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

MUNICIPIO DE BUCARAMANGA

TABLA DE CONTENIDO

1. MARCO DE LA SEGURIDAD DE LA INFORMACIÓN DEL MUNICIPIO DE BUCARAMANGA 4
1.1. DEFINICIÓN 4
1.2. CONTEXTO 4
1.3. ALIADOS ESTRATÉGICOS 5
1.4. CONTEXTO NORMATIVO Y ESTANDARIZACIÓN 6
1.4.1. ESTÁNDARES INTERNACIONALES 6
1.4.2. NORMATIVIDAD COLOMBIANA 6
1.5. POLÍTICAS 7
1.6. ARTICULACIÓN ESTRATÉGICA 8
1.7. CAPACITACIÓN, PROMOCIÓN Y SENSIBILIZACIÓN 8
1.8. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) 9
1.9. OBJETIVO 9
1.10. ALCANCE 10
1.11. LIMITES 10
1.12. ORGANIZACIÓN DEL SGSI 10
1.12.1. RESPONSABILIDADES 11
1.13. FASES DE IMPLEMENTACIÓN 13
2. SITUACION ACTUAL A NIVEL DE SEGURIDAD DE LA INFORMACION 15
2.1. FASE DE DIAGNOSTICO 16
2.2. FASE DE PLANIFICACIÓN 18
2.3. FASE DE IMPLEMENTACIÓN 20
2.4. FASE DE EVALUACIÓN 21
2.5. FASE DE MEJORA CONTINUA 22
CONCLUSIONES 24
ANEXOS ..... **¡Error! Marcador no definido.**

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 la 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. 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 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

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

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:

- **ColCERT**: Grupo de respuestas ante emergencias Cibernéticas de Colombia.
- **CCP**: Centro cibernético policial

[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

- **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

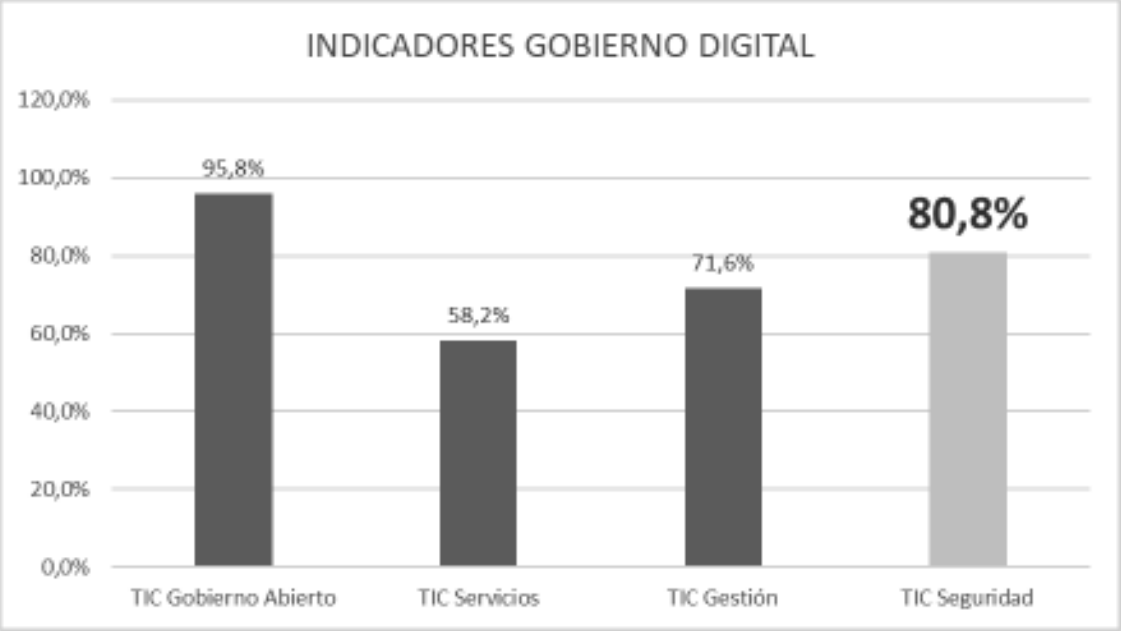
Tomando como base los resultados obtenidos en el habilitador de Seguridad de la Información de la política de Gobierno Digital, a continuación, se muestran los criterios y avances obtenidos a 31 de diciembre de 2020 por la Alcaldía de Bucaramanga.

