Código:	D-GR-05
Versión:	02

Plan de seguridad y Privacidad de la información

Direccion de las Tic

Julian Mauricio Montoya Cuartas

DIRECTOR ADMINISTRATIVO DE LAS TIC Y SOPORTE TECNOLÓGICO

ALCALDIA DE BELLO

BELLO - ANTIOQUIA

2021

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

El presente Plan de Seguridad y Privacidad de La Información, da cuenta de una serie de tareas que el Alcaldía Municipal de Bello realizará a fin de implementar la estrategia de gobierno digital alrededor del componente de seguridad y privacidad de la información, cuyo principal objetivo es proteger los derechos de los usuarios de la entidad y mejorar los niveles de confianza en los mismos a través de la identificación, valoración, tratamiento y mitigación de los riesgos de los sistemas de información.

En la situación actual que viven los sistemas de información es obligatorio implementar unas estrategias a nivel interno que pueda salvaguardar la información sensible de la entidad para que se pueda cumplir todo lo misional y que los procesos funcionen con normalidad.

Es de vital importancia para cada entidad acogerse a la política de gobierno digital, teniendo en cuenta que tiene todos los lineamientos y estandarizaciones para que cada entidad pueda cumplir y tener una hoja de ruta clara en estos aspectos.

La política de Gobierno Digital expedida 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 innovadores, que generen valor público en un entorno de confianza digital.

Teniendo en cuenta lo anterior, 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 documento denominado Modelo de Seguridad y Privacidad de la Información, MSPI, expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, nos indica que la adopción del mismo, por las entidades del estado, conduce a la preservación de la confidencialidad, integridad y 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.

OBJETIVO

Identificar, valorar, tratar y mitigar los riesgos de los sistemas de información con el fin de proteger los activos de información, el manejo de medios, el control de acceso y la gestión de los usuarios.

2.1 OBJETIVOS ESPECIFICOS

- Implementar la protección de los activos de información de la Alcaldía de Bello, con base en los criterios de confidencialidad, integridad y disponibilidad.
- Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.
- Sensibilizar a los servidores públicos y contratistas de la entidad acerca de la política de seguridad de la información y el modelo de seguridad y Privacidad de la Información, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información críticos de la Entidad.

1. ALCANCE

La adopción del Modelo de Seguridad y Privacidad de la Información, para la vigencia 2021, se enfocará en fortalecer la implementación de acciones de acuerdo a los lineamientos divulgados por el Ministerio de Tecnologías de la información y las Comunicaciones, dirigidos a la seguridad informática de las plataformas tecnológicas de la Alcaldía de Bello, teniendo en cuenta el capital humano (profesionales, técnicos, auxiliares), los recursos financieros y la capacidad disponible para mejorar la confianza de los ciudadanos, usuarios, socios y demás partes interesadas.

TERMINOS Y DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elementos relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización.

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.

Acuerdo de Nivel de Servicio: Un Acuerdo de Nivel de Servicio (ANS) es un convenio entre un proveedor de servicios de TI y un cliente. Describe las características del servicio de TI, los niveles de cumplimiento y las sanciones, y especifica las responsabilidades del proveedor y del cliente. Un ANS puede cubrir múltiples servicios de TI o múltiples clientes.

Aplicaciones o aplicativos: Las aplicaciones son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores tabletas o celulares3.

Autenticación: Proceso utilizado entre un emisor y un receptor, con el fin de asegurar la integridad de los datos y proporcionar la autenticidad de los datos originales4

Backup: Operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático. Es una copia de seguridad.

Clave de autenticación o Contraseñas: Clave criptográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos.

Copyright: Derecho exclusivo de un autor o editor a explotar una obra física o digital, literaria, científica o artística.

Dominio: Es un conjunto de computadores, conectados en una red, que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que

cada uno de los usuarios tiene en la red. Es la parte principal de una dirección en la Web, que usualmente indica la organización o compañía que administra dicha página

Internet: Herramienta de comunicación con decenas de miles de redes de computadoras unidas por el protocolo TCP/IP.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos. [NTC 5411-1:2006]

Intranet: Es una red de ordenadores privados que utiliza tecnología Internet para compartir, dentro de una organización, parte de sus sistemas de información y sistemas operacionales.

Dirección IP: La dirección IP (IP es un acrónimo para Internet Protocol) es un número único e irrepetible con el cual se identifica una computadora conectada a una red que corre el protocolo IP.

