PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

DIRECCIÓN DE CONECTIVIDAD E INFRAESTRUCTURA TECNOLÓGICA

2026

TABLA DE CONTENIDO

PROGRAMA INTEGRAL DE GESTION DE DATOS PERSONALES

OBJETIVO

Establecer, implementar, mantener y mejorar de manera continua un marco de gobernanza y control del tratamiento de datos personales en la GOBERNACIÓN DE BOLIVAR, a partir de una ruta con enfoque metódico, la cual facilite las pautas necesarias para desarrollar la Gestión Integral de los Datos y asegure el cumplimiento de la normativa vigente en materia de protección de datos personales.

ALCANCE

El alcance del programa comprende el conjunto de políticas, procesos, procedimientos, recursos y controles implementados por la Gobernación de Bolívar para regular el tratamiento de datos personales en todas sus dependencias, sistemas de información, plataformas tecnológicas y relaciones con terceros. En particular, el programa aplica a:

Sujetos obligados internos

El programa es de obligatorio cumplimiento para todos los servidores públicos, contratistas, practicantes, proveedores y terceros que, en ejercicio de sus funciones o actividades, realicen tratamiento de datos personales por cuenta de la Gobernación de Bolívar.

Tipos de datos personales tratados

Igualmente, cubre el tratamiento de datos personales públicos, semiprivados, privados y sensibles, así como los datos de niños, niñas y adolescentes, conforme a la clasificación establecida por la Ley 1581 de 2012.

Procesos institucionales

El programa se integra a los procesos estratégicos, misionales, de apoyo y de evaluación de la entidad, incluyendo la recolección, almacenamiento, uso, circulación, transmisión, transferencia y supresión de datos personales.

Ámbito tecnológico y documental

De manera complementaria, el alcance abarca todos los sistemas de información, bases de datos físicas y digitales, servicios en la nube, soluciones on-premise, archivos de gestión y repositorios documentales donde se traten datos personales.

Relaciones con terceros

De igual forma, incluye los tratamientos realizados por encargados del tratamiento, operadores, proveedores tecnológicos y aliados estratégicos que procesen datos personales por cuenta de la Gobernación, quienes deberán cumplir las obligaciones contractuales y legales correspondientes.

Cobertura territorial y funcional

Finalmente, el programa aplica a todas las sedes, dependencias y actuaciones administrativas de la Gobernación de Bolívar, independientemente del canal, medio o tecnología utilizada para el tratamiento de los datos personales.

La implementación del programa permitirá a la Gobernación de Bolívar demostrar cumplimiento normativo, reducir riesgos legales y reputacionales, fortalecer la seguridad de la información y garantizar el ejercicio efectivo de los derechos de los titulares.

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:

- 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.
- 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*".
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- CONPES No. 3701 del 2011 "Lineamientos de Políticas para la Ciberseguridad y Ciberdefensa"
- CONPES No. 3854 de 2016 "Política Nacional de Seguridad Digital"
- CONPES No. 3995 de 2020 "Política Nacional de Confianza y Seguridad Digital"
- 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 v5

- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”
- 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”
- 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”
- 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 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

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante 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 la misma (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).

PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

La Gobernación de Bolívar, en su calidad de responsable del tratamiento de datos personales, adopta el Programa Integral de Gestión de Datos Personales en cumplimiento de los deberes establecidos en el artículo 17 de la Ley 1581 de 2012, particularmente la obligación de “cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio” (Congreso de la República de Colombia, 2012). En este sentido, la entidad asume un enfoque sistemático y verificable orientado a garantizar la protección efectiva de los derechos de los titulares y la observancia del régimen colombiano de protección de datos personales.

En este sentido, la Superintendencia de Industria y Comercio ha desarrollado la Guía para la implementación del principio de responsabilidad demostrada, mediante la cual establece lineamientos para que los responsables adopten medidas “apropiadas y efectivas para cumplir la ley y demostrar ese cumplimiento” (SIC, 2016, p. 9). En coherencia con dichas directrices, el presente programa define el conjunto de políticas, procedimientos, controles y mecanismos de monitoreo necesarios para materializar los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y seguridad en el tratamiento de la información personal.