ITEM / DESCRIPCIÓN	ESTADO	% DE AVANCE
¿La entidad realiza un diagnóstico de seguridad de la información?	Completada	100
¿La entidad adopta una política de seguridad de la información?	En Curso	100
¿La entidad define roles y responsabilidades de seguridad de la información en entidad?	Completada	100
¿La entidad define y apropia procedimientos de seguridad de la información?	Completada	100
¿La entidad realiza gestión de activos de seguridad de la información?	En Curso	100
¿La entidad realiza gestión de riesgos de seguridad de la información?	Completada	100
¿La entidad realiza campañas de sensibilización y toma de conciencia en seguridad?	Completada	100
¿La entidad Implementa el plan de tratamiento de riesgos?	En Curso	50
¿La entidad cuenta con un plan de control operacional de seguridad de la información?	Completada	100
¿La entidad define indicadores de gestión de la seguridad de la información?	Completada	100

¿La entidad define un plan de seguimiento y evaluación a la implementación de seguridad de la información?	En Curso	50
Respecto al plan de auditoria de seguridad de la información, la entidad:	Por iniciar	0
¿La entidad define un plan de mejoramiento continuo de seguridad de la información?	En Curso	50

2.1. FASE DE DIAGNOSTICO

A continuación, se muestra el resultado del diagnostico realizado a final del 2020, donde se evidencia el porcentaje de avance del componente de seguridad y privacidad de la información:



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	Estado	Observaciones
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.	Realizada	Con base en el autodiagnóstico realizado por parte de la entidad, enmarcado dentro de la política de gobierno digital se determinó el estado actual a nivel de gestión de seguridad y

			privacidad de la información
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, revisado, aprobado y aceptado por la alta dirección	En curso	Actualmente se están estableciendo acciones para poder realizar esta identificación, involucrando a una entidad externa en dicho proceso.
Realizar pruebas que permitan a la Entidad medir la efectividad de los controles existentes.	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la dirección.	Por Iniciar	Se iniciará el proceso de diseño de la herramienta para poder medir la efectividad de los controles existentes.

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	Estado	Observaciones
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	Realizado	El documento fue actualizado con respecto al generado en la administración anterior y está en constante revisión y validación.
Políticas de seguridad y privacidad de la información (Ver anexo 1 y 2) *	Documento con las políticas de seguridad y privacidad de la información, debidamente aprobadas y socializadas al interior	Realizado	Los documentos fueron actualizados y publicados.

	de la Entidad, por la alta Dirección.		
Procedimientos de control documental del MSPI (Ver anexo 3) *	Formatos de procesos y procedimientos, debidamente definidos, establecidos y aprobados por el comité que integre los sistemas de gestión institucional.	Realizado	Anexo a este documento.
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.	En curso	El proceso se encuentra en preparación de documentos y guías de implementación para asignación de carga y roles
Inventario de activos de información.	Documento de inventario de activo de información, revisado y aprobado por la alta Dirección	Realizado	Se documentaros los activos de información de la entidad, dicho archivo está en constante revisión y validación.
Acciones para tratar riesgos y oportunidades de seguridad de la información. Identificación y valoración de riesgos de (Metodología, Reportes). o	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	Realizado	Se cuenta con una matriz de riesgos de seguridad de la información y un plan de tratamiento de riesgos de la seguridad digital.

Tratamiento de riesgos (Selección de controles).			
Toma de conciencia.	Documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección	Por iniciar	Se iniciará el proceso de diseño e implementación de un plan de dicho plan.
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.	En curso	se cuenta con el levantamiento de información y estado actual de los activos de información con respecto a la implementación y transición de IPv4 a IPv6.

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	Estado	Observaciones
Planificación y control operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Por iniciar	Se iniciará el proceso de diseño e implementación de la estrategia de planificación y control operacional.