Información personal: Es aquella suministrada por el usuario o el visitante para el registro o consulta de información, la cual incluye datos como nombre, identificación, edad, género, dirección, correo electrónico y teléfono, entre otros6.

Log: Uno o más ficheros de texto automáticamente creados y administrados por un servidor, en donde se almacena toda la actividad que se hace sobre éste7.

Cloud Computing: Es un nuevo concepto tecnológico que se basa en que las aplicaciones software y los equipos hardware con capacidad de proceso y almacenaje de datos que están ubicados en un Datacenter que permite a los usuarios acceder a las aplicaciones y servicios disponibles a través de Internet o como se conoce coloquialmente a través “la Nube” de Internet, de una forma sencilla y cómoda.

Clúster: Conjunto de servidores que trabajan como una única maquina mejorando el desempeño de las transacciones y operaciones implantadas en este sistema.

CPD: Centros de Procesamiento de Datos, ubicación física donde se concentran todos los equipos electrónicos necesarios para el procesamiento de la información de una organización.

CRM: “Customer Retationship Management”. Gestión de la Relación con el Cliente, son herramientas informáticas dedicadas a la gestión integrada de información sobre

clientes. Estas aplicaciones permiten, desde almacenar y organizar esta información, hasta integrar, procesar y analizar la misma.

- **Medios de almacenamiento físico:** Se considera como medio de almacenamiento físico las cintas, los discos extraíbles, los DCs y los DVDs entre otros.

- **Nombres de Grupos:** Seudónimos utilizados para la clasificación de conjuntos de computadoras dentro del dominio.
- **Portal web**: Es un sitio compuesto por varias páginas web, el cual, permite al usuario el fácil acceso a diferentes recursos y servicios que tienen relación con un mismo tema. El portal web de la Alcaldia Municipal de bello, se encuentraen la dirección: URL: https://www.bello.gov.co/
- **Publicar:** Es la acción de hacer visible un contenido o documento desde un portal o sitio web.
- **Servidor:** Computadora central en un sistema de red que provee servicios a otras computadoras.
- **Sistema Informático o de Información:** Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna forma mensajes de datos.
- **Usuario:** Es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático. Por lo general es una única persona. Se autentica e ingresa a los sistemas y sus servicios mediante un nombre de usuario (cuenta) y una contraseña de autenticación.
- **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).
- **Confidencialidad:** Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado
- **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)

2. MARCO NORMATIVO

Marco normativo	Año	Descripción
Políticas técnicas de seguridad de la información Función Pública	2020	La declaración de la Política de Seguridad de la Información institucional busca proteger los activos de información (grupos de valor, información, procesos, tecnologías de información incluido el hardware y el software), mediante el establecimiento de lineamientos generales para la aplicación de la seguridad de la información en la gestión de los procesos internos, bajo el marco del Modelo Integrado de Planeación y Gestión, consolidada en los procedimientos, guías, instructivos y publicaciones, así como la asignación de roles y responsabilidades
Decreto 103 de 2015	2019	Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.
Decreto 1494 de 2015	2019	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1008	2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
Ley 1712 de 2014;	2018	Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
Decreto 2573 de 2014	2018	Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones
Decreto 1377 de 2013	2018	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 2609 de 2012.	2017	Por el cual se reglamenta parcialmente la Ley 1581de 2012.
Ley estatutaria 1581 de 2012,	2017	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones

Ley 1474 de 2011	2017	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
Decreto 4632 de 2011	2017	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
Ley 1273 de 2009,	2016	Se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.
Ley 527 de 1999	2015	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Constitución Política de Colombia1991 - Artículo 15	2015	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.
Ley 23 de 1982	2015	Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.
Norma técnica colombiana NTC - ISO/IEC 27001	2013	3 Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa
Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.

Tabla 1. Marco Normativo

METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Plan de Seguridad y Privacidad de la Información en la Alcaldía Municipal de Bello, toma referencia Modelo de Seguridad y Privacidad de la Información en su versión 3.0.2 publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones.

En este punto es pertinente presentar el ciclo de funcionamiento del modelo de operación, a través de la descripción detallada de cada una de las cinco (5) fases que lo comprenden. Estas, contienen objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de la Alcaldía Municipal de Bello.

