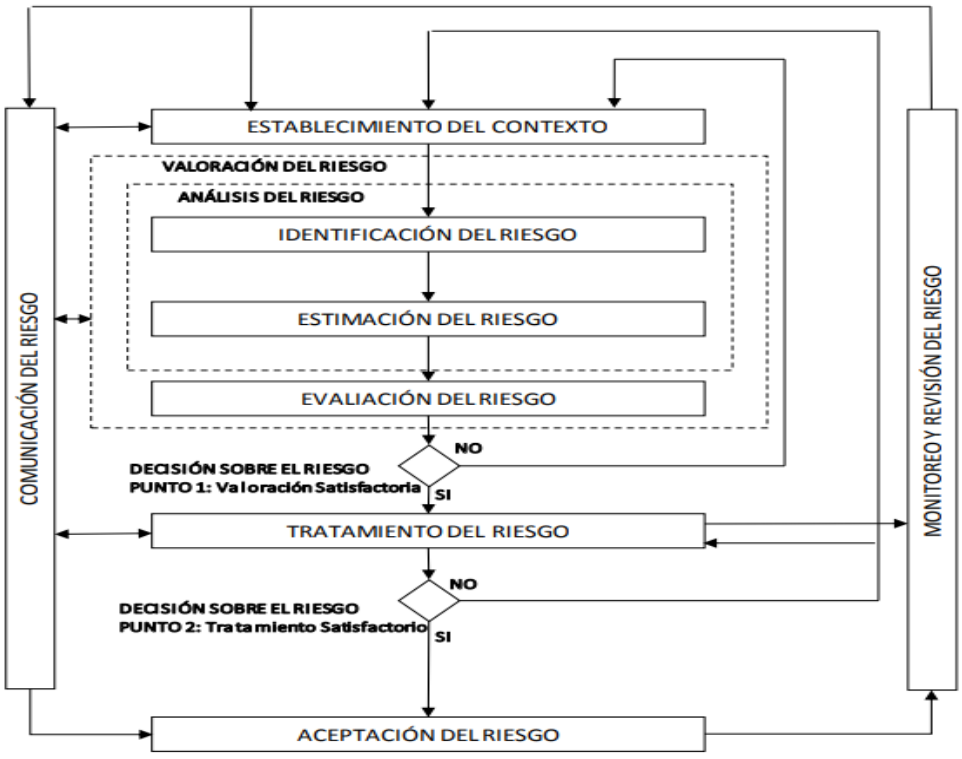

Imagen 2. Tomado de la NTC-ISO/IEC 27005

Modelo de gestión de riesgos de seguridad de la información. NTC/ISO 27005

Nota: La Metodología Instructivo Inventario de Activos de TI, así como la Metodología para el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información están definidas en el documento correspondiente.

CRONOGRAMA DE ACTIVIDADES

Este es el Plan propuesto para el Tratamiento de Riesgos del año 2026:

Plan de actividades de Inventario, Análisis de Riesgos de Seguridad Digital e Implementación de Controles 2026						
Cronograma de Actividades						
Item	**Actividad**	**Descripción**	**Responsable**	**Fecha de inicio**	**Fecha de finalización**	**Días dedicados**
1	**Invitación a líderes**	Dirección TIC invitará a los líderes de las diferentes dependencias a iniciar el proceso de "**Plan General de Tratamiento de Riesgos de Seguridad y Privacidad de la Información**"	Dirección TIC	25/04/26	01/05/2026	6
2	**Aceptación**	Los líderes de las dependencias definirán un delegado e informarán de la aceptación a la Dirección TIC.	Secretarios, Directores, Jefes	28/04/2026	28/04/2026	01
3	**Programación de reuniones**	Dirección TIC programará reuniones	Dirección TIC	29/04/26	01/05/26	2

4	**Reuniones "Sensibilización definiciones Seguridad de la Información"**	Dirección TIC realizará entrenamientos "**Sensibilización y definiciones Seguridad de la Información**"	Dirección TIC, Secretarios, Directores, Jefes	02/05/2026	08/05/26	6
5	**Reuniones "Identificación de Activos"**	Dirección TIC realizará entrenamiento **Reunión "Identificación de Activos"**	Dirección TIC, Secretarios, Directores, Jefes	09/05/26	12/05/26	3
6	**Identificación de Activos**	Los líderes o sus delegados realizarán el proceso de identificación de activos con el acompañamiento de la Dirección TIC.	Secretarios, Directores, Jefes	16/05/26	16/05/26	30
7	**Recibo de información identificación de activos**	Líderes entregarán información de activos-Dirección TIC consolidará la información.	Dirección TIC, Secretarios, Directores, Jefes	19/05/26	29/05/26	1
8	**Reuniones "Riesgo de Seguridad Digital"**	Dirección TIC realizará entrenamiento, Identificación Riesgos, Amenazas y Vulnerabilidades.	Dirección TIC, Secretarios, Directores, Jefes	30/05/26	30/05/26	1
9	**Identificación de Riesgos**	Líderes aplicarán la metodología de identificación de los riesgos asociados a los activos de información.	Secretarios, Directores, Jefes	30/05/26	30/05/26	3
10	**Recibo de información Identificación de Riesgos**	Líderes entregarán información de Riesgos a la Dirección TIC para consolidar información en la matriz de riesgos digitales	Dirección TIC, Secretarios, Directores, Jefes	18/06/26	20/06/26	2
11	**Reuniones de "Matriz de Riesgo Seguridad Digital"**	Dirección TIC realizará entrenamiento "**Matriz de Riesgo Seguridad Digital**"	Dirección TIC, Secretarios, Directores, Jefes	18/06/26	20/06/26	2
12	**Diligenciamiento "Matriz de Riesgos de Seguridad Digital"**	Líderes diligenciarán la **"Matriz de Riesgos de Seguridad Digital"**	Secretarios, Directores, Jefes	18/06/26	20/06/26	2
13	**Recibo de información Matriz de Riesgos de Seguridad Digital**	Líderes entregarán información a la Dirección TIC y consolidarán la información	Dirección TIC, Secretarios, Directores, Jefes	20/06/26	20/06/26	2
14	**Reuniones de controles**	Dirección TIC realizará entrenamiento "**Identificación e Implementación de Controles**"	Dirección TIC, Secretarios, Directores, Jefes	18/06/26	24/08/26	4
15	**Identificación de Controles**	Líderes identificarán acciones que se deben tomar para controlar o mitigar los riesgos a que se ven expuestos los activos de información con el fin de disminuir la posibilidad o las consecuencias de su materialización. Deben ser suficientes, efectivos y oportunos. Identificarán si son manuales, automáticos, discrecionales, obligatorios, preventivos o correctivos.	Secretarios, Directores, Jefes	18/06/2026	24/06/26	4
16	**Implementación de Controles**	Secretarios, Directores, Jefes deberán proveer las acciones para establecer los controles de sus dependencias respectivas.	Secretarios, Directores, Jefes	18/06/26	24/06/26	4
17	**Recibo de información de Implementación de Controles**	Líderes entregarán información de Controles a la Dirección TIC para consolidar información.	Dirección TIC, Secretarios, Directores, Jefes	10/07/26	18/07/26	3

