Personería de Floridablanca

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

FLORIDABLANCA, ENERO DE 2025

Personería de Floridablanca

CONTENIDO

INTRODUCCIÓN 3
TÉRMINOS Y DEFINICIONES 4
OBJETIVOS 7
  OBJETIVO GENERAL 7
  OBJETIVOS ESPECÍFICOS 7
ALCANCE 7
METODOLOGÍA DE IMPLEMENTACIÓN 7
FASE DE DIAGNÓSTICO - ETAPAS PREVIAS A LA IMPLEMENTACIÓN 8
  FASE DE PLANIFICACIÓN 9
  FASE DE IMPLEMENTACIÓN 10
  FASE DE EVALUACIÓN DE DESEMPEÑO 10
  FASE DE MEJORA CONTINUA 11
ACTIVIDADES PARA LA IMPLEMENTACIÓN 11
CUMPLIMIENTO DE IMPLEMENTACIÓN 12
TABLA DE CONTROL DE REVISIONES Y MODIFICACIONES 12

Personería de Floridablanca

INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la Entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer las situaciones que pueden comprometer el cumplimiento de los objetivos trazados del entorno TIC.

La Personería Municipal de Floridablanca., como entidad pública y de servicio al ciudadano, intercambia constantemente información con entidades públicas y privadas, así como con la ciudadanía en general. La información recibida de entidades y personas es fundamental para el desarrollo de sus funciones, y con base en ella se toman decisiones y se ejecutan acciones que pueden resultar en comunicados, resoluciones, oficios, etc. Esta información puede ser de carácter público para conocimiento de la ciudadanía o puede tratarse de investigaciones altamente confidenciales dentro de sus procesos misionales. Por ello, es crucial identificar claramente el tipo de información que se está procesando para determinar los riesgos a los que está expuesta y protegerla adecuadamente.

De igual manera el Modelo de Seguridad y Privacidad de la Información – MSPI, de la Política de Gobierno Digital de MINTIC, establece metas, resultados y entregables correspondientes a cada una de las fases de implementación del SGSI en sus fases de Planificación e Implementación, las cuales deben ser tenidas en cuenta.

Basado en la norma ISO31000 y el Modelo de Seguridad y Privacidad de la Información – MSPI, de la Política de Gobierno Digital de MINTIC, la Personería Municipal de Floridablanca. Establece el plan de trabajo para el año 2025 mediante el cual se adelantarán las actividades correspondientes para identificar, valorar y gestionar los riesgos de seguridad de la información en la entidad.

Personería de Floridablanca

TÉRMINOS Y DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Acciones asociadas:** son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.
- **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
- **Amenaza:** situación externa que no controla la entidad y que puede afectar su operación.
- **Análisis del riesgo**: etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente). · Asumir el riesgo: opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
- **Causa:** medios, circunstancias y/o agentes que generan riesgos.
- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- **Compartir o transferir el riesgo:** opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.
- **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.
- **Contexto estratégico:** son las condiciones internas y del entorno, que pueden generar eventos que originen oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
- **Control:** acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
- **Control preventivo:** acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.

- **Control correctivo:** acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.
- **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.
- **Evaluación del riesgo:** resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
- **Evitar el riesgo:** opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificados.
- **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- **Identificación del riesgo:** etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos.
- **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.
- **Mapa de riesgos:** documento que, de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
- **Materialización del riesgo:** ocurrencia del riesgo identificado.
- **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
- **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio.
- **Probabilidad:** medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.
- **Procedimiento:** conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
- **Proceso:** conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de

evaluación.

- **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.
- **Riesgo de corrupción:** posibilidad de que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
- **Riesgo inherente:** es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.
- **Riesgo institucional:** Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:

  - Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.

  - Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.

  - Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.
- **Riesgo de corrupción:** todos los riesgos identificados que hagan referencia a situaciones de corrupción, serán considerados como riesgos de tipo institucional.
- **Riesgo residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.
- **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si se necesita.