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	Realizado	Se realizo un documento que contiene los controles y acciones de acuerdo con cada uno de los riesgos establecidos en la matriz.
Implementación del plan de tratamiento de riesgos	Indicadores de gestión del MSPI, revisado y aprobado por la alta Dirección	En curso	Se cuenta con indicadores iniciales para el mantenimiento y seguimiento de los riesgos. El documento será completado durante el primer semestre de 2021.
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	En curso	Se cuenta con el diagnóstico y situación actual de IPv6 en la entidad. Durante el año 2021 se dará inicio a la ejecución de este proyecto.

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	Estado	Evidencia
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.	Por iniciar	Se iniciará el proceso de diseño e implementación del plan de seguimiento de MSPI.
Auditoría Interna	Documento con el plan de auditorías internas y resultados, de acuerdo a lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección.	En curso	Estas revisiones se hacen de manera anual y existen las evidencias del proceso.
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	En curso	De manera anual se hace la evaluación de la matriz de riesgos de la entidad, con respecto al 2020, la evaluación y ajuste para el 2021 se realizará durante el primer trimestre del año.

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	Estado	Evidencia
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	Por iniciar	Se iniciará el proceso de diseño e implementación del plan de seguimiento de MSPI.

Auditoría Interna Comunicación de resultados y plan de mejoramiento. Revisión y aprobación por la alta Dirección.	Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta Dirección	En curso	Estas revisiones se hacen de manera anual y existen las evidencias del proceso.

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 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.

ANEXO 1

Política Institucional de Seguridad de la Información para el municipio de Bucaramanga

RESOLUCION N° 0489 DE 2017

" POR LA CUAL SE ADOPTA, ADECUA Y SE ESTABLECE LOS PARAMETROS DE LA POLITICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACION PARA EL MUNICIPIO DE BUCARAMANGA"

LA ALCALDESA (E) DE BUCARAMANGA

En uso de sus atribuciones constitucionales y legales, en especial las consagradas en el numeral 3 del artículo 315 de la Constitución Política, el artículo 91 de la ley 136 de 1994.

CONSIDERANDO:

1. Que en el artículo 15 de la Constitución Política, consagra el derecho fundamental de las personas a conservar su intimidad personal y familiar, al buen nombre y a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellos en bancos de datos y en archivos de las entidades públicas y privadas.

2. Que la Ley 1273 de 2009 por medio del cual se modifica el Código Penal, crea un nuevo bien jurídico tutelado denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones "TIC", entre otras disposiciones.

3. Que la Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales reglamentado por el Decreto 1377 de 2013, incorporó los lineamientos necesarios para que los organismos públicos y privados identificaran los roles y la tipología de datos que son objeto de protección constitucional, así mismo, dispuso las condiciones las cuales se deben recolectar los datos personales que posteriormente serán vinculados con la administración de una base de datos.

4. Que la Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública en las instituciones del Estado, estableció los procedimientos para el ejercicio y garantías para el registro de activos de información.

5. Que por medio del Decreto 1078 de 2015, se expidió el Reglamento de Sector de Tecnologías de la Información y las Comunicaciones en el Artículo 2.2.9.1.2,1 de dicho decreto se instituye los componentes de la estrategia y es cuarto componente denominado **Seguridad de la Información** ***"Comprende las acciones transversales en los demás componentes enunciados, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada"***

6. Que se entiende por Seguridad de la Información, como el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma. Por lo tanto, es importante mitigar los riesgos alrededor de la información mediante la implementación de planes para el manejo de incidentes, así como las herramientas para respaldar las actividades ejecutadas en el Municipio de Bucaramanga, incentivando la cultura de seguridad de la información a los usuarios, previniendo o solucionando posibles ataques informáticos, virus, robos, uso indebido de software o pérdidas de información.

7. Que por medio de CONPES 3854 de 2016 se fijó la política Nacional de seguridad digital, para que las entidades del Estado constituyan mecanismos para la gestión de los riesgos digitales.

8. Que por medio del Acuerdo Municipal 006 de 2016 se adopta el Plan de Desarrollo "Gobierno de las Ciudadanas y los Ciudadanos" 2016-2019, que en la línea de acción 1.3 Gobierno Municipal en Línea señala los lineamientos e indicadores para el cumplimiento de la seguridad de la información.

9. Que el Decreto 0029 de 2016, creó el Comité Antitrámites y de Gobierno en Línea del Municipio de Bucaramanga, designando para presidirlo al Asesor de Despacho Código 105 Grado 26 TIC, ratificado mediante Resolución 0266 de 2016.

