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

2024

Concejo de Chía

@concejomunicipaldechía @concejochía @concejochía Concejo Municipal de Chía

concejomunicipalchia.gov.co

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

CONCEJO MUNICIPAL DE CHÍA
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

NATALIA GIL LOAIZA
PRESIDENTA CONCEJO MUNICIPAL CHÍA
2024

INTRODUCCIÓN

En Colombia se viene adelantando la implementación de la política de gobierno digital, tal como lo establece el decreto 1008 de 2018, cuyas disposiciones se compilan en el Decreto Único Reglamentario del Sector TIC, 1078 de 2015, específicamente en el capítulo 1, titulo 9, parte 2, libro 2, como un instrumento fundamental para mejorar la gestión pública y la relación del estado con los ciudadanos, la cual se ha articulado con el Modelo Integrado de Planeación y Gestión, como una herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo, articulada a otras políticas esenciales para la gestión pública en Colombia.

El Manual de la política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones establece que la política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital. Según el manual, la implementación de la política de gobierno digital se ha definido en dos componentes: TIC para el estado y TIC para la sociedad, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales. Estos cinco elementos, se desarrollan a través de lineamientos y estándares, que son requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros de la política.

El manual en mención, precisa que el habilitador de seguridad de la información busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, tramites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la información (MSPI). No obstante, el manual está amparado en el Decreto 1008 del 2018, que en su artículo 2.2.9.1.1.3 define que la política de Gobierno Digital se desarrollará conforme a los principios que rigen la función y los procedimientos administrativos adoptados en Colombia, en particular al principio de Seguridad de la Información, que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del estado, y de los servicios que prestan a la ciudadanía.

El documento denominado Modelo de Seguridad y Privacidad de la Información (MSPI), expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, expresa que la adopción del mismo, por las entidades del estado, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos. La adopción, implementación y evaluación del modelo mencionado, es una actividad obligatoria según lo expresado en el artículo 2.2.9.1.3.2., en el numeral 2, en los literales A, B y C, el cual debe ser planificado en atención a lo establecido en el decreto 612 de 2018, que en el artículo 1, señala la importancia de la integración de los planes institucionales y estratégicos al Plan de Acción institucional, en el ámbito de aplicación del modelo integrado de planeación y gestión.

Así mismo, la resolución 0500 de Marzo 10 del 2021 expedida por el Ministerio de Tecnologías de Información y de las Comunicaciones, que tiene como objeto

establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información, la guía de gestión de riesgos de Seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y establecer los lineamientos y estándares para la estrategia de seguridad digital. La resolución en mención precisa la necesidad de que los sujetos obligados deban adoptar las medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al Plan de Seguridad y Privacidad de la Información y así mitigar los riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Es precisamente a través del artículo 5 de la resolución 0500 que se precisa la necesidad de adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital, e incluirla en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos del artículo 2.22.22.3.14 del capítulo 3 del título 22 de la parte 2 del libro 2 del decreto 1083 de 2015. En atención a lo anterior, se presenta el plan de seguridad y privacidad de la información enfocado en la seguridad informática frente a ciber amenazas de activos de tecnologías de información de la entidad.

La adopción e implementación del Modelo de Seguridad y Privacidad de la información en las entidades públicas toma como sustento el estándar NTC ISO 27001:2013, así como principios regulatorios definidos por el Gobierno Nacional, tal como la Ley 1712 de 2014 o la Ley 1581 de 2012; así mismo, apoyan su enfoque en la implementación de un ciclo de identificación, valoración y tratamiento de riesgos de seguridad y privacidad de la información, para lo cual se ha expedido desde el Departamento Administrativo de la Función Pública la guía para la administración del riesgo y el diseño de controles en entidades públicas, como referente para abordar los riesgos de gestión, corrupción y de seguridad de la información. La adopción de prácticas de gestión de riesgos en las entidades públicas permitirá fortalecer la toma de decisiones en cuanto a la implementación de controles de acuerdo con el plan de tratamientos definido. Estos referentes constituyen el fundamento para la definición del plan de tratamiento de riesgos de seguridad y privacidad de la información con enfoque en la seguridad informática frente a ciber amenazas sobre activos de tecnologías de información y de las comunicaciones en el Concejo Municipal de Chía.

No obstante, durante la actual vigencia se desarrollará una modificación al actual Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Concejo Municipal de Chía, con el fin de generar los lineamientos presentados en la guía de seguridad y privacidad de Información del Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC para establecer los principios e implementar un sistema de gestión de riesgos, cuyo objetivo es minimizar, realizar una gestión y controlar cualquier tipo de riesgo, teniendo en cuenta el origen, la causa y su grado de incidencia, buscando proteger los datos de los ciudadanos y garantizando la seguridad de la información.

