POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PERSONAL

La Gobernación de Bolívar, cuya función misión es: "El gobierno del Departamento de Bolívar asume como su responsabilidad primigenia, la construcción de las condiciones para generar bienestar y desarrollo humano, a nivel regional y local en su territorio y comunidad, y ejercer con eficiencia, equidad y probidad la orientación del desarrollo del Departamento de Bolívar, la complementación de los esfuerzos de las administraciones locales, para la asignación de los recursos productivos entre los distintos grupos de la sociedad, involucrando a la totalidad de los actores públicos, privados y comunitarios.", en su propósito de salvaguardar la confidencialidad, disponibilidad e integridad de los datos personales, que se encuentran bajo nuestra protección, establece los siguientes objetivos:

1. OBJETIVO:

- **OBJETIVO GENERAL**

Establecer los lineamientos para garantizar la aplicación del marco normativo sobre la protección de datos personales establecida en la Ley 1581 de 2012 y sus decretos reglamentarios; donde todas las personas tienen el deber de conocer, actualizar y rectificar la información que se haya recogido sobre ellas en las bases de datos que maneja entidad, garantizando que la información suministrada por las personas cuente con los principios de la información, que son: confidencialidad, integridad y disponibilidad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- **OBJETIVOS ESPECÍFICOS**

✓ Identificar la información de metadatos y bases de datos con datos personales allegados a la Gobernación de Bolívar.

✓ Implementar las medidas adecuadas para garantizar una protección robusta de la información.

✓ Gestionar de manera eficaz los riesgos de seguridad y privacidad de la información identificados en la Entidad.

✓ Cumplir con las directrices contempladas en esta Política de Gestión de Incidentes de Seguridad de la información personal.

✓ Sensibilizar y apropiar la gestión adecuada de seguridad y privacidad de la información en los funcionarios, contratistas ciudadanos y demás partes interesadas de la entidad

2. ALCANCE

Esta política aplica a todos los funcionarios y contratistas que para el cumplimiento de sus funciones y obligaciones contractuales, recolectan, utilizan y almacenan información para la ejecución de los procesos enmarcados en el mapa de procesos de la entidad.

3. CUMPLIMIENTO

Todos los servidores públicos deberán dar cumplimiento con la presente política. El incumplimiento a la Política de Gestión de Incidentes de Seguridad de la información personal traerá consigo, las consecuencias legales que apliquen a la normativa de la entidad, incluyendo lo establecido en las normas que competen al gobierno nacional y

territorial en cuanto a las disposiciones generales para la protección de datos personales.

4. DIRECTRICES

4.1 Gestión de incidentes y mejoras de la seguridad de la información personal

4.1.1 Responsabilidades y procedimientos

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información personal.	Diseñar las medidas adecuadas para garantizar una protección robusta de la información.	**DIRECCIÓN TIC**	Política de Tratamiento de Datos Personales 2.0
	realizar la actualización de la información en la base de datos de los activos de información y en el RNBD.		Certificación RNBD
	Socializar la gestión adecuada de seguridad y privacidad de la información en los funcionarios, contratistas ciudadanos y demás partes interesadas de la entidad.		Enlace Capacitaciones en seguridad y tratamientos de datos personales.

4.2 Reporte de Incidentes de Seguridad de la información personal

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Informar sobre los Incidentes de Seguridad de la información personal, a través de los canales de gestión apropiados.	En caso de incidentes cibernéticos graves o muy graves deberán reportar dentro de los 15 días calendario siguientes a su detección al COLCERT.	**DIRECCIÓN TIC**	Infirme reporte incidente ante autoridades.
	En caso de incidentes cibernéticos graves o muy graves deberán reportar dentro de los 30 días calendario siguientes a su detección CAI Virtual de la Policía Nacional www.ccp.gov.co, Centro Cibernético Policial de la Policía Nacional al teléfono 4266900 ext. 104092		Infirme reporte incidente ante autoridades.
	Todos los incidentes que comprometan datos personales deberán ser reportados a la Superintendencia de Industria y Comercio dentro de los 15 días hábiles siguientes a su detección[1].		Reporte de registro de incidentes en el portal RNBD de la SIC.
	Todos los incidentes que comprometan datos personales deberán ser reportados a los Titulares dentro de los 30 días calendario siguientes a su detección[2].		Informe de notificación a titulares de datos personales.

[1] *Ley 1581 de 2012; la Guía para la Gestión de Incidentes de Seguridad en el Tratamientos de Datos Personales y la Guía para la Implementación del principio de Responsabilidad Demostrada de la Superintendencia de Industria y Comercio*
[2] *Ley 1581 de 2012; la Guía para la Gestión de Incidentes de Seguridad en el Tratamientos de Datos Personales y la Guía para la Implementación del principio de Responsabilidad Demostrada de la Superintendencia de Industria y Comercio*

4.3 Evaluación de eventos de seguridad de la información y decisiones sobre ellos

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Evaluar los eventos de Seguridad de la Información Personal	Recolectar evidencia lo más pronto posible después de que ocurra el incidente.	**DIRECCIÓN TIC**	Informe del estado y aplicación de controles de seguridad de la información, según la vulnerabilidad detectada.
	Realizar el análisis forense de seguridad de la información, según la vulnerabilidad detectada.		
	Implementar los controles correspondientes, los cuales se encuentran adecuados en las Políticas de seguridad de Tecnologías de información y comunicación de la Gobernación de Bolívar.		
	Documentar el Incidente.		

4.4 Monitoreo

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
En esta etapa se realizará seguimiento para velar porque las medidas que se hayan establecido sean efectivas	Se debe contemplar un proceso de seguimiento efectivo que facilite la rápida detección y corrección de las deficiencias en la administración de los riesgos identificados. Asegurar que los controles estén funcionando en forma oportuna, efectiva y eficiente. Aseverar que los riesgos residuales se encuentren en los niveles de aceptación establecidos.	**DIRECCIÓN TIC**	Informes de seguimientos a política de seguridad y tratamiento de datos personales.

5. INFORMACIÓN DE CONTACTO

Cualquier inquietud relacionada con la Política de Gestión de Incidentes de Seguridad de la información personal, favor remitirla a:

- Protección de Datos Gobernación de Bolívar
  Dir.: Carretera Cartagena-Turbaco Km. 3 Sector Bajo Miranda - El Cortijo
  Tel: (605)-6517444 ext 1007
  Mail: Protecciondedatos@bolivar.gov.co
  Web: www.bolivar.gov.co

6. REFERENTES NORMATIVOS

- Ley 1581 de 2012.
- Guía para la Gestión de Incidentes de Seguridad en el Tratamientos de Datos Personales.
- Guía para la Implementación del principio de Responsabilidad Demostrada de la Superintendencia de Industria y Comercio.
- Política de Tratamiento de Datos Personales 2.0 – Gobernación de Bolívar.

7. REVISIÓN, VIGENCIA Y APROBACIÓN

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 de la Dirección TIC y por el Comité Institucional de Gestión y Desempeño.

VIGENCIA Y CONTROL DE CAMBIOS

FECHA	AUTOR	VERSIÓN	CAMBIOS
01 de Agosto 2021	Dirección TIC	1.0	Versión inicial.