9. Que el Decreto 0029 de 2016, creó el Comité Antitrámites y de Gobierno en Línea del Municipio de Bucaramanga, designando para presidirlo al Asesor de Despacho Código 105 Grado 26 TIC, ratificado mediante Resolución 0266 de 2016.

10. Que mediante Resolución 103 de 2017, se adoptó *"el marco institucional de seguridad y privacidad de la información para el municipio de Bucaramanga"*, dándole un doble alcance: seguridad y privacidad, cuando solo debia enfocarse la regulación en el concepto de seguridad de la información, situación que se debe precisar en un nuevo documento.

11. Que el Ministerio de las Tics sugirió algunas observaciones para ser tenidas en cuenta para adecuar y ajustar la Resolución 103 de 2017, en procura del mejoramiento de la política de seguridad de la información, como base para la mejora continua de la misma, adaptándola a la realidad vigente en el sector, las tendencias tecnológicas y los cambios en la gestión de procesos y procedimientos tecnológicos en el Municipio de Bucaramanga.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1°: ADOPTAR el marco institucional de la Seguridad de la Información, en el Municipio de Bucaramanga, como Lineamiento General para la implementación de la Estrategia de Gobierno en Línea.

ARTÍCULO 2°: REGULAR las políticas, alcances, objetivos y procedimientos relacionados con la seguridad de la información, conforme a lo señalado en el presente Decreto.

CAPITULO 1
DISPOSICIONES GENERALES

ARTÍCULO 3°: OBJETO. Gestionar la toma de decisiones para la seguridad de información a través de la articulación de los Sistemas de Gestión de la Administración, implementando políticas, controles y procedimientos que permitan de manera oportuna la atención de riesgos en la seguridad de la información así como la buena gestión de la información en el Municipio.

ARTÍCULO 4°: ALCANCE. El marco institucional de seguridad de la información será la carta de navegación para garantizar el cumplimiento del componente de seguridad y de la información enmarcado en la estrategia de Gobierno en Línea, cuyo alcance comprende todas las secretarias y oficinas de la administración central, a sus servidores públicos, y contratistas para el manejo de la información del Municipio de Bucaramanga, propiciando el fortalecimiento de los sistemas de gestión institucional mediante el manejo adecuado de la información.

ARTÍCULO 5°: ESTABLECIMIENTO DE POLITICAS. El presente Decreto define la política institucional de seguridad de la información para el Municipio de Bucaramanga alineados con los objetivos institucionales, incorpora los diferentes actores de la administración, mediante la implementación de las mejores prácticas para el beneficio de los servicios prestados.

ARTÍCULO 6°: DEFINICIONES. Para una mayor comprensión de la política institucional de seguridad de la información, se define lo siguiente:

Seguridad de información. Es la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser: Electrónicos, En papel o Audio y vídeo, etc.

Activos de información. Los 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.

ARTÍCULO 7°: ROLES Y RESPONSABILIDADES. Para su desarrollo, implementación y cumplimiento se han asignado los siguientes roles y responsabilidades:

Rol Directivo: En cabeza de la Alta Gerencia de la Alcaldía de Bucaramanga, los Secretarios, Jefes de Oficina, Jefes de Área, asistido por el comité de Gobierno en Línea, donde se formulan y toman las decisiones y estrategias relacionadas con la seguridad de la información, así como gestionar y aprobar planes, presupuestos y políticas destinados a fortalecer e implementar la acciones de seguridad de la información.
Rol Operativo: A través del proceso de Gestión de las TIC del Municipio, en cabeza del Asesor de las TICs de la Alcaldía, se ejecutaran tareas y acciones para articular el cumplimiento e implementación de controles de seguridad de la información de carácter técnico y tecnológico articulando con otros procesos para la efectividad y mejoramiento de los mismos. Adicional, deberá garantizar que todo el software que se ejecute los activos de información de la administración central municipal esté protegido por derechos de autor y requiera licencia de uso o, sea software de libre distribución y uso.
Rol de Control: La oficina de Control Interno de Gestión en concurrencia con cada uno de los funcionarios del Nivel Directivo, realizarán evaluación de los planes de implementación relacionados con la seguridad de la información de acuerdo a los lineamientos nacionales de la estrategia de Gobierno en línea y los entes de control.
Rol Implementación: Todos los servidores públicos y contratistas del Municipio tienen el compromiso de cumplir la presente política velando por su correcta implementación ya apoyando los diferentes roles a la mejora continua de las acciones para prevenir incidentes relacionados con la seguridad de la información en el Municipio. A su vez, deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software, recordando que es ilegal duplicar software, duplicar documentación sin la autorización del propietario bajo los principios de derechos de autor y, la reproducción no autorizada es una violación a la ley.

