PERSONERIA MUNICIPAL DE FLORIDABLANCA

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

FLORIDABLANCA, ENERO DE 2021

INTRODUCCIÓN

El presente **PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**, se proyecta con el fin de ejecutar la implementación y socialización del Gobierno digital, en el Eje temático de la estrategia en **seguridad y privacidad de la información**, en busca de la protección de los datos de los ciudadanos para garantizar la seguridad de la información de la Personería Municipal de Floridablanca.

El no contar con una buena gestión de la seguridad de la información, para la entidad puede traer consecuencias graves, como pérdida fuga o robo de información, alteración de documentos, negación de servicios etc.

1. 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 identificado.

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.

- **Los riesgos 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.

2. OBJETIVO

Mitigar los riesgos informáticos de la Personería Municipal de Floridablanca, con el fin de salvaguardar los activos de información, el manejo de medios, el control de acceso y la gestión de los usuarios.

2.1. OBJETIVOS ESPECÍFICOS

✔ Establecer los controles y políticas de la seguridad de la información que garantice la confidencialidad integridad y disponibilidad de la misma.

✔ Realizar un plan de trabajo para la implementación del plan de tratamiento de riesgo de seguridad y privacidad de la información.

3. RECURSOS

- Humano: Personera Municipal, Líderes de los Procesos, funcionario y/o contratista encargado de las TICS
- Físico: PC y equipos de comunicación

4. RESPONSABLES

- Personera Municipal
- Líderes de los Proceso
- Funcionario y/o contratista encargado de las TICS

5. METODOLOGÍA DE IMPLEMENTACIÓN

Definir el contexto estratégico marca la pauta o ruta que la entidad debe asumir frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos, evitando establecer las condiciones ideales para la materialización.

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 del MSPI:

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

Ilustración 1 Ciclo de operación del Modelo de Seguridad y Privacidad de la Información
Fuente: Manual Modelo de seguridad y Privacidad de la Información – MinTIc

6. ACTIVIDADES PARA LA IMPLEMENTACIÓN

La Personería Municipal de Floridablanca, adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, con el fin de:

1. Conocer y cumplir la política de seguridad de la información de la entidad.

2. Replicar con sus equipos de trabajo fortaleciendo el trabajo mancomunado con la oficina de tecnología fortaleciendo la conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.

3. Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto para mitigar y lograr lo mencionado anteriormente es necesario que sean asignados recursos humanos, presupuestales y tecnológicos que permitan cerrar las brechas detectadas y mejorar los controles existentes.

7. 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

- ✔ Ejecutar 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

8. CRONOGRAMA

No.	ACTIVIDAD	RESPONSABLE	FECHA DE IMPLEMENTACIÓN
1.	Elaborar el Diagnóstico	Directora de Gestión Administrativa y Financiera	Marzo 2021
2.	Proyectar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información	Directora de Gestión Administrativa y Financiera	Abril 2021

3.	Elaborar un Inventario de Activos de Información con los líderes de cada Proceso	Directora de Gestión Administrativa y Financiera	Mayo 2021
4.	Hacer la Valoración de los Activos de Información con los líderes de cada Proceso	Líderes de proceso	Junio 2021
5.	Ejecutar el Plan de tratamiento de los riesgos (Riesgo Inherente y Riesgo Residual)	Directora de Gestión Administrativa y Financiera	Agosto 2021
6.	Socializar el Plan de Tratamiento de Riesgo	Directora de Gestión Administrativa y Financiera	Septiembre 2021
7.	Hacer seguimiento del Plan de Tratamiento de Riesgo	Directora de Gestión Administrativa y Financiera	Octubre 2021

9. SEGUIMIENTO y EVALUACIÓN

Al finalizar cada etapa se concluirá con una reunión con la alta dirección y el equipo de trabajo, para presentar el informe de avance a la implementación del PTR y de esta manera evaluar todas las actividades propuestas en dicho plan.

10. ENTREGABLES

- ✔ Informe de avance al PTR
- ✔ Actas de Reunión.
- ✔ Plan de tratamiento de riesgo aprobado por los líderes
- ✔ Política de Seguridad
- ✔ Evidencias de la socialización con funcionarios de la entidad

MARIA MARGARITA SERRANO ARENAS
Personera Municipal (e)

Revisó: Diana Carolina Duarte - DGAF