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

ANA MARIA AGUIRRE BETANCUR

PERSONERA MUNICIPAL

PERSONERÍA DE RIONEGRO

(ANTIOQUIA)

2021

CONTENIDO

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

INTRODUCCIÓN

La Personería Municipal de Rionegro, distingue el papel fundamental que tiene la información en el cumplimiento de los procesos, por esta razón, se reconoce la relevancia para cumplir con un manejo adecuado a la información brindando la protección idónea; así mismo, se debe reconocer el valor que tienen las acciones que se derivan desde la entidad, como lo son los acuerdos de confidencialidad que se plasman en los contratos y las demás acciones que por su valoración deban estar bajo una administración de custodia que le impida ser conocida por las demás personas que no hagan parte del proceso.

La seguridad que se le da a la información tiene un pilar que es la protección de los activos de información, para prevenir una amenaza que violente los principios fundamentales de confidencialidad, integridad y disponibilidad; así pues, se debe propiciar la creación de sistemas adecuados de protección de la información para evitar que incrementen los riesgos y que la información se use de la manera debida para brindar un proceso efectivo.

Por ende, el plan de tratamientos de riesgos se realiza con la finalidad de conocer cómo se realizará la implementación, con los requisitos del componente de Gobierno digital, que busca dar protección a los datos de las personas tanto jurídicas como naturales, brindando una seguridad en la información que se da a conocer y sobre todo asumiendo los retos que trae la tecnología día a día, actualizando los planes de acción a la era digital.

1. TÉRMINOS Y DEFINICIONES

1.1. Seguridad de la información: "consiste en asegurar que los recursos del sistema de información de una empresa se utilicen de la forma que ha sido decidido y el acceso de información se encuentra contenida, así como controlar que la modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización." (SGSI,2015).

1.2. Privacidad: "se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos pueden ser compartidos con terceros en un sistema informático." (SDC, 2014)**.**

1.3. 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, entre otros) que tenga valor para la organización. (ISO/IEC 27000).

1.4. Activo de información: "algo que una organización valora y por lo tanto debe proteger" (ISO/IEC 27001).

1.1. Habeas data: acción de derecho constitucional, que confirma a cualquier persona solicitar a una persona natural o jurídica en obtener la información que existe en su nombre y solicitar eliminarla, corregirla o no compartirla.

1.5. 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).

1.6. Confidencialidad: Ee la garantía de acceso a la información de los usuarios que se encuentran autorizados para tal fin. (2.13 ISO 27000).

1.7. Integridad: es la preservación de la información completa y exacta. (2.36 ISO 27000).

1.2. Disponibilidad: es la garantía para que el usuario acceda a la información que necesita en ese preciso momento. (2.10 ISO 27000).

1.8. Protección de datos: “es el proceso de proteger la información importante de la corrupción y/o pérdida” (SDC, 2016).

1.9. Análisis de riesgo: proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

1.10. Amenazas: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

1.11. 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)

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Mitigar y revisar los riesgos que se relacionen con los procesos que existen en la Personería Municipal de Rionegro, tomando como finalidad la protección de los activos de valor, controlando el acceso a la información, manejo de medios y gestión en los usuarios.

2.2. OBJETIVOS ESPECIFICOS

2.2.1. Crear un plan de trabajo específico para la implementación de mecanismos de gestión de riesgos de seguridad y privacidad de la información.

2.2.2. Definir los principales activos de valor que se manejan mediante la información en la entidad.

2.2.3. Identificar las principales amenazas que puedan afectar los activos de valor de la información.

2.2.4. Aplicar las metodologías propuestas por DAPF o la ISO en seguridad y privacidad de la información.

2.2.5. Proponer soluciones para minimizar el riesgo al cuál se exponen los activos de valor de la información.

3. ALCANCE

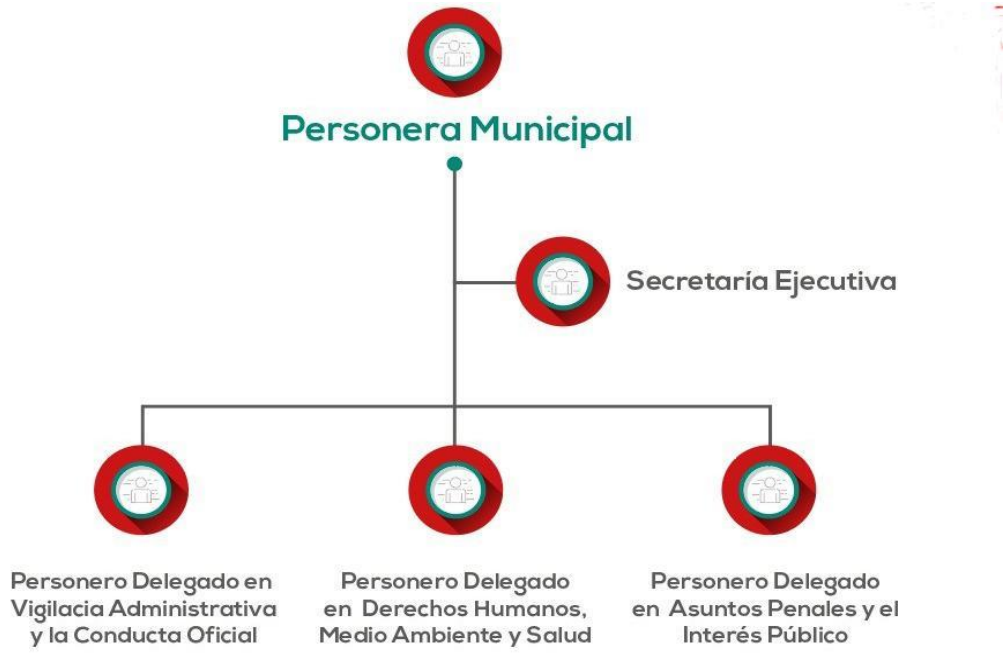
El presente plan de tratamiento de riesgos de seguridad y privacidad de riesgos regirá y se aplicará a todos los procesos estratégicos propuestos por la Personería Municipal de Rionegro.