ARTÍCULO 8°: PROMOCIÓN DE LA CULTURA DE LA SEGURIDAD DE LA INFORMACIÓN. Se promoverá la cultura organizacional de la seguridad de la información mediante capacitaciones, directrices u otras alternativas tendientes a sensibilizar sobre el manejo de la información mitigando los riesgos asociados a la misma.

CAPITULO 2
POLITICA INSTITUCIONAL DE SEGURIDAD INFORMACIÓN

ARTÍCULO 9°: DEFINICION. El municipio de Bucaramanga como entidad territorial fundamental de la división político administrativa del Estado, con autonomía política, fiscal y administrativa, dentro de los límites que señalen la Constitución y la ley y cuya finalidad es el bienestar general y el mejoramiento de la calidad de vida de la población en su respectivo territorio, está comprometido a proteger los activos de información de la entidad (Empleados, información y entorno laboral), orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, a la continuidad de las operaciones de gobemabilidad, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad en los funcionarios, contratistas, proveedores y personas que hagan uso de los activos de información creando condiciones de seguridad y confianza en el manejo de sus activos de información desde la administración.

Las Políticas de Seguridad de la Información, surgen como una herramienta institucional de obligatorio cumplimiento por parte de cada uno de los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la administración central municipal.

PARAMETROS DE LA POLÍTICA INSTITUCIONAL DE SEGURIDAD LA INFORMACIÓN

ARTÍCULO 10°: PROPIEDAD DE LA INFORMACIÓN. El Municipio de Bucaramanga tiene la propiedad absoluta de la información manejada en la gestión institucional por los servidores públicos y contratistas u otros delegados del Municipio para el manejo de la información, deberán acordar la confidencialidad del manejo de la información garantizando su buen uso de acuerdo a sus funciones u obligaciones para el manejo operativo y de conservación, sin perjuicio para el Municipio de Bucaramanga de perder la propiedad de la información.

ARTÍCULO 11°: GESTIÓN DE ACTIVOS. Se entenderá como activo de información todo documento u archivo físico, electrónico o digital que tiene valor para la gestión institucional del Municipio de Bucaramanga, por lo tanto es la intención de la Alta Gerencia de la Alcaldía de Bucaramanga, los Secretarios, Jefes de Oficina, Jefes de Área, funcionarios, contratistas, y en general a todos los usuarios de la información que permitan el cumplimiento de los propósitos generales en la protección de los activos de información, su confidencialidad, integridad, disponibilidad y legalidad de la misma, garantizando la continuidad de los Sistemas, gestionar los riesgos para disminuir los posibles daños y asignar los recursos y personal para tal fin. Así mismo, el responsable de gestión documental y la oficina asesora de TIC se encargarán de:

1. Inventariar activos de información según su categoría y uso.
2. Determinar el proceso responsable.
3. Determinar posibles riesgos asociados al manejo de activo de información.
4. Proteger los activos según lo determinado por el plan de gestión de riesgos.

Para poder cumplimiento a lo anterior, el Municipio deberá asignar los respectivos recursos técnicos y humanos para una adecuada gestión de los Activos.

ARTÍCULO 12°: CONTROL DE ACCESO. El Municipio de Bucaramanga a través de la oficina asesora de TIC, determinará los controles de acceso a la información necesarios en sus equipos, sistemas de información, redes internas u otros activos de información que lo requieran.

Por lo cual, será función de la oficina asesora de TIC fijará mantener y actualizar medidas de control de acceso soportados en la cultura de seguridad en la entidad, garantizando el uso exclusivo de los activos de información para la realización de las funciones u obligaciones de los servidores públicos y contratistas gestionando la trazabilidad y el no repudio del uso de los accesos.