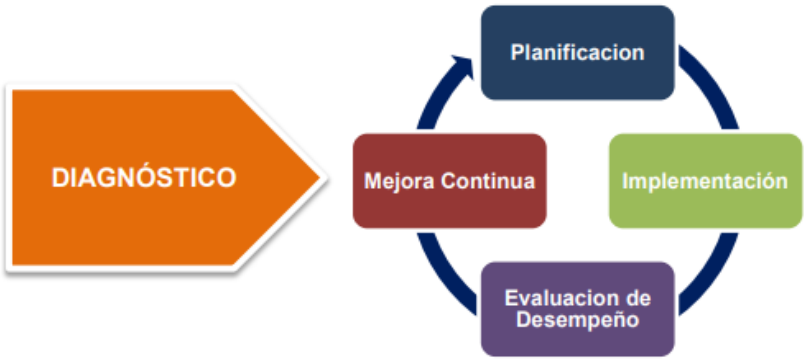

Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

FASE DE DIAGNÓSTICO - ETAPAS PREVIAS A LA IMPLEMENTACIÓN

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior la Alcaldía Municipal de Bello.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad.

Para realizar dicha fase la Alcaldía Municipal de Bello debe efectuar la recolección de la información con la ayuda de la herramienta de diagnóstico y la metodología de pruebas de efectividad. Una vez se tenga el resultado del diagnósticoinicial y se haya determinado el nivel de madurez de la entidad se procede al desarrollo de la fase de Planificación. Los resultados asociados a la fase de Diagnostico previas a la implementación deben ser revisados y socializados por las partes interesadas.

Figura 2 – Etapas previas a la implementación

FASE DE PLANIFICACIÓN

Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

El alcance del MSPI permite a la Corporación definir los límites sobre los cuales se implementará la seguridad y privacidad. Este enfoque es por procesos y debe extenderse a todo la Alcaldía Municipal de Bello.

Para desarrollar el alcance y los límites del Modelo se deben tener en cuenta las siguientes recomendaciones: Procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos.

Figura 3 - Fase de planificación[1]

FASE DE IMPLEMENTACIÓN

Esta fase le permitirá al Municipio de Bello, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI.

Figura 4 - Fase de implementación[2]

FASE DE EVALUACIÓN DE DESEMPEÑO

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

Figura 5 - Fase de Evaluación de desempeño[3]

FASE DE MEJORA CONTINUA

En esta fase la Alcaldía Municipal de Bello debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

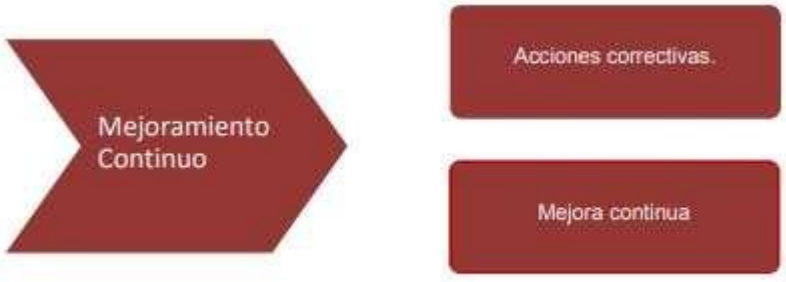

Figura 6 - Fase de mejoramiento continúo[4]

En esta fase es importante que la Entidad defina y ejecute el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño.

Utilizando los insumos anteriores, la Entidad puede efectuar los ajustes a los entregables, controles y procedimientos dentro del MSPI. Estos insumos tendrán como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por la Alta Dirección de la entidad. La revisión por la Alta Dirección hace referencia a las decisiones, cambios, prioridades etc. tomadas ensus comités y que impacten el MSPI.

INFORMACIÓN PERSONAL RECOLECTADA

La Información Personal que la Alcaldía Municipal de Bello. Puede recolectar y someter a tratamiento es la siguiente:

- Nombre completo del titular de la información;
- Identificación:
- Fecha de nacimiento;
- Domicilio;
- Dirección para notificación;
- Teléfonos de contacto;
- Correo electrónico;
- Identidad de género

- **TRATAMIENTO DE DATOS PERSONALES DE MENORES DE EDAD**

- En aplicación de lo establecido en la ley, la Alcaldía Municipal de Bello procederá a efectuar el Tratamiento de la Información personal; de niños, niñas y adolescentes, respetando el interés superior de los mismos y asegurando, en todos los casos, el respeto de sus derechos fundamentales y garantías mínimas.

- En todos los eventos en los que se requiera darle tratamiento a la información personal de menores de edad, la Alcaldía Municipal de Bello obtendrá la autorización de sus representantes legales, que para este efecto son el padre y/o madre o tutor.