Personería de Floridablanca

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 Municipal de Floridablanca que reduzca al mínimo los riesgos de pérdida de activos de información

OBJETIVOS ESPECÍFICOS

- Establecer controles de seguridad en la información para asegurar su confidencialidad, integridad y disponibilidad.
- 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
- Desarrollar un plan de trabajo para la implementación de planes de eliminación de riesgos de seguridad y privacidad de la información.

ALCANCE

Este documento, proporciona el plan de trabajo para desarrollar la administración y gestión de los riesgos de seguridad de la información a nivel de los procesos en la Entidad, desde la identificación de los riesgos de seguridad de la información hasta la definición del plan de tratamiento, responsables y fechas de implementación

METODOLOGÍA DE IMPLEMENTACIÓN

La Personería Municipal de Floridablanca, en alineación con los lineamientos del Gobierno Nacional, cumple con la Ley de Transparencia 1712 de 2014. Este programa impulsa a las entidades públicas a ajustarse a modelos y estándares que garanticen la seguridad de la información, conforme al Decreto 1078 de 2015.

La metodología de gestión de riesgos, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que: el concepto de riesgo, así como el contexto, se planean mediante la programación de acciones y controles que permiten reducir la afectación a la Entidad en caso de materialización. Adicional, busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer las situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el entorno de las TIC.

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la Personería Municipal de Floridablanca, se toma referencia la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Manual de implementación versión 3.02 del Ministerio de Tecnologías de la

Información y las Comunicaciones.

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

- ***Diagnosticar.***
- ***Planear.***
- ***Hacer.***
- ***Verificar.***
- ***Actuar.***

FASE DE DIAGNÓSTICO - ETAPAS PREVIAS A LA IMPLEMENTACIÓN

En esta etapa, se busca evaluar el estado actual de la organización en relación con los requisitos del Modelo de Seguridad y Privacidad de la Información.

En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

1. Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad
2. Determinar el nivel de madurez de los controles de seguridad de la información.
3. Identificar el avance de la implementación del ciclo de operación al interior

de la entidad.

4. Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
5. Identificación del uso de buenas prácticas en ciberseguridad

Para llevar a cabo esta etapa, las Personeria Municipal de Floridablanca recopila la información con la ayuda de una herramienta de diagnóstico y una metodología de pruebas de efectividad.

FASE DE PLANIFICACIÓN

Para llevar a cabo esta etapa, la entidad debe emplear los resultados de la fase previa y proceder a desarrollar el plan de seguridad y privacidad de la información, alineado con el objetivo misional de la entidad. El propósito es definir las acciones a implementar en términos de seguridad y privacidad de la información, mediante una metodología de gestión del riesgo.

El alcance del Modelo de Seguridad y Privacidad de la Información (MSPI) permite a la entidad definir los límites dentro de los cuales se implementarán las medidas de seguridad y privacidad. Este enfoque está basado en procesos y debe extenderse a toda la entidad.

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.

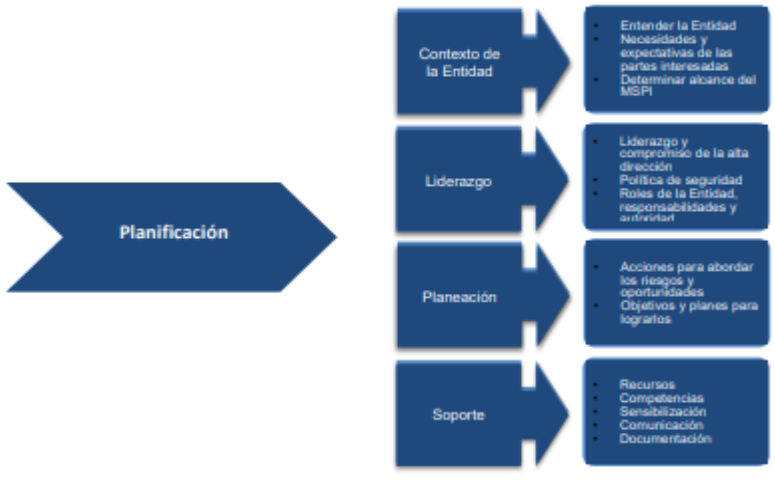

Figura 3 - Fase de planificación[1]

Los resultados de la fase de Diagnóstico previas a la implementación deben ser revisados y socializados por las partes interesadas.

