PLAN PARA LA IMPLEMENTACION DE LA ESTRATEGIA DE GOBIERNO DIGITAL SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

MUNICIPIO DE BUCARAMANGA

TABLA DE CONTENIDO

INTRODUCCIÓN

Teniendo en cuenta los lineamientos impartidos a nivel de seguridad y privacidad de la información establecidos por el gobierno nacional en cabeza del Ministerio de tecnologías de información y las comunicaciones – MINTIC para las entidades públicas, se generó y actualizo el presente documento, el cual se ha establecido como la guía a seguir para apoyar el cumplimiento de la estrategia de gobierno digital en cuanto a la implementación de un sistema de Gestión de seguridad y privacidad de la información (SGSI) basado en las normas internacionales ISO 27000:2013 , el cual debe estar articulado con la normatividad colombiana para la reglamentación de la protección de datos personales (privacidad), ley 1581 de 2012 y decreto 1377 de 2013.

El presente documento debe ser revisado y actualizado de manera periódica y las actividades y entregables que están contemplados dentro del mismo, deben ser validados de igual forma y actualizados de acuerdo a nuevos lineamientos o cambios en las políticas publicas si es el caso.

1. MARCO DE LA SEGURIDAD DE LA INFORMACIÓN DEL MUNICIPIO DE BUCARAMANGA

El marco de la seguridad y privacidad de la información establece los lineamientos generales para implementar la estrategia de acuerdo con la necesidad del Municipio y su misión y visión además es el documento de partida que regula las políticas, alcances, objetivos y limitaciones de la implementación del SGSI.

Es importante mencionar que este marco esta apoyado por el documento de ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACION el cual enmarca y establece los lineamientos generales que apoyan este modelo. Está compuesto por los siguientes ítems:

1.1. DEFINICIÓN

En cumplimiento del decreto 1078 de 2015 para la implementación de la estrategia de gobierno en línea donde se estable la necesidad de gestionar los riesgos de la seguridad y privacidad de la información de las entidades territoriales como el MUNICIPIO DE BUCARAMANGA, es de vital importancia la toma de decisiones que establezcan mecanismos y acciones para asumir los retos de la estrategia. El marco de seguridad y privacidad de la información (MSPI) ha de ser la carta de navegación para alcanzar las metas de dicho componente a través de la implementación de un sistema de gestión de la seguridad de la información articulado con los diferentes procesos de la entidad y otros modelos de gestión institucional.

1.2. CONTEXTO

Colombia es uno de los 40 países con mayor número de ataques y amenazas cibernéticas[1]con alrededor de 10 millones de ciberataques diarios (cifra 2015), lo que evidencia la necesidad de la gestión de riesgos digitales para evitar la ciberdelincuencia y

[1] Tomado de: https://cybermap.kaspersky.com/

el cibercrimen donde pueden verse afectados las instituciones de carácter público como lo es el Municipio. Es de considerar también el crecimiento de la gobernanza del internet para la realización de trámites y servicios a través de este medio donde actualmente se supera en más de cien (100) funciones que pueden realizarse en línea[2] registrados ante la SI virtual Y el SUIT (Sistema único de información de trámites) , es de vital importancia reconocer las tendencias tecnológicas que aportan productividad a entidades como son la internet de las cosas (IoT, Internet of things), la gestión de dispositivos de usuarios (BYOD, Bring your own device) y el teletrabajo.

Las instituciones de carácter gubernamental según estadísticas del ColCERT son las segundas con mayores incidentes digitales con una representación del 23,9 % del número reportado a esta entidad[3]; la visión del MUNICIPIO DE BUCARAMANGA contempla en ser una entidad pública de servicio social encargada del desarrollo y el mejoramiento de la calidad de vida de sus habitantes. Cumple su propósito promoviendo la participación ciudadana, con gobernabilidad y alto sentido de pertenencia, fundamentado en su sistema de gestión de la calidad, sus valores y principios y en la transparencia de su gestión[4]. Por lo cual, con la implementación de los componentes de la estrategia de gobierno en línea, se hará un mayor uso de las tecnologías de la información para lograr las metas definidas en la misión y visión de la entidad a nivel estratégico en el MUNICIPIO DE BUCARAMANGA.