De igual forma, el documento se fundamenta metodológicamente en las guías emanadas por la SIC y se articula con el Plan General para el Tratamiento de Riesgos de Seguridad de la Información de la Gobernación de Bolívar, el cual complementa y fortalece la gestión integral de riesgos asociados al tratamiento de datos personales. En consecuencia, el programa integra los componentes jurídicos, técnicos y organizacionales requeridos para la prevención, mitigación y control de riesgos de privacidad, promoviendo una cultura institucional de protección de datos y mejora continua.

SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES

Según la “Guía para la Implementación del Principio de Responsabilidad Demostrada” la entidad debe “*desarrollar un sistema de administración de riesgos, acorde con su estructura, procesos y procedimientos, la cantidad de BD y tipos de datos personales”,* la GOBERNACIÓN DE BOLÍVAR ejecutará el siguiente modelo de gestión de riesgos de la Guía de Gestión de

Riesgos del MINTIC basados en la norma ISO 27005, 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

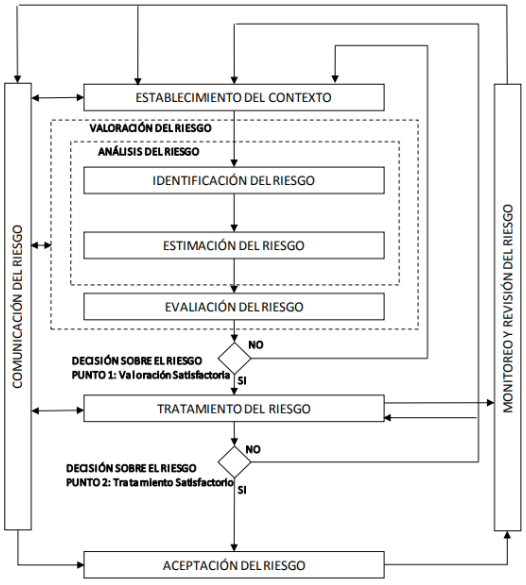


Imagen 2. Tomado de la NTC-ISO/IEC 27005

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

COMPROMISO DE LA ORGANIZACIÓN

La Gobernación de Bolívar comprometida con la protección de datos personales publica el Decreto 531 de 2018 - 11 DIC. 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” en el cual se DECRETA:

“ARTÍCULO 1. ADOPCIÓN: *Adóptese el* ***Manual de Políticas y Procedimientos de Protección de Datos Personales*** *de la Gobernación de Bolívar contenida en documento anexo, que hace parte integral de presente acto administrativo, contentiva de los lineamientos que garantizan la aplicación del marco normativo sobre la protección de datos personales establecida en la Ley 1581 de 2012 y sus decretos reglamentarios: el cual impone a todas las personas el deber de conocer, actualizar y rectificar la información que se haya recogido sobre ellas en las bases de datos que maneja la Gobernación, garantizando que la información suministrada por estas, cuente con los principios que la rigen, como son la confidencialidad, integridad y disponibilidad.”* Y establece responsabilidades:

“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."*

Que 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."*

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."

ETAPAS

El programa consta de las siguientes etapas:

1. **Identificación**.

En esta etapa se identifican las bases de datos con datos personales y se determina su criticidad. Se deben:

- Socialización del marco normativo de datos personales.
- Documentar los procesos y procedimientos que se implementen dentro del ciclo de vida de los datos personales.
- Definir la metodología del Inventario de Bases de Datos.
- Definir la metodología de identificación de los riesgos asociados al tratamiento de información personal.

Metodología identificación de Bases de Datos

El proceso consiste en:

a. **Describir bases de datos**

La primera actividad es realizar un inventario de las bases de datos con datos personales por parte de las dependencias, sus propiedades y Criticidad para lo cual se utilizó la Metodología de Inventario de Activos de TI Gobernación de Bolívar y la Matriz de Inventario de Activos.

b. **Determinar la Criticidad del Activo**

La criticidad de las bases de datos estará determinada por la tabla publicada en la Guía de Gestión de riesgos del MINTIC:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 1. Criterios de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Tabla 2. Niveles de Clasificación

Nota: La Información No Clasificada debe tratarse como Información Pública Reservada.

