



**PLAN DE TRATAMIENTO DE  
RIESGOS DE SEGURIDAD Y  
PRIVACIDAD DE LA  
INFORMACION  
2023**

***#Máscercamásvisible***



**PLAN DE TRATAMIENTO DE RIESGOS  
DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACION  
2023**

**DANIEL GUILLERMO ARENAS GAMBOA**

PERSONERO DE BUCARAMANGA

***#Máscercamásvisible***



## INTRODUCCIÓN

La Personería de Bucaramanga teniendo en cuenta las directrices del Ministerio TIC y la reglamentación propia al tema de seguridad y privacidad de la información formulará y aplicará el presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad.

Es fundamental definir y establecer un plan para la Entidad en la que se establezcan los parámetros y protocolos para salvaguardar la información. Diariamente se genera información confidencial y a su vez de interés general, la cual debe tener un tratamiento especial en cada caso, para así garantizar su privacidad y adecuado tratamiento.

## OBJETIVOS

### Objetivo general

Formular, desarrollar y poner en práctica el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la Personería de Bucaramanga y que sirva de referencia en cuanto al tratamiento de información propia de la Entidad, así como de usuarios externos.

### Objetivos específicos

- ✓ Diagnosticar el estado de la Entidad en materia de Tratamiento de Riesgos de seguridad y privacidad de la información.
- ✓ Aplicar las metodologías, mejores prácticas y recomendaciones dadas por la función pública y el MinTic para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información
- ✓ Optimización de los recursos de la institución en la aplicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información.



## ALCANCE

El plan de riesgos de seguridad y privacidad aplica a todos los procesos de la Entidad los cuales manejen, procesen o interactúen con información institucional.

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, que permita integrar en los procesos de la Entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos.

## RESPONSABLES

La estructura organizacional de los procesos responsables de la realización del plan es la siguiente:



Figura 1. Estructura organizacional de los procesos.



## MARCO CONCEPTUAL

**Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

**Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

**Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

**Ciberseguridad:** Capacidad del estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

**Confidencialidad:** Que la información solo sea accedida por las personas autorizadas para ello.

**Contratista externo:** Trabajador que, sin tener una vinculación laboral directa con la Personería de Bucaramanga, presta sus servicios para la Entidad (por ejemplo, a través de un contrato de prestación de servicios o por medio de una organización que tenga un contrato con la Entidad).

**Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las Entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).



**Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

**Entidad:** Término que se usa en el presente documento para identificar a la Personería de Bucaramanga.

**Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

**Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

**Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

**Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.

**Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

**Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

**Trazabilidad:** Calidad que permite que todas las acciones realizadas sobre



la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).

**Usuario:** Persona, proceso o aplicación de la Entidad autorizada para acceder a la información de la Entidad o a los sistemas que la manejan.

**Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

### MARCO NORMATIVO

- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública.
- Ley Estatutaria 1581 de 2012 - Protección de datos personales
- Decreto Nacional 2573 de 2014 - “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones”.

### DESCRIPCIÓN DEL PLAN

Para llevar a cabo la implementación en la Personería de Bucaramanga, se toma referencia la metodología PHVA (Planear, Hacer, Verificar y Actuar) o ciclo Deming, y los lineamientos emitidos por el Manual de implementación versión 3.02 del Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC.

De acuerdo con esto, se definen las siguientes fases de implementación:

1. Diagnosticar
2. Planear



**PERSONERÍA  
DE BUCARAMANGA**

**#Máscercamásvisible**

- 3. Implementar
- 4. Gestionar
- 5. Mejora continua.



Figura 2. Fuente: Modelo de Seguridad y Privacidad de la Información emitida por MinTIC

### FASE DE DIAGNÓSTICO - ETAPAS PREVIAS A LA IMPLEMENTACIÓN

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.



Figura 3. Fase de diagnóstico

- ✓ Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Personería.
- ✓ Determinar el nivel de madurez de los controles de seguridad de la información.
- ✓ Identificar el avance de la implementación del ciclo de operación al interior de la Entidad.
- ✓ Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- ✓ Identificación del uso de buenas prácticas en ciberseguridad.

### FASE DE PLANIFICACIÓN

Para el desarrollo de esta fase la Entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la Entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.



# PERSONERÍA DE BUCARAMANGA

**#Máscercamásvisible**

El alcance permite a la Entidad definir los límites sobre los cuales se implementará la seguridad y privacidad en la Personería. Este enfoque es por procesos y debe extenderse a toda la organización.

Para desarrollar el alcance y los límites del Modelo se deben tener en cuenta las siguientes recomendaciones: Procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos.