1.3. ALIADOS ESTRATÉGICOS

Los aliados estratégicos para el funcionamiento del marco se consideran como actores que en cualquier momento pueden intervenir para la gestión, colaboración, reporte e investigación de incidentes de carácter informático para la gestión de la seguridad de la información, entre ellos se encuentran:

[2] Tomado de: https://www.sivirtual.gov.co/
http://www.suit.gov.co/
[3] Tomado de: Documento CONPES 3854 de Seguridad Digital.
[4] Tomado de: http://www.bucaramanga.gov.co/Contenido.aspx?param=271

- **ColCERT**: Grupo de respuestas ante emergencias Cibernéticas de Colombia.
- **CCP**: Centro cibernético policial
- **Fiscalía general de la nación**: Órgano investigativo para delitos informáticos
- **SIC**: Superintendencia de industria y comercio, autoridad para la protección de datos personales.
- **MINTIC**: Ministerio de Tecnologías de la información y Comunicaciones líder la implementación de estrategia de Gobierno en línea.
- **Universidades y otras entidades del sector tecnológico**.

1.4. CONTEXTO NORMATIVO Y ESTANDARIZACIÓN

1.4.1. ESTÁNDARES INTERNACIONALES

- **ISO 27000:2013:** Estándar internacional para la implementación de los sistemas de gestión de la seguridad de la información.
- **ITIL v3**: Es una librería de buenas practica para la gestión de servicios de tecnología de la información (TI), una de las librerías es la gestión de la seguridad de la información; actualmente en su versión 3.

1.4.2. NORMATIVIDAD COLOMBIANA

- **Ley 1213 de 2009,** código penal colombiano
- **Ley 1341 de 2009,** Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- **Ley 1581 de 2012, Decreto 1377 de 2013;** normatividad para la gestión de datos personales.
- **Decreto 32 de 2013,** Por el cual se crea la Comisión Nacional Digital y de Información Estatal para la atención de incidentes de ciberdefensa y ciberseguridad.

- **Ley 1712 de 2014,** Ley de transparencia de la información pública.
- **Decreto 2573 de 2014,** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea.
- **Decreto 1078 de 2015,** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **CONPES 3854,** Documento para la seguridad digital.
- Otra normatividad vigente en derecho de autor propiedad intelectual y comercio electrónico.

1.5. POLÍTICAS

Con la necesidad de gestionar la seguridad y privacidad de la información se requiere crear, documentar y socializar las siguientes políticas:

- **Política de seguridad de la información:** Documento en el cual se establecen las indicaciones generales para el manejo de la seguridad de la información dentro de la administración central e institutos centralizados dependientes.
- **Política de privacidad y protección de datos personales:** Documento por el cual se da cumplimiento a la ley 1581 de 2012 y el decreto reglamentario 1377 de 2013 para el manejo de datos personales en la administración.

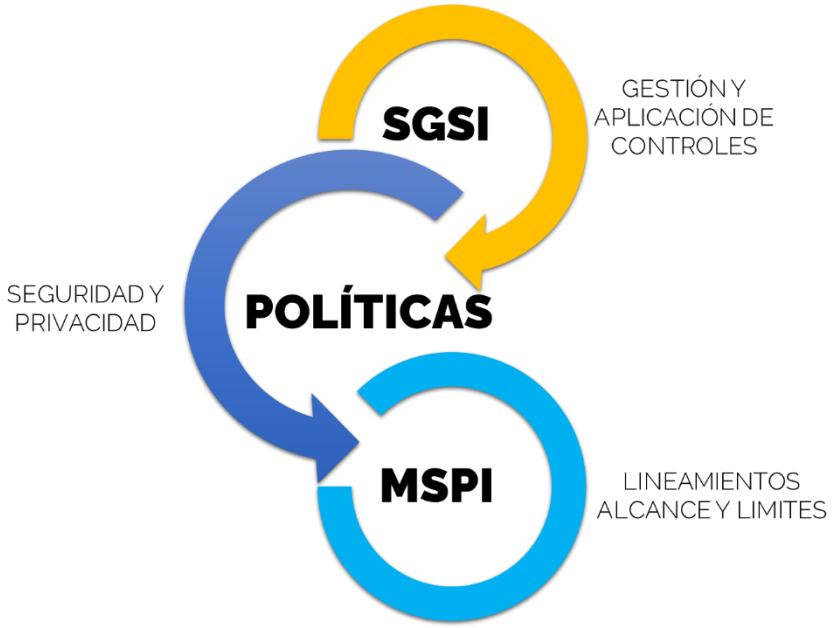


Figura 1. Articulación del MSPI y las políticas
Fuente: Oficina TIC

1.6. ARTICULACIÓN ESTRATÉGICA

La gestión de la seguridad de la información es importante asumirlo desde diferentes puntos de vista de la organización con el fin de lograr los alcances del sistema de gestión de seguridad de la información de manera que se articulen con las herramientas institucionales para el control de la entidad para lograr la integración de:

Figura 2. Sistema de gestión integrado
Fuente: Autor

1.7. CAPACITACIÓN, PROMOCIÓN Y SENSIBILIZACIÓN

Para articular las acciones y documentos alrededor del marco de seguridad y privacidad de la información es importante capacitar a los servidores públicos, funcionarios y contratistas sobre los riesgos de digitales y tendencias en el manejo de la información. Por lo cual las acciones tomadas para dicho fin serán:

- **Capacitación en seguridad de la información, políticas y documentación asociada al SGSI**: Según los requerimientos se pueden establecer al menos dos jornadas de capacitación sobre la seguridad de la información para contratistas y funcionarios del Municipio, incluyendo la actualización de políticas, procedimientos y acciones que ayuden a garantizar buenas prácticas a nivel de usuario sobre el SGSI.

- **Promoción de las herramientas de protección, tendencias y amenazas frecuentes** en la entidad mediante campañas de sensibilización con el uso de herramientas tecnológicas y otros medios (impresos, pantallazos, material audiovisual, etc.). Esta estrategia estará constantemente actualizando a los usuarios sobre riesgos digitales para identificarlos y mitigarlos para evitar incidentes como robo, secuestro o perdida de la información vital para el Municipio.

- **Portal web interno y externo de la entidad** sobre el manejo de la seguridad y privacidad de la información. ARCANA, con el cual se podrá mantener la documentación del SGSI de manera actualizada, el plan de sensibilización y capacitación, tendencias tecnológicas relacionadas con seguridad y la administración de incidentes y eventos dentro de la misma plataforma de manera que se puedan obtener estadísticas sobre la gestión del sistema.

Es importante mantener la articulación de la mesa de servicios HELPTIC para optimizar los recursos institucionales y humanos para la disponibilidad de los servicios de TI.

1.8. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Se define como el conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

1.9. OBJETIVO

Gestionar la toma de decisiones para la seguridad y privacidad de información articulando con los diferentes sistemas de gestión la implementación de políticas, controles y procedimientos, así como también la respuesta ante incidentes de seguridad.

1.10. ALCANCE

EL SGSI tendrá un alcance interno para las dependencias y usuarios en la administración central del Municipio de Bucaramanga.

1.11. LIMITES

El SGSI no hará control de incidentes a nivel de los ciudadanos o usuarios externos a la entidad, sin embargo, con los medios disponibles se sensibilizará sobre la existencia de la gestión de la seguridad dentro de la entidad a personal externo.

1.12. ORGANIZACIÓN DEL SGSI

El SGSI funcionara **liderado** por el asesor de despacho TIC o un delegado para dicha función, quien articulara con las dependencias de la entidad a través del comité de gobierno en línea las actividades relacionadas en esta gestión. Las funciones o roles importantes para el SGSI son:

- **Seguridad y controles:** Con el cual se establecerán los mecanismos o herramientas para el control de la seguridad de la información con base a la política de seguridad de la información.

- **Privacidad de datos:** La función es articular la gestión de la política de protección de datos personales mediante las herramientas, controles o procedimientos necesarios para el pleno cumplimiento de la legislación actual.

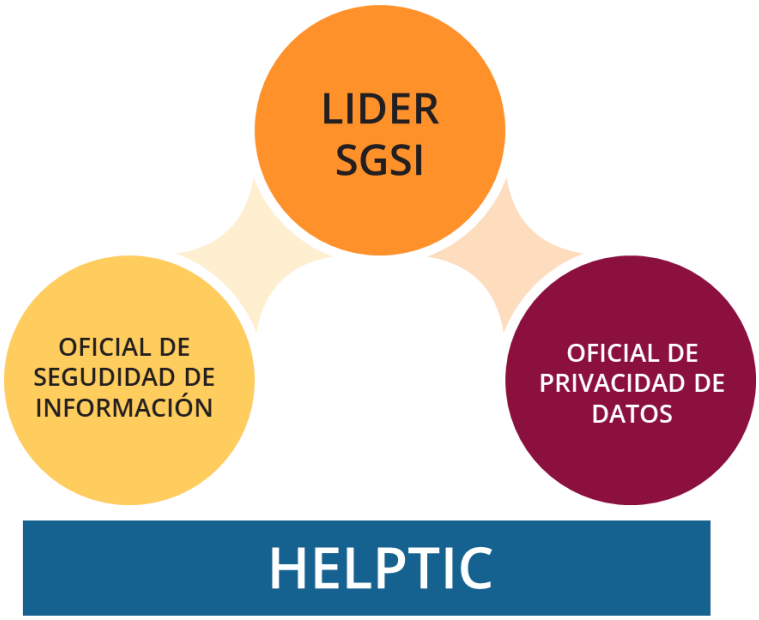


Figura 3. Roles y responsabilidades del SGSI
Fuente: Autor

1.12.1. RESPONSABILIDADES

Las funciones específicas de cada rol en la organización del SGSI son:

- **Líder del SGSI**
  - Coordinar la implementación y gestión de las políticas relacionadas con la seguridad y privacidad.
  - Supervisar el cumplimiento normativo.
  - Garantizar la privacidad de los datos.

- Administrar al Equipo de Respuesta ante Incidentes de Seguridad de la información HELPTIC.
- Supervisar la administración de identidades y acceso.
- Coordinar y supervisar la arquitectura de seguridad del Municipio.
- Llevar a cabo el descubrimiento electrónico y las investigaciones forenses digitales.
- Trabajar con otros ejecutivos de alto nivel para establecer los planes de recuperación de desastres (DR) y continuidad del negocio.

- **Oficial de seguridad de la información**
  - Apoyar la implementación y gestión del MSPI.
  - Definir, revisar y evaluar la Política de seguridad de la información del Municipio.
  - Definir, revisar y evaluar los procedimientos para aplicar la Política de seguridad de la información.
  - Seleccionar y gestionar los mecanismos y herramientas adecuados que permitan aplicar las políticas de seguridad de la información.
  - Aplicar metodologías de análisis de riesgo en el Municipio.
  - Promover la aplicación de auditorías enfocadas a la seguridad, para evaluar las prácticas de seguridad.
  - Crear y vigilar los lineamientos necesarios que coadyuven a tener los servicios de seguridad.
  - Coordinar el grupo de seguridad informática y la gestión de incidentes en la organización articulado don la mesa de ayuda HELPTIC.
  - Promover e impulsar la formación, educación y concienciación seguridad de la información.

- **Oficial de privacidad de datos:**
  - Apoyar la implementación y gestión del MSPI.
  - Definir, revisar y evaluar la Política de privacidad y de protección de datos del Municipio.

- Valorar el impacto sobre el marco de privacidad y la protección de los datos personales de nuevos proyectos o de normas que afecten al Municipio.
- Coordinar la atención de los ejercicios de los derechos de los interesados en cuento a reclamaciones formuladas por los titulares de la información.
- Establecer relaciones con las autoridades en protección de datos (SIC).
- Supervisar la gestión de incidencias con ayuda del grupo de respuesta HELPTIC.
- Coordinar los planes de auditoría, ya sea de carácter interno o externo.
- Impulsar la adopción de medidas en con junto a las políticas de seguridad da la información para asegurar el cumplimiento de la normativa de protección de datos.
- Impulsar y promover buenas prácticas en protección de datos.
- Promover e impulsar la formación, educación y concienciación en protección de datos.

- **Mesa de servicios (HelpTIC)**
  - Desarrollar acciones de mitigación de incidentes de seguridad de la información.
  - Reportar y registrar incidentes en la base documental disponible del Municipio.
  - Reportar a los oficiales de seguridad y privacidad riesgos de activos de información, malas prácticas por parte de los usuarios.
  - Implementar controles y configuraciones en pro de la seguridad y privacidad.

1.13. FASES DE IMPLEMENTACIÓN

Mediante las cartillas publicadas por el MINTIC se establecen las siguientes fases que serán adoptadas por el MUNICIPIO DE BUCARAMANGA:

- **Diagnóstico de seguridad y privacidad de la información:** Con el cual se podrá establecer el nivel actual de la entidad en este tema.
- **Planificación:** Donde se determinarán las acciones a tomar verificando la alineación estratégica de la entidad para la construcción de acciones objetivas.

- **Implementación:** Se busca la identificación valoración, tratamiento y mitigación de riesgos asociados al manejo de la información.
- **Evaluación y mejoramiento continuo:** para la revisión de acciones tomadas y la mejora continua a través de la gestión del conocimiento y lecciones aprendidas en la implementación.