2. Medición

En esta etapa se determina la posibilidad de ocurrencia de los riesgos relacionados con el tratamiento de datos personales y su impacto en caso de materializarse.

a. Determinar el Riesgo

Tiene como objetivo conocer los escenarios que pueden producir en la entidad y los efectos que puedan tener sobre los objetivos de esta.

El procedimiento para la gestión de riesgos contiene el reconocimiento de las causas y la procedencia del riesgo que puedan afectar a los objetivos.

- Riesgo de Disponibilidad
- Riesgo de Integridad
- Riesgo de Confidencialidad

Riesgos	Descripción
Incumplimiento de las políticas de seguridad y privacidad de la información que atenten contra la disponibilidad, integridad y confidencialidad de la información	Políticas o controles de seguridad y privacidad de la información no aplicados total o parcialmente por desconocimiento o actos intencionales.
Información imprecisa o inexacta en las operaciones	La información podría ser modificada o alterada sin autorización. Se puede dar por alteración o cambios de la información (digital o electrónica) generada, recolectada, procesada o almacenada.
Pérdida en la trazabilidad de las operaciones realizadas	Las operaciones realizadas con la información no pueden rastrearse o no presenta claramente quién y qué se ha realizado con la misma.
Indisponibilidad de la Información oportuna o de los sistemas para las operaciones	La información no se encuentra disponible en el momento que se necesita para cumplir la operación o funciones propias en la Agencia.
Fuga o acceso de información por personal no autorizado	La información puede ser accedida por personal no autorizado por posible interceptación de tráfico en las redes, falla en los controles de acceso de los sistemas o instalaciones, o publicación sin autorización de esta accidental o intencionalmente.

Por cada riesgo se determina:

b. Vulnerabilidades

Las Vulnerabilidades son las indicadas en la **Matriz de Riesgos de Seguridad Digital**:

Vulnerabilidades
Desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información
Manejo manual de la información
Ausencia de validación de autenticación de la información
Ausencia de copias de respaldo o backups de la información
Retraso en la salida de información de los sistemas
Retraso en la entrega de información por parte del personal
Información sensible sin cifrado
Ausencia o deficiencia en los sistemas de autenticación de los aplicativos
Deficiencia en la autorización de permisos de la información

c. Amenazas

Las Amenazas son las propuestas en **Matriz de Riesgos de Seguridad Digital**:

Amenazas
Fallas humanas
Pérdida de información
Falla en los sistemas
Hurto de información

d. Probabilidad

La Secretaría de las Tecnologías de la Información y de las Comunicaciones determina que la mejor manera de establecer la Probabilidad de ocurrencia de un incidente es por Factibilidad, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

Tabla 4 Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Esta es una tabla alternativa para mayor claridad:

Frecuencia de la actividad	Probabilidad	Calificación
Dos veces al año	Muy baja	1
Dos veces al mes	Baja	2
Dos veces a la semana	Media	3
Dos veces al día	Alta	4
Varias veces al día	Muy alta	5

e. Impacto

Teniendo en cuenta los tipos de datos recogidos en el Formato de registro nacional de bases de datos, la Secretaría de las Tecnologías de la Información y de las Comunicaciones determinó la siguiente tabla de impacto.

Tipo de Datos Personales	Impacto	Calificación
N/A	Muy bajo	1
N/A	Bajo	2
Datos generales	Medio	3
Datos socioeconómicos, Datos de ubicación, Otros datos	Alto	4
Datos sensibles, datos de identificación	Muy alto	5

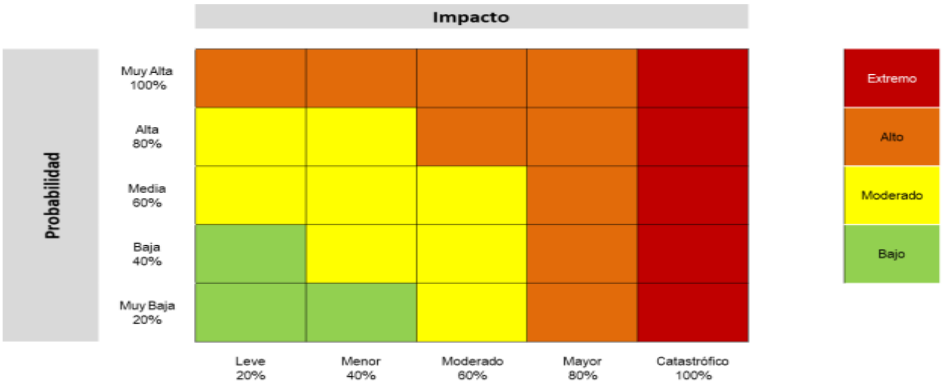
f. Zona de Riesgo = Probabilidad * Impacto