1. OBJETIVO

Establecer un marco de acción para aportar al tratamiento de riesgos de seguridad y privacidad de la información del Concejo Municipal de Chía, sobre los activos de tecnologías de información que soportan la prestación de servicios digitales de la Entidad, desde el enfoque de la seguridad informática frente a ciber amenazas, mediante el cual se definen acciones para aportar al tratamiento de riesgos de seguridad y

privacidad, en atención al contexto organizacional de la entidad, las capacidades y recursos disponibles, para fortalecer la confianza de los ciudadanos, usuarios, socios y demás partes interesadas.

2. OBJETIVOS ESPECIFICOS

- Establecer los controles que permitan proteger los activos de Información del Concejo Municipal de Chía, con base a los criterios de confidencialidad, integridad y disponibilidad.
- Determinar el alcance del Plan de Gestión de Riesgos de la Seguridad y Privacidad de la información en la corporación.
- Definir a través de una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.
- Proponer acciones para minimizar los riesgos a los que está expuesta la información.

3. ALCANCE

El plan de tratamiento de riesgo está orientado para la ser aplicada a toda la entidad, sus servidores públicos, terceros y partes interesadas de la entidad que en el ejercicio de sus funciones utilicen información y servicios de tecnología de la información del Concejo Municipal de Chía.

4. MARCO NORMATIVO

- Constitución Política de Colombia. 1991. Artículo 15.
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23/ 1982 y se modifica la Ley
  29/1944.
- Ley 527 de 1999. Define y reglamenta el acceso y uso de mensajes de datos, de comercio electrónico y de firmas digitales y se establecen las entidades de certificación.
- Ley 594 de 2000. Expide la Ley General de Archivos.
- Ley 1266 de 2008. Disposiciones generales del Hábeas Data y regula el manejo de la
  información contenida en bases de datos personales y la proveniente de terceros países.
- Ley 1221 de 2008. Normas para promover y regular el Teletrabajo.
- Ley 1273 de 2009. Modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos.
- Ley 1341 de 2009. Define principios y conceptos sobre la sociedad de la información y la organización TICS.
- Ley 1474 de 2011. Orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción.
- Ley 1581 de 2012. Disposiciones para la protección de datos personales.
- Ley 1712 de 2014. Ley de Transparencia y del Derecho de Acceso a la Información
  Pública Nacional.
- Ley 1915 de 2018. Modifica la Ley 23 de 1982.

- Ley 1978 de 2019. Se moderniza el sector de las TIC.
- Decreto 2609 de 2012. Reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011.
- Decreto 0884 del 2012. Reglamenta parcialmente la Ley 1221 de 2008.
- Decreto 1377 de 2013. Reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Reglamenta el Registro Nacional de Bases de Datos.
- Decreto 103 de 2015. Reglamenta parcialmente la Ley 1712 de 2014.
- Decreto 1078 de 2015. Expide el Decreto Único Reglamentario del Sector de las TIC.
- Decreto 728 de 2017. Adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
- Decreto 1499 de 2017. Modifica Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 1008 de 2018. Establece lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de las TIC.
- Decreto 2106 de 2019. Se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- Decreto 620 de 2020. Subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad Digital.
- CONPES 3905 de 2020. Política Nacional de Confianza y Seguridad Digital.
- Resolución N°.107 de 30 de diciembre de 2020 *"por medio de la cual se adopta la política de privacidad y seguridad informática del concejo municipal de Chía".*
- Resolución N°.108 de 2020 *"por medio de la cual se adopta la política de tratamiento de datos personales de la corporación del concejo municipal de Chía".*

5. GLOSARIO

Activo: Es un recurso que tiene un valor específico para la entidad y debe ser protegido.

Activos de Información: Son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección.

Análisis de riesgo: Uso metódico de la información para identificar fuentes y para evaluar el riesgo.

Acciones asociadas: Son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo.

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.

Causa: Medios, circunstancias y/o agentes que generan riesgos.

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.

Evento de seguridad: Situación previamente desconocida que puede ser relevante para la seguridad.

Información: La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada

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.

Riesgo: Eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

Valoración del riesgo: Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

6. ROLES Y RESPONSABLES

Es primordial tener claridad sobre los objetivos institucionales y estratégicos de la entidad, tener una visión sistémica de la gestión, de manera que se analicen las oportunidades o amenazas relevantes, que puedan generar riesgos y afecten el cumplimiento de los objetivos misionales de la entidad, formulados en el Plan Estratégico PEI 2020-2024.

Proceso Gestión de Tecnologías de la Información: La construcción del Plan de Tratamiento de Riesgos es Liderado por el Proceso Gestión de Tecnologías de la Información. La administración de los riesgos de seguridad y privacidad depende de la participación de todo el equipo de funcionarios y contratistas del Concejo Municipal de Chía.