MANEJO DE LA INFORMACIÓN

CLASIFICACIÓN DE LA INFORMACIÓN

La información resultante de los procesos misionales y de apoyo de la entidad se tratará conforme a los lineamientos y parámetros establecidos en el Manual de Gestión Documental de la entidad.

Los activos informáticos asociados a cada sistema de información, serán identificadosy clasificados por su tipo y uso siguiendo lo establecido en las tablas de retención documental vigentes, de acuerdo con los siguientes criterios:

a) Pública: Datos misionales y críticos.
b) Interna: Aplicativos, archivos de software, archivos de usuarios, herramientas yprogramas de desarrollo. Manuales, procedimientos internos, guías y formatos.
c) Confidencial: Bases de Datos, Documentación, procedimientos operativos, configuraciones.

ACTIVIDADES PARA LA IMPLEMENTACIÓN.

- Realizar diagnóstico.
- Comparar el objetivo con lo identificado
- Realizar inventario de activos de información (Software, bases de datos) conlos líderes de cada proceso
- Realizar la valoración de los activos de información con los líderes de cadaproceso y emitir el plan
- Socializar el plan
- Ejecución del plan
- Realizar seguimiento del plan

PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Alcaldía de Bello ha adoptado la Política de Seguridad del Gobierno Nacional y como entidad territorial como parte integral de su funcionamiento y gestión. Para lograr su implementación y fortalecimiento, ha diseñado varios planes orientados a avanzar en diferentes actividades, para dar cumplimiento a las orientaciones del Ministerio de Tecnologías de Información y de las Comunicaciones, en cuanto a la adopción e implementación del modelo de seguridad y privacidad de la información.

Para viabilizar una propuesta, se ha organizado un plan estratégico de implementación que define el conjunto de planes y actividades que se deben realizar para fortalecer las acciones encaminadas a la implementación de la Política de seguridad de la información, como eje fundamental, para dar cumplimiento a lo propuesto en la Política de Gobierno Digital.

Así mismo, en atención, tanto a lo especificado en el modelo de seguridad y privacidad, como lo planteado en el estándar NTC ISO 27001:2013, se aborda la identificación, valoración, tratamiento y gestión de riesgos de seguridad digital, como parte fundamental del modelo y en cumplimiento en lo dispuesto en la Política de Seguridad Digital. A continuación, se presenta el Plan estratégico para la fortalecer la implementación del modelo de seguridad y privacidad de la Alcaldía de Bello, enfocado desde la Seguridad Informática, detallando el nombre del plan y responsables.

PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ITEM	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FECHA
1	Actualización del Diagnóstico del Modelo de Seguridad y Privacidad de la Información.	Dirección de las TIC y Soporte Tecnológico Municipio de Bello	01/01/2021 20/03/2021
2	Identificación, clasificación, valoración y asignación de responsables de Activos de Información (Software, Hardware, Redes, Servicios de Tecnologías de Información y de las Comunicaciones, Soportes, Servicios de Tecnologías de Información.	Líder seguridad Dirección de las TIC Municipio de Bello	21/03/2021 31/07/2021
3	Identificación, valoración y tratamiento de riesgos de Seguridad Digital desde la Seguridad Informática.	Líder seguridad Dirección de las TIC Municipio de Bello	01/07/2021 28/11/2021
4	Gestión de Incidentes de Seguridad Informática.	Líder seguridad Dirección de las TIC Municipio de Bello	01/01/2021 31/12/2021
5	Implementación de la Seguridad Informática.	Líder seguridad Dirección de las TIC Municipio de Bello	01/01/2021 31/12/2021
6	Implementación de Controles de Seguridad Informática.	Líder seguridad Dirección de las TIC Municipio de Bello	20/02/2021 31/12/2021
7	Acciones para apoyar la transición de IPv4 a IPv6 de la plataforma tecnológica de la entidad.	Dirección de las TIC y Soporte Tecnológico Municipio de Bello	20/10/2021 31/12/2021

NOTAS DE CAMBIO

BREVE DESCRIPCIÓN DEL CAMBIO	VERSIÓN	FECHA aaaa-mm-dd
No aplica para la primera versión.	01	2021-01-15
Se incluye el cronograma del plan y el marco normativo	02	2022-03-16

Elaboró:	Julián Montoya – Director TIC Jaime Atehortua Marin – Contratista Dirección TIC	Fecha:	2021-01-15
Revisó:	Julián Montoya Cuartas – Director TIC	Fecha:	2022-03-16
Aprobó:	Julián Montoya Cuartas – Director TIC	Fecha:	2022-03-16