Permite determinar la severidad de un Incidente a partir del impacto y la probabilidad de su ocurrencia, así como también determinar el riesgo inherente de cada activo y asignar el responsable.

La probabilidad dirá cuál puede ser la ocurrencia del riesgo y el impacto inherente en la Gobernación de Bolívar sin tener presente los controles al materializarse, por lo que debe verse en el peor de los escenarios posibles.

En la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V7 de la Función Pública se obtiene:

Figura 14 Matriz de calor (niveles de severidad del riesgo)



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

g. Priorización

La priorización del establecimiento de controles será realizada con respecto a la criticidad del activo y el resultado de la Matriz de calor, es decir, la zona de riesgo.

h. Riesgo Inherente

Es el riesgo que se evalúa sin tener en cuenta la existencia ni el efecto de los controles asociados a los riesgos o sus causas.

3. Control

En esta etapa se realizan las acciones que se deben tomar para controlar o mitigar los riesgos a que se ven expuestos los datos personales con el fin de disminuir la posibilidad o las consecuencias de su materialización. Deben ser suficientes, efectivos y oportunos, identificar si son manuales, automáticos, discrecionales, obligatorios, preventivos o correctivos.

a. Establecer Controles

Finalmente, con base en la priorización se identifican los controles y se proponen a la dirección para su implementación:

b. Plan de tratamiento de Riesgos

El plan de tratamiento de riesgos establece que se debe tomar alguna de las siguientes acciones ante los riesgos encontrados.

1. Reducir el riesgo, establecer controles que mitiguen el impacto o la probabilidad.
2. Aceptar el riesgo mediante una elección informada.
3. Evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo.
4. Compartir el riesgo, utilizando un seguro.

c. Declaración de Aplicabilidad (SOA)

Es necesario indicar en cada control las justificaciones de la aplicación o elección de los controles, en éste también se justifica por qué no se eligieron los controles que hayan quedado por fuera, después del plan de tratamiento de riesgos.

Plan de Sensibilización

Finalmente se debe establecer un plan de Sensibilización en riesgos de tal manera que podamos incorporar a los usuarios en el sistema.

Esta actividad está descrita en el **Plan de capacitación sobre riesgos y controles en Datos Personales.**

d. Controles del Programa

Según la información necesaria para el registro de las bases de datos con Datos Personales, es necesario indicar si se tienen los siguientes controles:

"***MEDIDAS DE SEGURIDAD***,

Seguridad de la información personal

- *¿Tiene un documento de seguridad de la información personal o general aprobado? ( )*
- *¿Ha realizado documentación de procesos en torno a la seguridad de la información personal? ( )*
- *¿Tiene procedimientos de asignación de responsabilidades y autorizaciones en el tratamiento de la información personal? ( )*
- *¿Ha implementado acuerdos de confidencialidad con las personas que tienen acceso a la información personal? ( )*
- *¿Tiene controles de seguridad en la tercerización de servicios para el tratamiento de la información personal? ( )*

Sistema de Gestión de Seguridad de la Información

- *¿Tiene implementadas herramientas de gestión de riesgos en el tratamiento de datos personales? ( )*
- *¿Tiene implementado un sistema de gestión de seguridad de la información o un programa integral de gestión de datos personales? ( )*

Seguridad de la información personal en torno al recurso humano

- *¿Tiene implementados controles de seguridad de la información personal para el recurso humano antes de la vinculación y una vez finalizado el contrato laboral? ( )*