Líderes de los Procesos: Se encargan de identificar los riesgos y establecer acciones para mitigarlos, analizando las causas, proponiendo acciones y presentando evidencias para el plan de mejoramiento de los procesos.

Comité Institucional de Gestión y Desempeño: realiza seguimiento a la gestión de los riesgos de seguridad digital de la corporación y toma acciones.

7. POLITICAS DE LA GESTIÓN DEL RIESGO

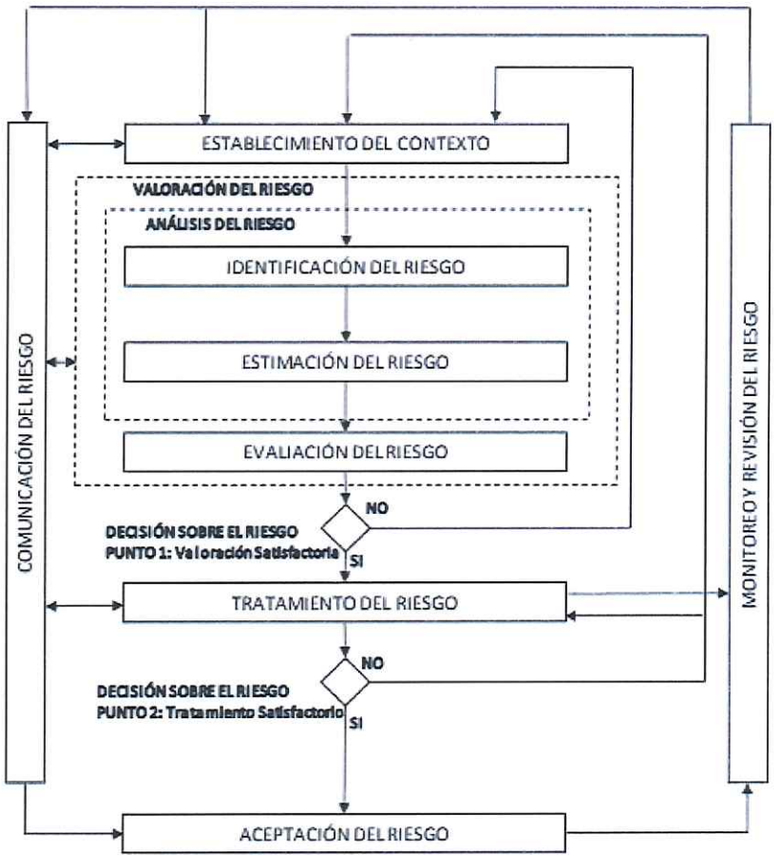
Frente a la gestión del riesgo de seguridad digital se tiene prevista las siguientes políticas:

- Implementar la Política de Seguridad y Privacidad de la información.
- Identificar aspectos organizativos de la seguridad de la información en los procesos.
- Seguridad de la Información enfocada a los recursos humanos.
- Revisión de los Controles de acceso.
- Eventos de riesgo en los procesos.
- Gestión de incidentes de Seguridad de la Información.

Para minimizar los riesgos, es importante que sean asignados recursos humanos, tecnológicos, operativos y de presupuesto, que permitan de una manera continua desarrollar esquemas de trabajo y actividades para mejorar las políticas de seguridad y privacidad existentes.

8. PROCESO PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Figura 1
Proceso para la administración del riesgo en seguridad de la información

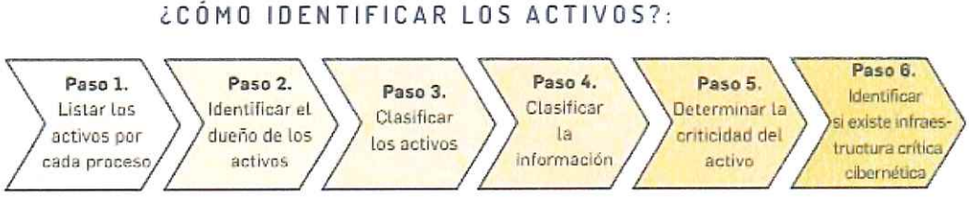


Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

El anterior proceso, se deberá desarrollar teniendo en cuenta los siguientes aspectos:

8.1. IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

Figura 2
Proceso de identificación de activos de seguridad de la información



Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC. 2018.