18	**Reuniones de monitoreo**	Dirección TIC realizará entrenamiento de "**Monitoreo**"	Secretarios, Directores, Jefes, Dirección TIC	10/07/26	10/07//26	60 días
19	**Diseño y consolidación de información de Monitoreo**	Líderes, Secretarios, Directores, Jefes, Dirección TIC contemplarán un proceso de seguimiento efectivo que facilite la rápida detección y corrección de las deficiencias en la administración de los riesgos identificados. Líderes, Secretarios, Directores, Jefes establecerán indicadores que evidencien la efectividad del sistema de administración de riesgos adoptados. Dirección TIC asegurará que los controles estén funcionando en forma oportuna, efectiva y eficiente. Líderes, Secretarios, Directores, Jefes asegurarán que los riesgos residuales se encuentren en los niveles de aceptación establecidos. Dirección TIC llevará un registro de incidentes que contemple: Bases de datos y datos comprometidos, titulares, fecha del incidente y de descubrimiento, acciones correctivas realizadas y responsables.	Secretarios, Directores, Jefes, Dirección TIC	10/07//26	25/07/26	15
20	**Preparación y Entrega de informes**	Preparación y entrega de informe de los resultados del proceso y controles establecidos.	Dirección TIC	25/07/26	06/08/26	10

RESPONSABLES

1. Gobernador del Departamento de Bolívar - Representante Legal
2. Comité Institucional de Gestión y Desempeño - Aprobación
3. Comité de Seguridad de la Información - Seguimiento y Aprobación de documentos
4. Dirección de Conectividad e Infraestructura Tecnológica- Diseño e Implementación. Acompañamiento Secretaria TIC.
5. 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

CONTROL DE CAMBIOS			
Fecha	Autor	Versión	Cambio
Diciembre 28 de 2018	Tairo Mendoza Piedrahita Profesional Especializado Dirección TIC	1.0	• Versión Inicial
Diciembre 26 de 2019	Tairo Mendoza Piedrahita Profesional Especializado Dirección TIC	2.0	• Se detalló la evaluación del riesgo asociados la seguridad y privacidad de la información
Noviembre 30 de 2020	Tairo Mendoza Piedrahita Profesional Especializado Dirección TIC	3.0	• Se definieron de manera general los riesgos, vulnerabilidades y amenazas. • Se incluyeron los controles según la norma ISO/IEC 27002:2013
Agosto 31 de 2021	Tairo Mendoza Piedrahita Profesional Especializado Dirección TIC	4.0	• Se agregan Amenazas del Catálogo de Enisa
Diciembre 06 de 2022	Tairo Mendoza Piedrahita Profesional Especializado Dirección TIC	4.1	• Se agregó cronograma de actividades.
Enero 26 de 2024	Tairo Mendoza Piedrahita Profesional Especializado	5.0	• Revisión catálogo de amenazas

	Dirección de Conectividad e Infraestructura Tecnológica		• Actualización de fechas
Septiembre 19 de 2025	**Robinson Domínguez Reyes** Cargo: **Profesional Especializado** **Lizeth Gómez Padilla** Cargo: **Asesora Externa** Dirección de Conectividad e Infraestructura Tecnológica	6.0	• Actualización Decreto 297 de 2024 • Actualización fechas • Actualización redacción • Se incluyeron los controles según la norma ISO/IEC 27001:2022 y ISO/IEC 27002:2022

ELABORÓ	**REVISÓ**	**APROBÓ**
Robinson Domínguez Reyes **Cargo:** Profesional Especializado Lizeth Gómez Padilla **Cargo:** Asesora Externa **19/09/2025**	Laura Abuchar Camacho **Cargo:** Directora de Conectividad e Infraestructura Tecnologica **02/10/2025**	**Nombre**: Comité Institucional de Gestión y Desempeño. Comité de Seguridad digital de la Gobernacion de Bolívar **Fecha**:


NB ORDINE
LIBERTAS
GOBERNACIÓN
DE BOLÍVAR