CONTRALORIA
Municipal de Bucaramanga

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD

Vigencia 2024

SECRETARIA GENERAL

1. INTRODUCCION

La Contraloría Municipal 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, garantizar su privacidad y adecuado tratamiento.

2. DEFINICIONES

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Riesgo de Seguridad de la Información: 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).

Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

Impacto: consecuencias que puede ocasionar a la organización la materialización del riesgo.

Control o Medida: Medida que permite reducir o mitigar un riesgo.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Formular, desarrollar y poner en práctica el Plan de Tratamiento de Riesgos de Seguridad y Privacidad para la Contraloría Municipal de Bucaramanga para que sirva de referencia en cuanto al tratamiento de información propia de la entidad así como de usuario externos.

3.2 OBJETIVOS ESPECÍFICOS

Diagnosticar la entidad en lo que realmente tiene 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 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 tratamientos de riesgos de seguridad y privacidad de la información..

4. 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.

5. RESPONSABLES

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

Figura 1. Estructura Organizacional

- Contralor Municipal de Bucaramanga
- Secretaria General
- Asesor de Planeación
- Técnico

6. 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 ciudadano, ante amenazas o incidentes de naturaleza cibernética.

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).

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: Cualidad 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).

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

7. 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

8. IMPLEMENTACIÓN DEL PLAN

Identificación del riesgo:

Se implementaran encuestas a los funcionarios de la entidad para determinar los riesgos en cuanto al manejo de la información generada por cada uno de ellos, así como de la documentación colectiva.

De acuerdo a los lineamientos otorgados por MinTic se aplicarán las matrices de medición del riesgo de la entidad, actividad que se realizará con los líderes de procesos involucrados.

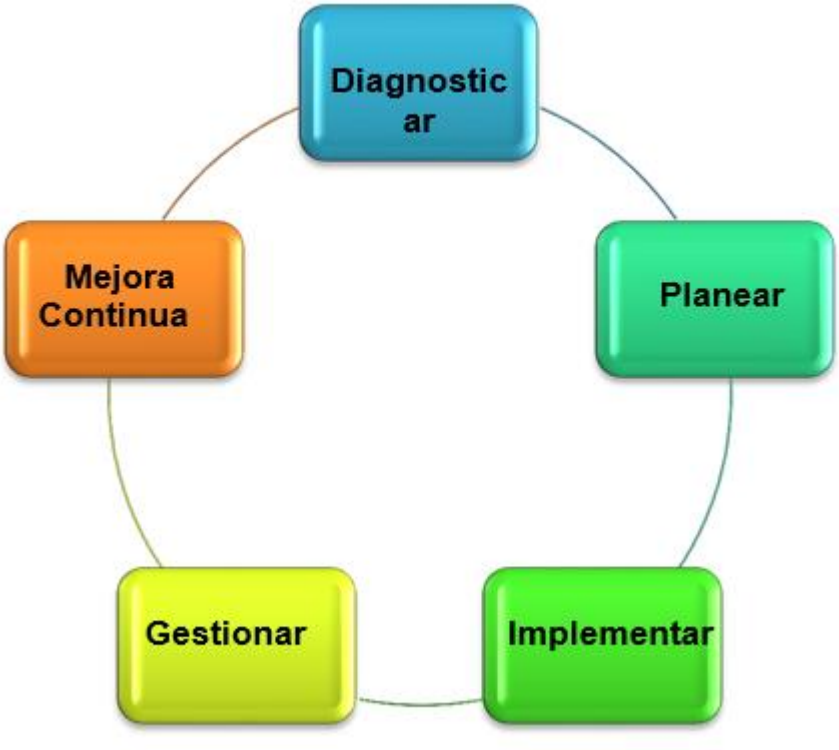

Figura 2. Fuente: Modelo de Seguridad y Privacidad de la Información emitida por MinTIC

9. ACTIVIDADES

ACTIVIDADES	TAREAS	RESPONSABLE	FECHAS PROGRAMACIÓN	
			Fecha Inicio	Fecha Final
Aprobación del Plan de Tratamiento de Riesgo Seguridad y privacidad de la información.	Aprobar Plan	Comité Institucional	2 Enero de 2024	31 de Enero del 2024
Socialización del Plan de Tratamiento de Ries de Seguridad y Privacidad de la Información.	Enviar por medio de correo electrónico a todo el personal el plan aprobado	Secretaria General	1 de marzo de 2024	30 de Abril del 2024
Reevaluar los Riesgos identificados con los líderes del Proceso.	Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Comité Institucional	1 de mayo del 2024	31 de Julio del 2024
Aceptación de Riesgos identificados	Aceptación, aprobación riesgos identificados	Comité Institucional	1 de Agosto del 2024	31 Agosto de 2024
Actualización y Socialización de los Riesgos		Equipo de Gestión del riesgo	1 Septiembre del 2024	31 Octubre del 2024
Seguimiento y Control	Seguimiento y Controles	Área Sistemas	1 de Enero del 2024	

10. ENTREGABLES

- Acta de Reunión.
- Plan de tratamiento de riesgo aprobado por los líderes
- Productos de cada etapa

BIBLIOGRAFÍA

Mintic - http://www.mintic.gov.co/
http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf
Mintic - http://www.mintic.gov.co/
http://www.mintic.gov.co/gestionti/615/w3- propertyvalue-7275.html

RIESGOS DE EJECUCIÓN PLAN

La ejecución del Plan de Tratamiento de Riesgos de Seguridad y privacidad estará sujeto a modificaciones teniendo en cuenta que la Entidad se someterá a un Rediseño Institucional derivado de un déficit presupuestal causado desde la vigencia 2021.

EL PRESENTE PLAN ES SOCIALIZADO Y APROBADO EN COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO, MEDIANTE ACTA No. 001 DEL 30 DE ENERO DE 2024.