Para la evaluación de riesgos de seguridad y privacidad de la información se tomará como insumo la matriz de Activos de Información, sobre la cual se implementará el presente Plan sobre los Activos de Información que tengan un nivel alto de clasificación al evaluar los criterios de confidencialidad, integridad y disponibilidad, según los siguientes criterios:

Figura 3
Criterios de Clasificación

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Figura 4
Niveles de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

8.2. IDENTIFICACIÓN DEL RIESGO

Los riesgos identificados a partir del Contexto Institucional, se podrán identificar a partir de los siguientes tres (3) tipos de riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

8.3. CONTROLES ASOCIADOS A LA SEGURIDAD DE LA INFORMACIÓN

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", siempre y cuando se ajusten al análisis de riesgos.

8.4. ELABORAR PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Se realizará la revisión de los actuales procedimientos, con el objeto de identificar las necesidades de documentación y/o actualización de procedimientos en el marco de la implementación del Modelo de Seguridad y Privacidad de la información. El propósito de esta actividad se fundamenta en desarrollar y formalizar procedimientos que permitan gestionar la seguridad y privacidad de la información en todos los procesos de la Entidad.

8.5. ANÁLISIS DE RIESGOS

El análisis del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo. Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados, probabilidad e impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado, o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por Impacto se entiende las consecuencias que puede ocasionar a la Entidad la materialización del riesgo.

8.6. VALORACIÓN DE RIESGOS

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo. Lo anterior de acuerdo con los formatos Identificación y evaluación de controles y Valoración del riesgo.

8.7. EVALUACIÓN DE CONTROLES

Evaluación de Controles Permite determinar en qué medida los controles identificados están aportando para disminuir los niveles de probabilidad e impacto del riesgo. Se evalúan verificando su documentación, aplicación y efectividad

8.8. SOCIALIZACIÓN Y COMUNICACIÓN POLÍTICAS DE RIESGOS

Actividad mediante la cual se da conocer a los funcionarios, contratistas y terceros de la Corporación las políticas de tratamiento de riesgos de Seguridad y Privacidad de la Información, mediante charlas y el uso de las herramientas de comunicaciones disponibles en la Corporación.

8.9. MONITOREO Y REVISIÓN AL TRATAMIENTO DE LOS RIEGOS

El monitoreo y revisión debe asegurar que las acciones establecidas en los mapas de riesgo se están llevando a cabo y evaluar la eficacia en su implementación, adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden influir en la aplicación de acciones preventivas.

9.

PLAN DE TRATAMIENTO DE RIESGOS Y SEGURIDAD DE LA INFORMACIÓN

Gestión de Riesgos				
Actividad	**Tarea**	**Responsable**	**Fecha**	**Fecha Final**
Identificación de los activos de información				
Sensibilización institucional sobre Política de Seguridad de la Información	Realizar la divulgación de las reglas de comportamiento adecuadas para el uso de los sistemas y la información de la entidad.	Proceso Gestión de Tecnologías de la Información	Enero 2024	31/12/2024
Inventario de Activos	Analizar los activos Vinculados a la información.	Proceso Gestión de Tecnologías	Enero 2024	31/12/2024
Definir metodología para la gestión de los riesgos de seguridad y privacidad de la información	Definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos de información.	Proceso Gestión de Tecnologías de la Información	Enero 2024	31/12/2024
Calificación de la criticidad de los activos				
Identificación de riesgos de seguridad y privacidad de la información.	Evaluación de los activos y amenazas.	Proceso Gestión de Tecnologías de la Información	Enero 2024	31/12/2024

Gestión de Riesgos				
Actividad	**Tarea**	**Responsable**	**Fecha**	**Fecha Final**

Análisis de Riesgos	Establecer la probabilidad de ocurrencia de los riesgos y sus consecuencias, calificándolos y evaluándolos, con el fin de obtener información para establecer el nivel de riesgo.	Todos los procesos	Enero 2024	31/12/2024
Valoración del riesgo.	Comparar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos.	Direccionamiento Estratégico	Enero 2024	31/12/2024
Evaluación de Controles	Determinar en qué medida los controles identificados están aportando para disminuir los niveles de probabilidad e	Oficina de Control Interno en conjunto con los procesos.	Enero 2024	31/12/2024
Socialización y Comunicación Políticas de Riesgos	Dar conocer a funcionarios contratistas y terceros de la Entidad las políticas de tratamiento de riesgos de Seguridad y Privacidad de la Información, mediante el uso de las herramientas de comunicaciones disponibles en la Entidad.	Proceso Gestión de Tecnologías de la Información	Enero 2024	31/12/2024

Gestión de Riesgos				
Actividad	**Tarea**	**Responsable**	**Fecha**	**Fecha Final**

Monitoreo y revisión al tratamiento de riesgos	El monitoreo y revisión debe asegurar que las acciones establecidas en los mapas de riesgo se lleven a cabo, así como evaluar la eficacia en la implementación.	Control Interno	Enero 2024	31/12/2024

NATALIA GIL LOAIZA
Presidenta Concejo Municipal de Chía
2024