ARTÍCULO 13°: ADMINISTRACIÓN DE REDES Y EQUIPOS. Los recursos tecnológicos del Municipio de Bucaramanga, son herramientas de apoyo a las labores y responsabilidades de los servidores públicos y contratistas. Por lo tanto, la oficina asesora de TIC como administradora de la infraestructura tecnológica, dispondrá de los lineamientos necesarios para garantizar la disponibilidad, soporte y mantenimiento de redes y equipos.

ARTÍCULO 14°: USO DE SOFTWARE Y SISTEMAS DE INFORMACIÓN, CORREO ELECTRÓNICO Y USO DE INTERNET. Todos los servidores públicos y contratistas del Municipio de Bucaramanga son responsables del buen uso del software, sistemas de información, correo electrónico y uso de internet, respetando la legalidad del software, evitando instalar software no licenciado de equipos.

El uso de sistemas de información, herramientas de correo electrónico o el acceso a internet que provee o delega el Municipio de Bucaramanga para las funciones u obligaciones del servidor público o contratistas deberá solo ser usado con fines institucionales evitando cualquier uso con interés personal.

ARTÍCULO 15°: RESPONSABILIDADES Y CONTRASEÑAS. Todos los servidores públicos y contratistas del Municipio de Bucaramanga a los que le asignen contraseñas tendrán un uso adecuado a los fines institucionales.

Por lo tanto, cada servidor público o contratistas debe asumir la responsabilidad del cuidado del usuario y contraseña asignada evitando el préstamo u otra actividad que suponga el uso indebido de los activos de información.

ARTÍCULO 16°: SEGURIDAD FÍSICA DEL ENTORNO. El Municipio de Bucaramanga a través de la oficina asesora de TIC, determinará las áreas seguras donde reposan activos de información críticos para el Municipio de Bucaramanga, proponiendo planes para impedir el acceso no autorizado, evitar robo, pérdida, daño, entre otros que puedan afectar los activos de información, medios de procesamientos y comunicaciones.

ARTÍCULO 17°: GESTIÓN DE RIESGOS. Para la gestión de riesgos asociados al manejo de la información, la oficina asesora de TIC trabajará conjuntamente con las oficinas de control interno de gestión y el sistema de gestión integrado con el fin de apoyar la identificación de riesgos a las demás dependencias, elaborar planes de mitigación de riesgos y realizar monitoreo promoviendo las acciones preventivas y correctivas requeridas.

ARTÍCULO 18°: GESTIÓN DEL CONOCIMIENTO. La oficina Asesora de TIC liderará la adopción de herramientas para garantizar la conservación del conocimiento relacionado con la seguridad de la información y otros temas de carácter estratégico, para lograr procesos de mejora continua y permitir acciones en cumplimiento de la estrategia de Gobierno en línea.

ARTÍCULO 19°: GESTIÓN DE INCIDENTES. La oficina asesora de TIC establecerá los procedimientos de preparación, detección y análisis, contención / respuesta, erradicación y recuperación ante incidencias asociadas a la seguridad de la información de acuerdo a la capacidad institucional disponible.

ARTÍCULO 20°: CONTINUIDAD DE SERVICIOS DE TECNOLOGIA DE LA INFORMACION "T.I.". Se deberá desarrollar planes de continuidad para aquellos servicios que son críticos para el Municipio de Bucaramanga. Los planes deben considerar medidas tanto técnicas como administrativas para garantizar la disponibilidad de los servicios de TI, por lo cual desde la oficina asesora de TIC de promoverá la construcción integral de un plan de contingencia de acuerdo a la capacidad institucional disponible.

ARTÍCULO 21°: EFECTOS RELACIONADOS CON EL INCUMPLIMIENTO DE LA POLITICA. De incumplirse los parámetros fijados para la Política Institucional de Seguridad de la Información, los responsables de su ejecución y los demás usuarios involucrados en su cumplimiento, quedarán sujetos a las acciones disciplinarias contenidas en el Código Disciplinario Único y sus modificaciones, así como en el manual o reglamento de trabajo, sin perjuicio de las acciones penales o contractuales a que haya lugar.