Control de acceso a la información personal

- *¿Tiene una política de control de acceso a la información personal, tanto en las instalaciones físicas como a nivel tecnológico? ( )*
- *¿Cuenta con un procedimiento para la gestión de usuarios con acceso a la información personal? ( )*
- *¿Ha implementado una política específica para el acceso a la información personal de las bases de datos con información personal sensible? ( )*
- *¿Tiene una política implementada de copia de respaldo de la información personal? ()*
- *¿Ha implementado una política de protección para el acceso remoto a la información personal? ( )*

Seguridad en los sistemas de información personal

- *¿Tiene implementado un procedimiento que contemple la definición de especificaciones y requisitos de seguridad de los sistemas de información personal? ()*

- *¿Tiene implementados controles de seguridad de la información durante el mantenimiento (Control de cambios) de los sistemas de información personal? ( )*
- *¿Tiene un procedimiento implementado de auditoría de los sistemas de información que contengan datos personales? ¿Las bases de datos con información personal poseen monitoreo de consulta? ( )*

Procesamiento de la información personal

- *¿Cuenta con una política implementada para el correcto tratamiento de la información personal en las diferentes etapas del ciclo de vida del dato (Recolección, circulación y disposición final)? ( )*
- *¿Cuenta con un procedimiento implementado para la validación de datos de entrada y procesamiento de la información personal, para garantizar que los datos recolectados y procesados sean correctos y apropiados, como confirmación de tipos, formatos, longitudes, pertinencia, cantidad, uso, etc.? ( )*
- *¿Cuenta con un control de seguridad de información para la validación de datos de salida? ( )*
- *¿Cuenta con una política implementada para el intercambio físico o electrónico de datos (como por ejemplo durante el comercio electrónico para la compra y venta de productos o servicios), transporte y/o almacenamiento de información personal? ( )*
- *¿Tiene un procedimiento o control implementado para la disposición final de la información personal (Supresión, archivo, destrucción, etc.)? ( )*

Gestión de incidentes de la información personal

- *¿Cuenta con una política y procedimientos implementados de gestión de incidentes de seguridad de la información personal? ( )*
- *¿Tiene implementada una política para mejorar la seguridad de la información personal a partir de los incidentes o vulnerabilidades detectados? ( )*

Auditorías de seguridad de la información personal

- *¿Tiene una política de auditorías de seguridad de la información personal? ( )*
- *¿Dentro de las auditorías de seguridad de información personal, tiene en cuenta el cumplimiento de requisitos, políticas y normas que específicamente le apliquen a la base de datos? ( )"*

MARCO NORMATIVO INTERNO

Las políticas de seguridad para la Gestión de datos personales de la Gobernación de Bolívar son complementadas con el documento "POLÍTICAS DE SEGURIDAD INFORMÁTICA"

- El decreto 531 de 2018 en el "Artículo 4. Control: La Dirección de Tecnologías de la Información y las Comunicaciones -TIC- s*erá 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 Publica de Protección de Datos Personales de la Gobernación de Bolívar".*
- *El decreto 531 de 2018 en el "Artículo 1: Adopta el Manual de Políticas y Procedimientos de Protección de Datos Personales de la Gobernación de Bolívar contenida en documento anexo, que hace parte integral del presente acto administrativo, contentiva de los lineamientos que garantizan la aplicación del marco normativo sobre la protección de datos personales establecida en la Ley 1581 de 2012 y sus decretos reglamentarios; el cual impone a todas las personas el deber de conocer actualizar y rectificar la información que se haya recogido sobre ellas en las bases de datos que maneja la Gobernación, garantizando que la información suministrada por estas, cuente con los principios que la rigen, como son la confidencialidad, integridad y disponibilidad.*"

  En el punto 2.10 Área Responsable de Atención de Peticiones, Consultas y Reclamos:

  "El responsable ha asignado a la DIRECCIÓN TIC como el responsable 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 y rectificar el dato.

  A su vez la Dirección TIC actuará como oficial de protección de datos, estará presta para dar cumplimiento 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: Via 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"*

El Oficial de Seguridad tiene la responsabilidad de planear, coordinar y comunicar a los delegados de las dependencias la información concerniente a las actividades necesarias en las etapas de recolección, almacenamiento, uso, circulación y eliminación o disposición final de los datos personales que reciben tratamiento en la Gobernación de Bolívar.

