

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

PERSONERIA MUNICIPAL DE FLORIDABLANCA

ENERO DE 2019



CONTENIDO

| Int | trod | ucción | 3 |
|-----|------|------------------------------------|------|
| | 1. | Términos y definiciones | 3-4 |
| | 2. | Objetivo | 5 |
| | | l Objetivo Específico | |
| | | Recursos | |
| | 4. | Responsables | 5 |
| | 5. | Metodología de Implementación | .5-6 |
| | 6. | Actividades para la Implementación | 7 |
| | 7., | Cumplimiento de la Implementación | 7 |
| | 8. | Cronograma | .8-9 |
| | 9. | Seguimiento y Evaluación | 9 |
| | 10 | . Entregables | 9 |



INTRODUCCION

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.

1. TERMINOS Y DEFINICIONES

- > Acceso a la Información Pública: Consiste en la facultad que tienen todos los ciudadanos de conocer y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014 art. 4).
- > Activo: En relación con la seguridad de la información, hace referencia a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...), que tenga valor para la entidad. (ISO/IEC 27000).
- Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- > Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- Confidencialidad: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000)
- ➤ Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- > 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).

- ▶ Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000).
- ➤ 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).
- > Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000).
- Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- ➢ Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- Privacidad: En el contexto de este documento, por privacidad se entiende, el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o, esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación.
- Procedimiento: Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.
- ➢ 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).



2. OBJETIVO

Conocer y supervisar los riesgos asociados a los procesos existentes 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 ESPECIFICOS

- Realizar un plan de trabajo para la implementación del plan de tratamiento de riesgo de seguridad y privacidad de la información.
- Emplear las metodologías del DAFP o de la ISO respectivamente en seguridad y riesgo de la información.

3. RECURSOS

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

4. RESPONSABLES

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

5. METODOLOGÍA DE IMPLEMENTACIÓN

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:

- 1. Diagnosticar
- 2. Planear
- 3. Hacer
- 4. Verificar
- 5. 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 – MinTlc



6. ACTIVIDADES PARA LA IMPLEMENTACION

- 1. Elaborar el Diagnóstico
- 2. Proyectar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información
- 3. Elaborar un Inventario de Activos de Información con los líderes de cada Proceso
- 4. Hacer la Valoración de los Activos de Información con los líderes de cada Proceso
- 5. Ejecutar el Plan de tratamiento de los riesgos (Riesgo Inherente y Riesgo Residual)
- 6. Socializar el Plan de Tratamiento de Riesgo
- 7. Hacer seguimiento del Plan de Tratamiento de Riesgo

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.
- Aspectos organizativos de la seguridad de la información
- Seguridad de la Información enfocada a los recursos humanos
- · Fiscalización de los Controles de acceso
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.



8. CRONOGRAMA

| No. | ACTIVIDAD | RESPONSABLE | FECHA DE IMPLEMENTACION |
|-----|--|---|-------------------------|
| 1. | Elaborar el Diagnóstico | Directora de Gestión Administrativa y Financiera | Abril de 2019 |
| 2. | Proyectar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información | Directora de Gestión Administrativa y Financiera | Mayo de 2019 |
| 3. | Elaborar un Inventario de Activos de Información con los líderes de cada Proceso | Directora de Gestión Administrativa y Financiera | Mayo de 2019 |
| 4. | Hacer la Valoración de los Activos de Información con los líderes de cada Proceso | Líderes de proceso | junio de 2019 |
| 5. | Ejecutar el Plan de tratamiento de los riesgos (Riesgo Inherente y Riesgo Residual) | Directora de Gestión Administrativa y Financiera | Julio de 2019 |
| 6. | Socializar el Plan de Tratamiento de Riesgo | Directora de Gestión Administrativa y Financiera | julio de 2019 |



| 7. | Hacer seguimiento del Plan de Tratamiento de Riesgo | Directora Gestión Administrativa Financiera | de y | Julio de 2019 | |
|----|--|--|---------|---------------|--|
|----|--|--|---------|---------------|--|

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.

11

10. ENTREGABLES

- ❖ Informe de avance al PTR
- Actas de Reunión.
- Plan de tratamiento de riesgo aprobado por los lideres
- Política de Seguridad
- Productos de cada etapa

LUIS JOSE ESCAMILLA MORENO

Personero Municipal

Proyectó: LDFM -TA Revisó: MMC - DGAF

to a second above that of the con-

ESPACIONE THE SER

the second secon

same to see specific unit and discussion in the a

beding of an explore of

SO VENEZA CARREST TO THE STATE OF STATE

· me