CAPÍTULO 3.
MODIFICACIONES, CUMPLIMIENTO Y VIGENCIA

ARTÍCULO 22°: El presente marco de política institucional de seguridad de la información podrá ser modificado, adicionado y ajustado previa aprobación del Comité Antitrámites y de Gobierno en Línea, de acuerdo al mejoramiento continuo de los procesos de la Administración y por los requerimientos legales vigentes.

ARTÍCULO 23°: La presente resolución rige a partir de la fecha de publicación, y deroga las disposiciones que le sean contrarias, en especial la Resolución 103 de 2017.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dada en Bucaramanga, 29 DIC 2017

ALBA ASUSENA NAVARRO FERNANDEZ.
Alcaldesa de Bucaramanga (E).

Proyectó/ Sergio Cajias Lizcano-Asesor TIC

TABLA DE CONTENIDO

1. OBJETIVO, ALCANCE Y USUARIOS 2

2. DOCUMENTOS DE REFERENCIA 2

3. TERMINOLOGÍA BÁSICA SOBRE SEGURIDAD DE LA INFORMACIÓN 2

4. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 3

4.1. OBJETIVOS Y MEDICIÓN 3
4.2. REQUISITOS PARA LA SEGURIDAD DE LA INFORMACIÓN 4
4.3. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN 4
4.4. RESPONSABILIDADES 4
4.5. COMUNICACIÓN DE LA POLÍTICA 5
4.6. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN 5

5. APOYO PARA LA IMPLEMENTACIÓN DEL SGSI 6

6. VALIDEZ Y GESTIÓN DE DOCUMENTOS 6

7. HISTORIAL DE CAMBIOS 6

1. OBJETIVO, ALCANCE Y USUARIOS

La ALCALDÍA MUNICIPAL DE BUCARAMANGA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para la ALCALDÍA MUNICIPAL DE BUCARAMANGA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, capítulos 5.2 y 5.3
- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Disponible en https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Versi%C3%B3n+5+-+Diciembre+de+2020.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=1611247032238&download=true
- Modelo de Seguridad y Privacidad de la Información. Disponible en https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

3. TERMINOLOGÍA BÁSICA SOBRE SEGURIDAD DE LA INFORMACIÓN

- **Confidencialidad**: característica de la información por la cual solo está disponible para personas o sistemas autorizados.
- **Integridad**: característica de la información por la cual solo que es modificada por personas o sistemas autorizados y de una forma permitida.
- **Disponibilidad**: característica de la información por la cual solo pueden acceder las personas autorizadas cuando sea necesario.
- **Seguridad de la información**: es la preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Sistema de gestión de seguridad de la información**: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

4. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.1. Objetivos y medición

Esta política aplica a la ALCALDÍA MUNICIPAL DE BUCARAMANGA según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

a. Minimizar el riesgo en las funciones más importantes de la entidad.
b. Cumplir con los principios de seguridad de la información.
c. Cumplir con los principios de la función administrativa.
d. Mantener la confianza de sus clientes, socios y empleados.
e. Apoyar la innovación tecnológica.
f. Proteger los activos tecnológicos.
g. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
h. Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la ALCALDÍA MUNICIPAL DE BUCARAMANGA.
i. Garantizar la continuidad del negocio frente a incidentes.
j. La ALCALDÍA MUNICIPAL DE BUCARAMANGA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

La ALCALDÍA MUNICIPAL DE BUCARAMANGA medirá el cumplimiento de todos los objetivos. El Líder de Seguridad y Privacidad de la Información es el responsable de definir el método para medir el cumplimiento de los objetivos; la medición se realizará al menos al menos una vez al año y el Líder de Seguridad y Privacidad de la Información analizará y evaluará los resultados y los reportará al Líder de Planeación como material para la revisión por la Dirección. El Líder de Seguridad y Privacidad de la Información es responsable de registrar los detalles sobre los métodos de medición, periodicidades y resultados en el Informe de Medición.

4.2. Requisitos para la seguridad de la información

Esta Política, y todo el SGSI, deben cumplir los requisitos legales y normativos importantes para la organización en el ámbito de la Seguridad y Privacidad de la información, como también con las obligaciones contractuales.

En la Lista de obligaciones legales[1], normativas y contractuales se detalla una lista de requisitos contractuales y legales.