Oficial de Protección de Datos

***Función**: Velar por la implementación efectiva de las políticas y procedimientos adoptados por esta para cumplir las normas, así como la implementación de buenas prácticas de gestión de datos personales dentro de la organización.*

Tendrá la labor de estructurar, diseña y administrar el programa que permita a la Gobernación de Bolívar, cumplir las normas sobre protección de datos personales, así como establecer los controles de este programa, su evaluación y revisión permanente.

***Actividades**:*

- *Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales.*
- *Coordinar la definición e implementación de los controles del programa de gestión de datos personales.*
- *Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal del programa integral de gestión de datos personales.*
- *Impulsar una cultura de protección de datos dentro de la organización.*
- *Mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo.*
- *Registrar las bases de datos de la organización en el registro nacional de bases de datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la SIC.*
- *Obtener las declaraciones de conformidad de la SIC cuando sea requerido.*
- *Revisar los contenidos de los contratos de transmisiones internacionales de datos se suscriban con encargados no residentes en Colombia.*
- *Analizar las responsabilidades de cada cargo de la organización, para diseñar un programa de entrenamiento en protección de datos personales específico para cada uno de ellos.*
- *Realizar un entrenamiento general en protección de datos personales para todos los empleados de la compañía.*
- *Realizar el entrenamiento necesario a los nuevos empleados, que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización.*
- *Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización.*
- *Medir la participación y calificar el desempeño, en los entrenamientos de protección de datos.*

- *Requerir que, dentro de los análisis de desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre protección de datos personales.*
- *Velar por la implementación de planes de auditoría internos para verificar el cumplimiento de sus políticas de tratamiento de la información personal.*
- *Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la SIC.*
- *Realizar seguimiento al programa integral de gestión de datos personales.*
- El Programa Integral de Gestión de Datos Personales establecerá un cronograma de actividades tendientes a actualizar el RNBD anualmente.
- Los responsables de los Datos personales deben realizar la recolección, almacenamiento, uso, circulación y supresión o disposición final de la información personal, los requisitos para obtener la autorización de los titulares atendiendo a las directivas de la Guía para la Implementación del Principio de Responsabilidad Demostrada, la Ley 1581 del 2012 y las normas que la modifiquen.
- La Gobernación de Bolívar entrenará a las personas que internamente realicen tratamiento en protección de datos personales.
- Los responsables de los Datos Personales deberán informar al Oficial de Privacidad la información de las personas que realizarán Tratamiento de Datos Personales para realizar el respectivo entrenamiento, así como indicarles a las personas el deber del manejo responsable de los Datos Personales.
- La Gobernación de Bolívar entrenará a los delegados de las diferentes dependencias en protección datos personales.
- Los responsables de los Datos Personales deben identificar e indicar desde el proceso de diseño la información de los metadatos de las bases de datos con datos personales, el área encargada debe convocar para este proceso al Oficial de Privacidad.
- Los responsables de la información deben revisar los contratos de tratamiento de Datos Personales suscritos con los encargados.
- Los responsables de los Datos Personales deben incluir en todos los medios contractuales, las cláusulas, el acuerdo de confidencialidad y de manejo de información, donde se afirme que se conoce a suficiencia la política de la empresa, se acepta y se permite la compañía utilizar dicha información de forma responsable.
- Los responsables deben conocer que datos personales almacenan, como los utilizan y si realmente los necesitan, teniendo en cuenta la finalidad para la cual los recolectan.