FASE DE IMPLEMENTACIÓN

Esta fase le permitirá a la Entidad, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI

Figura 4 - Fase de implementación[2]

La entidad debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información, permitiendo así la implementación de las acciones definidas en el plan de tratamiento de riesgos.
Es esencial que la entidad mantenga información documentada en la medida necesaria para garantizar que los procesos se lleven a cabo según lo planificado. Además, se debe llevar un control de cambios para tomar acciones que mitiguen efectos adversos cuando sea necesario.

FASE DE EVALUACIÓN DE DESEMPEÑO

El proceso de seguimiento y monitoreo del Modelo de Seguridad y Privacidad de la Información (MSPI) se basa en los resultados obtenidos a partir de los indicadores de seguridad de la información. Estos indicadores permiten verificar la efectividad, eficiencia y eficacia de las acciones implementadas.

1. En esta actividad la Personería debe crear un plan que contemple las siguientes actividades: a. Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
2. Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
3. Seguimiento a la programación y ejecución de las actividades de autorías internas y externas
4. Seguimiento al alcance y a la implementación
5. 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.
6. Medición de los indicadores de gestión

7. Revisiones de acciones o planes de mejora

FASE DE MEJORA CONTINUA

En esta etapa, la entidad debe consolidar los resultados obtenidos de la fase de evaluación de desempeño. Esto se hace para diseñar un plan de mejoramiento continuo de la seguridad y privacidad de la información. Además, se deben tomar acciones oportunas para mitigar las debilidades identificadas.

ACTIVIDADES PARA LA IMPLEMENTACIÓN

ACTIVIDAD	FECHA DE INICIO	FECHA FIN
Actualizar políticas y metodología de gestión de Riesgos	ENERO	ENERO
Socialización guías y herramientas gestión de riesgos del SGSI y continuidad de la operación	FEBRERO	MARZO
Identificación de los puntos de riesgo	MARZO	ABRIL
Seguimiento estado planes de tratamiento de riesgos identificados y verificación evidencias	MAYO	JUNIO
Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	JULIO	AGOSTO
Actualizar políticas y metodología de gestión de riesgos de acuerdo a los cambios solicitado	ENERO	DICIEMBRE
Seguimiento y control	ENERO	DICIEMBRE
Generación, presentación y reporte de indicadores	OCTUBRE	NOVIEMBRE

Personería de Floridablanca

CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo con las fases mencionadas anteriormente, se describen a continuación los dominios que se deben ejecutar y los plazos de implementación de acuerdo a lo establecido por la Personería Municipal de Floridablanca:

- Continuar con la ejecución de la Política de Seguridad de la Información.
- Seguridad de la Información enfocada a los recursos humanos.
- Fiscalización de los controles de acceso.
- Seguridad en las telecomunicaciones.
- Aspectos organizativos de la seguridad de la información.
- Gestión de Incidentes de Seguridad de la Información

TABLA DE CONTROL DE REVISIONES Y MODIFICACIONES

CONTROL DE REVISIONES							
NO	**FECHA**	**DESCRIPCIÓN**	**ELABORO**	**CARGO**	**REVISO**	**APROBO**	**CARGO**
1.	21 de Enero de 2025	Actualización del Plan	Henry Alberto Restrepo Gamboa	Dirección de Gestión Administrativa y Financiera	Henry Alberto Restrepo Gamboa	María Alejandra Ramírez Ayala	Personera Municipal (E)
			FIRMAS				

HENRY ALBERTO RESTREPO GAMBOA
Dirección de Gestión Administrativa y Financiera