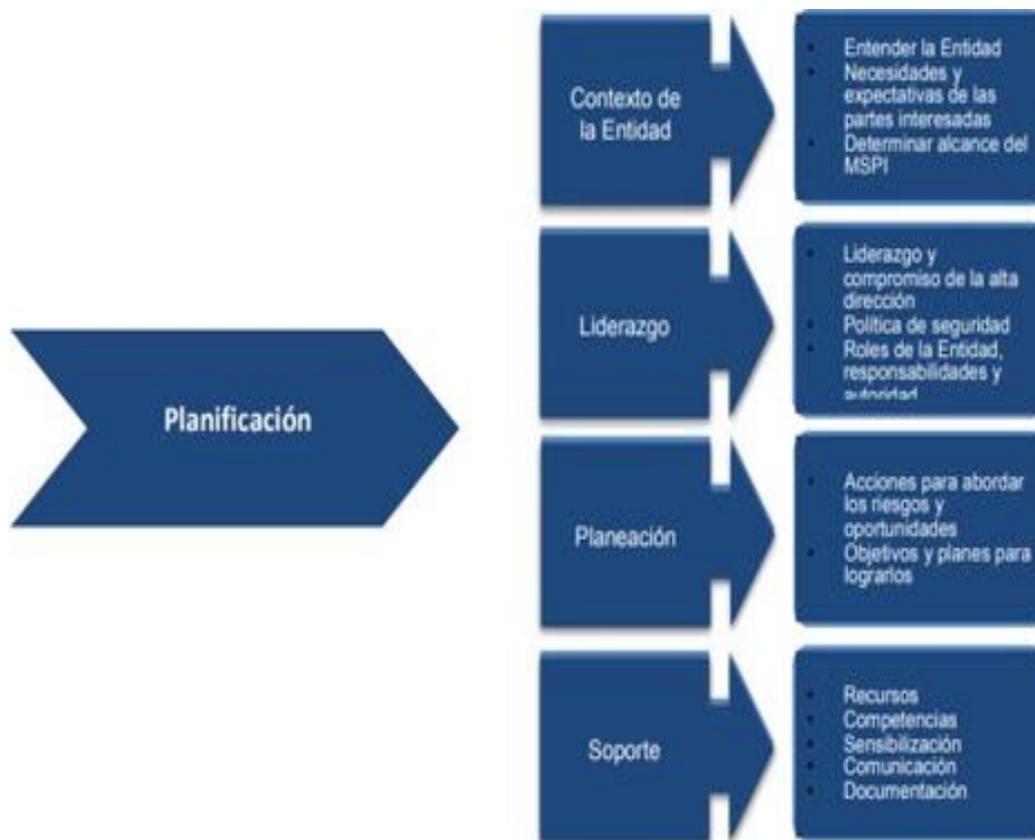


Figura 4. Fase de planificación

## FASE DE IMPLEMENTACIÓN

Esta fase le permitirá a la Personería de Bucaramanga llevar a cabo la implementación de la planificación realizada en la fase anterior.



Figura 5. Fase de implementación

## FASE DE EVALUACIÓN DE DESEMPEÑO

El proceso de seguimiento y monitoreo se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

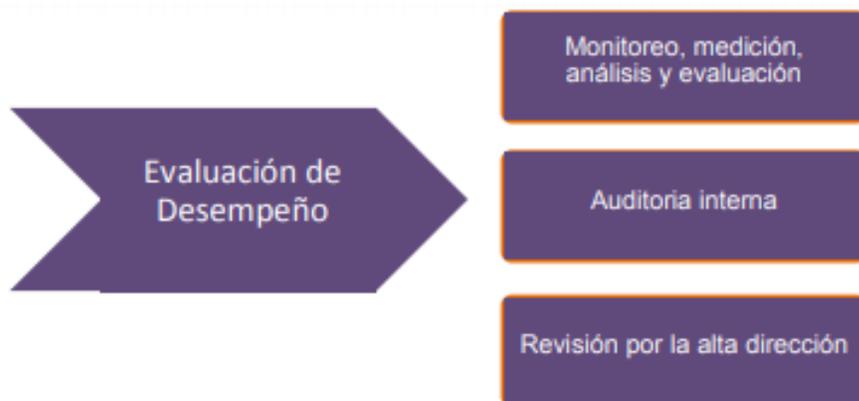


Figura 6. Fase de evaluación de desempeño

En esta actividad la Personería debe crear un plan que contemple las siguientes actividades:

- Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
- Seguimiento a la programación y ejecución de las actividades de autorías internas y externas
- Seguimiento al alcance y a la implementación
- Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la Entidad.
- Medición de los indicadores de gestión
- Revisiones de acciones o planes de mejora

Este plan deberá permitir la consolidación de indicadores periódicamente y su evaluación frente a las metas esperadas; deben ser medibles permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI.



**PERSONERÍA  
DE BUCARAMANGA**

**#Máscercamásvisible**

## FASE DE MEJORA CONTINUA



En esta fase la Personería debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

### ACTIVIDADES

- Socialización del Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información.
- Reevaluar los Riesgos identificados con los líderes del Proceso.
- Socialización de los riesgos identificados.

**CRONOGRAMA**

<b>CRONOGRAMA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>												
<b>Actividad</b>	<b>Enero - Marzo</b>			<b>Abril - Junio</b>			<b>Julio - Septiembre</b>			<b>Octubre - Diciembre</b>		
	<b>1</b>	<b>2</b>	<b>3</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>1</b>	<b>2</b>	<b>3</b>
Socialización del plan de tratamiento de riesgos de seguridad y privacidad	■	■	■									
Reevaluar los riesgos identificados				■	■	■						
Socialización de los riesgos identificados							■	■	■			
Actualizar políticas y/o planes de acuerdo a la normatividad vigente para la fecha.										■	■	■
Seguimiento y Control	■	■	■	■	■	■	■	■	■	■	■	■

**SEGUIMIENTO Y EVALUACIÓN**

Al finalizar cada etapa se realizará una reunión con el Personero de Bucaramanga y la Secretaría General para presentar el informe del avance del proyecto y de esta manera evaluar todos los pasos que se han ido realizando.