- Los responsables deben identificar en que parte del procedimiento o actividad se obtienen los datos, si deben solicitar la autorización del titular y, de ser así, si están conservando prueba de esta para su posterior consulta.
- En los casos en que recolecten datos personales sensibles o datos de niños, niñas y adolescentes, es necesario:
    - Implementar las medidas adecuadas para garantizar una protección reforzada de dicha información.
    - Asegurarse de que se esté informando al titular o a quien corresponda (Cuando se trata de datos de menores) que no existe obligación de suministrar tales datos.
        - Sensible
        - Confidencial
        - Publica
- Para el registro de las Bases de Datos en RNBD es necesario establecer:
    - Encargado de la Base de Datos.
    - Forma de Tratamiento.
    - Tipo de información contenida.
    - Controles establecidos.
    - Información concerniente a la autorización del Titular.
    - Información sobre Transferencia o Transmisión de Datos Personales.
- Se realizará una capacitación al año a los Secretarios, Directores y Jefes de oficina de Datos Personales de las dependencias.
- Los Encargados de datos personales de la Gobernación de Bolívar se comprometerán a cumplir con la política de datos personales y firmar el correspondiente acuerdo de confidencialidad.
- El Oficial de Privacidad debe realizar la actualización de la información en la base de datos de los activos de información y en el RNBD.

4. Monitoreo

En esta etapa una vez al año se realizará seguimiento para velar porque las medidas que se hayan establecido sean efectivas, entre otros:

- Contemplar un proceso de seguimiento efectivo que facilite la rápida detección y corrección de las deficiencias en la administración de los riesgos identificados.
- Verificar que los controles estén funcionando en forma oportuna, efectiva y eficiente.

- Propender que los riesgos residuales se encuentren en los niveles de aceptación establecidos.

a. Presentación de Informes

Es esta actividad se recogen las evidencias y se documentan las actividades del programa Integral de Gestión de Datos Personales para realimentar el sistema y como parte de la información para el responsable de la Alta Dirección.

b. Plan de supervisión

El Plan de supervisión y revisión es anual, este se incluye dentro de las actividades del Plan de Datos Personales y se realizan actividades como: Calendario de revisión de documentación.

c. Indicadores

Los indicadores necesarios para evaluar la efectividad del presente documento son:

- Número de delegados entrenados.
- Número de encargados entrenados.
- Número de personas que realizan tratamiento entrenados.
- Número de Bases de Datos nuevas registradas.
- Número de controles nuevos establecidos.

d. Determinar Riesgo Residual

El ciclo PHVA establece que es necesario evaluar el proceso para determinar si han sido efectivos los controles, por lo tanto, se evalúan los controles con los indicadores, lo cual reinicia el proceso.

5. Protocolos de respuesta en el manejo de incidentes

El programa Integral de Gestión de Datos Personales establece una Política de Gestión de Incidentes de Seguridad de la Información Personal, en el cual se establecen medidas para la mitigación del impacto tales como informar a los titulares sobre incidentes relacionados con los datos personales.

REPORTE DE INCIDENTES:

CSIRT GOBIERNO

1. Identificado el incidente cibernético, por el CISO o encargado de seguridad digital de la entidad, diligenciar el formato de reporte de incidentes en su totalidad y enviarlo al CSIRT Gobierno para su gestión y acompañamiento.

2. Contactando a la mesa de servicio, llamando a la línea gratuita **018000910742**, Opción 2, seguridad digital.
3. Enviando un mensaje de correo electrónico informando el incidente al buzón csirtgob@mintic.gov.co, adjuntando el Formato de Reporte de Incidentes debidamente diligenciado.

COLCERT

- En caso de incidentes cibernéticos graves o muy graves deberán reportar dentro de los 15 días calendario siguientes a su detección al Colcert en el siguiente enlace formulario: https://www.colcert.gov.co/800/w3-article-198656.html
- Puede reportar un incidente o vulnerabilidad deberá escribir directamente a: Correo electrónico: contacto@colcert.gov.co
  Clave PGP/GPG: 0x8B134C7E
- Para enviar una muestra de malware se podrá escribir a:
  Correo electrónico: malware@colcert.gov.co
  Clave PGP/GPG: 0xEE3184F1

Adjuntar los siguientes datos:

1. **Información de contacto:**
   1. Nombre(s) y Apellido(s)
   2. País
   3. Zona horaria
   4. Número de Teléfono
   5. Correo electrónico
   6. Nombre de la Entidad (si aplica)
   7. Número de Teléfono de la entidad (si aplica)
   8. Número de Móvil
   9. Tipo de Organización:
      a. Gobierno
      b. Privada
      c. Operador de Infraestructura Crítica
   10. Tipo de Sector
   https://enciclopedia.banrepcultural.org/index.php?title=Sectores_econ%C3%B3micos
2. **Información del host(s) objetivo(s):**