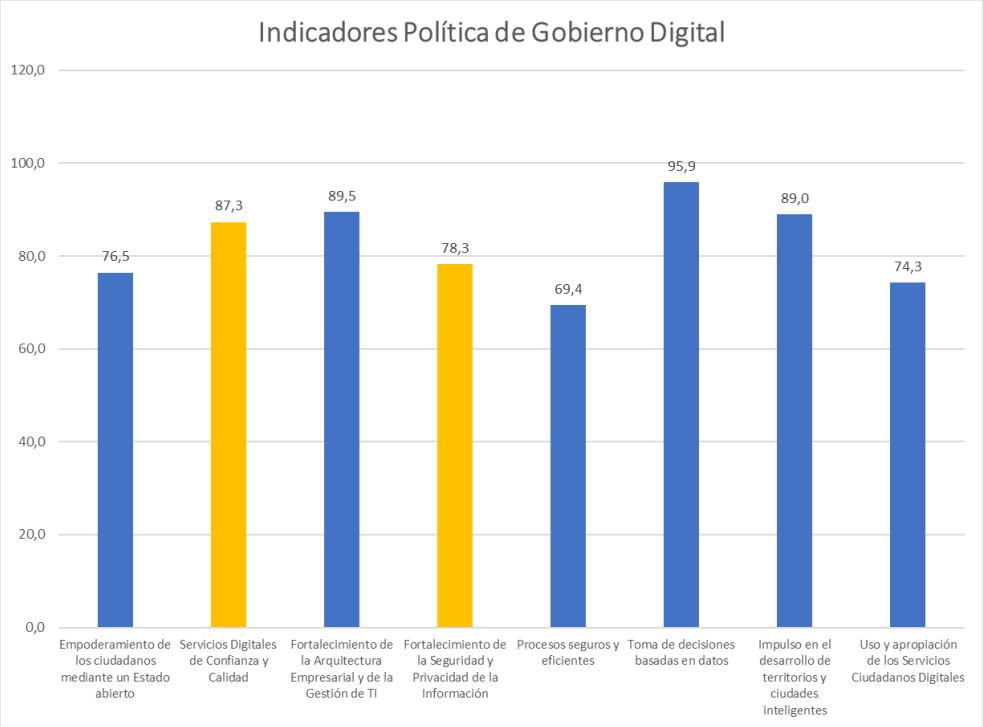
Figura 4. Fases de implementación
Fuente: Manual GEL 3.1

2. SITUACION ACTUAL A NIVEL DE SEGURIDAD DE LA INFORMACION

Tomando como base los resultados obtenidos en la política de seguridad de la información en la última evaluación (2021) del FURAG, la entidad obtuvo un puntaje de 77.8, logrando una mejora de 11 puntos porcentuales con respecto al año 2.020 donde se obtuvo un puntaje de 66.8 , es importante mencionar que estas mediciones se realizan año vencido, por tal motivo la medición realizada en 2022 corresponde a la vigencia 2.021.

2.1. FASE DE DIAGNOSTICO

A continuación, se muestra el resultado del diagnóstico realizado a final del 2021, donde se evidencia el porcentaje de avance de los indicadores relacionados con Seguridad y Privacidad de la información incluidos en la Política de Gobierno Digital, los cuales apoyan la Política de Seguridad Digital:



Para el cumplimiento de esta fase se establecen los siguientes lineamientos:

- **LI.ES.01:** Las instituciones de la administración pública deben contar con una estrategia de TI que esté alineada con las estrategias sectoriales, el Plan Nacional de Desarrollo, los planes sectoriales, los planes decenales -cuando existan- y los planes estratégicos institucionales. La estrategia de TI debe estar orientada a generar valor y a contribuir al logro de los objetivos estratégicos.

- **LI.ES.02:** Cada sector e institución, mediante un trabajo articulado, debe contar con una Arquitectura Empresarial que permita materializar su visión estratégica utilizando la tecnología como agente de transformación. Para ello, debe aplicar el Marco de Referencia de Arquitectura Empresarial para la gestión de TI del país, teniendo en cuenta las características específicas del sector o la institución.

- **LI.ES.03:** La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e implementar un esquema de Gobierno TI que estructure y direccione el flujo de las decisiones de TI, que garantice la integración y la alineación con la normatividad vigente, las políticas, los procesos y los servicios del Modelo Integrado de Planeación y Gestión de la institución.

A continuación, se muestra el estado de cada uno de los entregables planteados de acuerdo con la trazabilidad y seguimiento realizado con respecto al documento anterior:

Meta	Entregable
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad, teniendo en cuenta la infraestructura de red de comunicaciones (IPv4/IPv6).	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección.

Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.	Documento con el resultado de la herramienta de la encuesta.
Realizar pruebas que permitan a la Entidad medir la efectividad de los controles existentes.	Documento con el resultado de las estrategias implementadas por la entidad.

2.2. FASE DE PLANIFICACIÓN

A continuación, se muestra el estado de cada uno de los entregables planteados de acuerdo con la trazabilidad y seguimiento realizado con respecto al documento anterior:

Meta	Entregable
Objetivos, alcance y límites del MSPI.	Documento con el alcance y límites de la seguridad de la información, debidamente aprobado y socializado al interior de la Entidad, por la alta dirección
Políticas de seguridad y privacidad de la información.	Documento con las políticas de seguridad y privacidad de la información, debidamente aprobadas y socializadas al interior de la Entidad, por la alta Dirección.
Procedimientos de control documental del MSPI.	Formatos de procesos y procedimientos, debidamente definidos, establecidos y aprobados por el comité que integre los sistemas de gestión institucional.
Asignación de recurso humano, comunicación de roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (ó el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección.
Inventario de activos de información.	Documento de inventario de activo de información, revisado y aprobado por la alta Dirección
Acciones para tratar riesgos y oportunidades de seguridad de la información. Identificación y valoración de riesgos de (Metodología, Reportes). o Tratamiento de riesgos (Selección de controles).	Documento con el informe de análisis de riesgos, matriz de riesgos, plan de tratamiento de riesgos y declaración de aplicabilidad, revisado y aprobado por la alta Dirección

Toma de conciencia.	Documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección
Plan y estrategia de transición de IPv4 a IPv6.	Documento con el plan y estrategia de transición de IPv4 a IPv6, revisado y aprobado por la alta Dirección.

2.3. FASE DE IMPLEMENTACIÓN

A continuación, se muestra el estado de cada uno de los entregables planteados de acuerdo con la trazabilidad y seguimiento realizado con respecto al documento anterior:

Meta	Entregable
Planificación y control operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
Implementación de controles.	Documento con el informe del plan de tratamiento de riesgos, que incluya la implementación de controles de acuerdo con lo definido en la declaración de aplicabilidad, revisado y aprobado por la alta Dirección
Implementación del plan de tratamiento de riesgos	Indicadores de gestión del MSPI, revisado y aprobado por la alta Dirección
Implementación del plan y estrategia de transición de IPv4 a IPv6	Documento con el informe de la implementación del plan y la estrategia de transición de IPv4 a IPv6, revisado y aprobado por la alta Dirección

2.4. FASE DE EVALUACIÓN

A continuación, se muestra el estado de cada uno de los entregables planteados de acuerdo con la trazabilidad y seguimiento realizado con respecto al documento anterior:

Meta	Entregable
Plan de seguimiento, evaluación y análisis del MSPI.	Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.
Auditoría Interna	Documento con el plan de auditorías internas y resultados, de acuerdo con lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección.

Evaluación del plan de tratamiento de riesgos.	Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección

2.5. FASE DE MEJORA CONTINUA

A continuación, se muestra el estado de cada uno de los entregables planteados de acuerdo con la trazabilidad y seguimiento realizado con respecto al documento anterior:

Meta	Entregable
Plan de seguimiento, evaluación y análisis para el MSPI	Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección
Auditoría Interna	Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta Dirección
Comunicación de resultados y plan de mejoramiento.	
Revisión y aprobación por la alta Dirección.	

CONCLUSIONES

Es importante entender que, como tal, la información es el activo más importante en la actualidad para cualquier organización pública o privada, es por ello por lo que el mantener debidamente documentado los procesos, estrategias y políticas que la protegen y gestionan permiten a dichas organizaciones garantizar en gran medida la disponibilidad e integridad de la misma.

Mantener los principios de confidencialidad, disponibilidad e integridad de la información, especialmente al interior de la entidad públicas es fundamental para brindar la seguridad adecuada tanto a los usuarios internos como externos (ciudadanos) de que sus datos y la trazabilidad de estos están protegidos adecuadamente.

El presente documento tiene como uno de sus objetivos, servir de referente a las entidades descentralizadas del municipio, para que pueda ser usado como base y ser adaptado de acuerdo con cada una de las mismas, buscando sinergias e integraciones que beneficien la labor a nivel protección y privacidad de la información en el municipio de Bucaramanga.

TABLA DE REVISIONES

Versión	Fecha	Autor
Versión 1.0	31/12/2020	Equipo Gobierno Digital - OATIC
Versión 2.0	30/10/2021	Equipo Gobierno Digital – OATIC