4. RECURSOS

- **Personal:** Personera municipal, personeros delegados, líderes de los procesos, abogados, funcionarios, contratistas, equipo de comunicación, informático en sistemas.

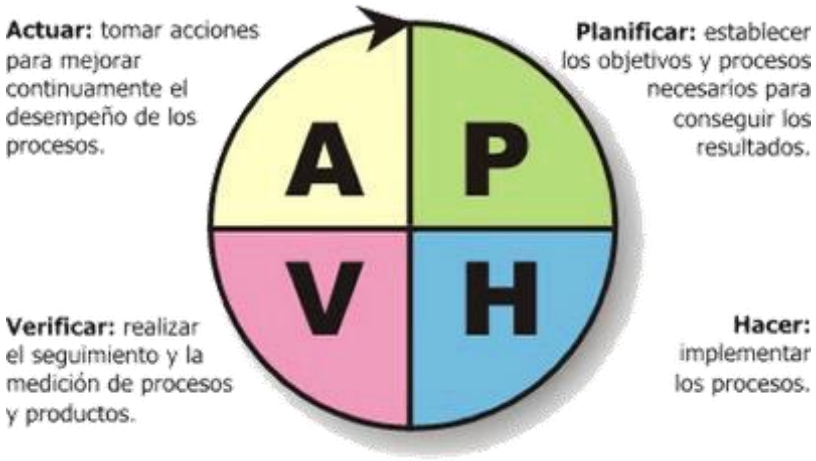
- **Físico:** implementos de trabajo, computadores y equipos de comunicaciones.

5. RESPONSABLES



6. METODOLOGÍA DE IMPLEMENTACIÓN

Para realizar el presente plan de tratamientos de riesgos de seguridad y privacidad de la información se tomará como pilar los lineamientos dados por el Ministerio de Tecnologías consignado en el Manual 3.02 de la información, las comunicaciones; igualmente se implementará la metodología PHVA:



7. ACTIVIDADES PARA LA IMPLEMENTACIÓN

- ✓ Realizar un diagnóstico que permita la identificación de los riesgos.
- ✓ Realizar el plan de tratamiento de riesgos y privacidad de la información basados en unos alcances y lineamientos para una mayor efectividad.
- ✓ Proponer un inventario donde se evidencie cuáles son los activos de información que pertenecen a los procesos que se llevan a cabo por los líderes de la entidad.
- ✓ Hacer una valoración en orden prioridad de los activos de información.
- ✓ Identificar los diferentes riesgos que puedan existir.
- ✓ Dar a conocer el plan de tratamiento de riesgos por los funcionarios, contratistas y terceros que intervengan en la entidad.

- ✓ Realizar un balance y seguimiento evaluativo del plan de tratamientos de riesgos de la seguridad y privacidad de la información, para que periódicamente se puedan identificar los puntos a potencializar.

8. CUMPLIMIENTO DE LA IMPLEMENTACIÓN

Teniendo en cuenta las actividades enumeradas anteriormente, se trazarán los acuerdos que se deben realizar y los debidos plazos que se darán para que estos se implementen, además de resaltar los parámetros actualmente existentes en seguridad y privacidad de la información para que los mismos sean optimizados.

- ✓ Implementar las políticas existentes y planteadas en este plan sobre la seguridad que debe brindarse a la información.
- ✓ Realizar esquemas organizacionales para resaltar la protección de la información.
- ✓ Proporcionar contraseñas a los equipos de cómputo y de comunicación de los funcionarios y contratistas de la entidad, para brindar una mayor seguridad a la información.
- ✓ Continuar con la prohibición de colocar USB o demás dispositivos externos no aprobados a los equipos de cómputo y de comunicación de los funcionarios y contratistas de la entidad.
- ✓ Seguir compartiendo o recibiendo la información por un único medio (correo electrónico) no permitiendo que estas acciones se realicen por medio de USB, discos, etc.
- ✓ Revisar los controles de acceso de la información.
- ✓ Enfocar la seguridad de la información igualmente en los recursos humanos.
- ✓ Proporcionar una seguridad en los medios de comunicaciones.
- ✓ Hacer cambios periódicos de las contraseñas de los equipos y correos institucionales para fomentar la seguridad de la información.

9. SEGUIMIENTO Y EVALUACIÓN

Después de la realización de cada actividad, en cada periodo se propondrá realizar una reunión entre el equipo encargado de la acción para así presentar los avances obtenidos y poder optimizar el plan, brindando cada vez más efectividad en el mismo.