1. Nombres de los hosts y direcciones IPs
2. Función del sistema (web server, mail server, etc.)
3. Sistema(s) Operativo(s)
4. Aplicaciones involucradas en el incidente

3. **Información del host(s) origen:**
    1. Nombres de los hosts y direcciones IPs
    2. Función del sistema (web server, mail server, etc.)
    3. Sistema(s) Operativo(s)
    4. Aplicaciones involucradas en el incidente
4. **Información del Incidente:**
    1. Fecha y hora (Timestamp)
    2. Zona horaria del Incidente
    3. Tipo de Incidente:
    4. Taxonomía (seleccione la clase y el tipo que aplique al incidente): https://www.colcert.gov.co/800/articles-198656_taxonomia.pdf

CAI VIRTUAL

También es necesario reportar a Cai Virtual de la Policía Nacional www.ccp.gov.co, https://adenunciar.policia.gov.co/Adenunciar/default.aspx

Centro Cibernético Policial de la Policía Nacional al teléfono 4266900 ext. 104092

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, indicando:

- Tipo de incidente
- Fecha en que ocurrió
- Fecha en la que se tuvo conocimiento del mismo
- Causal
- Tipo de datos personales comprometidos
- Cantidad de titulares afectados

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Todos los incidentes que comprometan datos personales deberán ser reportados a los Titulares dentro de los 30 días hábiles siguientes a su detección, e informarles:

- El incidente de seguridad relacionado con sus datos personales las posibles consecuencias.
- Proporcionar herramientas a dichos Titulares afectados para minimizar el daño potencial o causado.

La información correspondiente a la identificación, análisis, tratamiento de incidente debe ser socializada con el delegado de datos personales de la dependencia para aprovechar su conocimiento y establecer los posibles controles para los activos.

- El Oficial de Privacidad entregará un reporte semestral al representante legal de la empresa la evolución del riesgo, los controles implementados, el monitoreo y, en general, los avances y resultados del programa.
- El Oficial de Privacidad entregará un informe anual de los indicadores especificados en el Programa Integral de Gestión de Datos Personales.
- El Oficial de Privacidad revisará anualmente el Programa Integral de Gestión de Datos Personales y realizará los ajustes necesarios.

Indicadores de incidentes

- Número de incidentes donde se registre:
  - Bases de datos y datos comprometidos.
  - Riesgo
  - Vulnerabilidad
  - Amenaza
  - Titulares
  - Fecha del incidente.
  - Fecha de descubrimiento.
  - Acciones correctivas realizadas.
  - Responsables

CRONOGRAMA DE ACTIVIDADES

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 de dicados**
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**	Dirección TIC realizará entrenamientos **"Sensibilización y**	Dirección TIC, Secretarios,	02/05/2026	08/05/26	6

	Seguridad de la Información "	**definiciones Seguridad de la Información"**	Directores, Jefes			
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	Secretarios, Directores, Jefes	18/06/2026	24/06/26	4

		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.				
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 consolidaci**	Líderes, Secretarios, Directores, Jefes,	Secretarios,	10/07//26	25/07/26	15

	ón de información de Monitoreo	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	Directores, Jefes, Dirección TIC			

		datos y datos comprometidos, titulares, fecha del incidente y de descubrimiento, acciones correctivas realizadas y responsables.				
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 de Seguridad de la Información - Seguimiento y Aprobación de documentos
3. Dirección de Conectividad e Infraestructura Tecnológica- Diseño e Implementación. Acompañamiento Secretaria TIC.
4. Dependencias – Implementación.

Aprobación y revisión 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 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
Enero 26 de 2024	Tairo Mendoza Piedrahita Profesional Especializado Dirección TIC	1.0	• Versión Inicial
Marzo 03 de 2026	**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 **03/03/2026**	Laura Abuchar Camacho **Cargo:** Directora de Conectividad e Infraestructura Tecnologica **04/03/2026**	**Nombre**: Comité de Seguridad digital de la Gobernacion de Bolívar **Fecha**: 10/03/2026


NB ORDINE
LIBERTAS
GOBERNACIÓN
DE BOLÍVAR