4.3. Controles de seguridad de la información

El proceso de elegir los controles (protección) está definido en la metodología de evaluación y tratamiento de riesgos.

Los controles seleccionados y su estado de implementación se detallan en la Declaración de aplicabilidad.

4.4. Responsabilidades

Las responsabilidades para el SGSI son las siguientes:

- El Líder de Seguridad y Privacidad de la Información es el responsable de garantizar que el SGSI sea implementado y mantenido de acuerdo con esta Política y de garantizar que todos los recursos necesarios estén disponibles.
- El Líder de Seguridad y Privacidad de la Información es el responsable de la coordinación operativa del SGSI, como también de informar su desempeño.
- El alcalde Municipal o a quien designe, debe revisar el SGSI al menos una vez por año o cada vez que se produzca una modificación significativa; y debe elaborar actas de dichas reuniones. El objetivo de las verificaciones por parte de la dirección es establecer la conveniencia, adecuación y eficacia del SGSI.
- El Líder de Seguridad y Privacidad de la Información implementará programas de formación y concienciación de empleados sobre seguridad de la información.
- La protección de la integridad, disponibilidad y confidencialidad de los activos es responsabilidad del propietario de cada activo.
- Todos los incidentes o debilidades de seguridad deben ser informados al Líder de Seguridad y Privacidad de la Información.
- El Líder de Seguridad y Privacidad de la Información definirá qué información relacionada con la seguridad y privacidad de la información será comunicada a qué parte interesada (tanto interna como externa), por quién y cuándo.

[1] Ley 1581 de 2012 , Política de Gobierno Digital

- El Líder de Seguridad y Privacidad de la Información es el responsable de adoptar e implementar el Plan de formación y concienciación, que corresponde a todos los funcionarios que participan en la gestión de la seguridad de la información.

4.5. Comunicación de la Política

El Líder de Seguridad y Privacidad de la Información debe asegurarse de que todos los funcionarios de la ALCALDÍA MUNICIPAL DE BUCARAMANGA, como también los participantes externos correspondientes, estén familiarizados con esta Política.

4.6. Principios de Seguridad de la Información

A continuación, se establecen once principios de seguridad que soportan el SGSI de La ALCALDÍA MUNICIPAL DE BUCARAMANGA:

i. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
ii. La ALCALDÍA MUNICIPAL DE BUCARAMANGA protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
iii. La ALCALDÍA MUNICIPAL DE BUCARAMANGA protegerá la información creada, procesada, transmitida o resguardada por sus procesos internos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
iv. La ALCALDÍA MUNICIPAL DE BUCARAMANGA protegerá su información de las amenazas originadas por parte de orígenes internos o externos.
v. La ALCALDÍA MUNICIPAL DE BUCARAMANGA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
vi. La ALCALDÍA MUNICIPAL DE BUCARAMANGA controlará la operación de sus procesos internos garantizando la seguridad de los recursos tecnológicos y las redes de datos.
vii. La ALCALDÍA MUNICIPAL DE BUCARAMANGA implementará control de acceso a la información, sistemas y recursos de red.
viii. La ALCALDÍA MUNICIPAL DE BUCARAMANGA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
ix. La ALCALDÍA MUNICIPAL DE BUCARAMANGA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

x. La ALCALDÍA MUNICIPAL DE BUCARAMANGA garantizará la disponibilidad de sus procesos internos y la continuidad de su operación basada en el impacto que pueden generar los eventos.
xi. La ALCALDÍA MUNICIPAL DE BUCARAMANGA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

5. APOYO PARA LA IMPLEMENTACIÓN DEL SGSI

A través del presente, el ALCALDE MUNICIPAL DE BUCARAMANGA declara que en la implementación y mejora continua del SGSI se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta Política, como también para cumplir con todos los requisitos identificados.

6. VALIDEZ Y GESTIÓN DE DOCUMENTOS

Este documento es válido hasta el 31 de diciembre de 2022

El propietario de este documento es el Líder de Seguridad y Privacidad de la Información, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de funcionarios y participantes externos que cumplen una función en el SGSI pero que no están familiarizados con el presente documento.
- No cumplimiento del SGSI con las leyes y normas, las obligaciones contractuales y con los demás documentos internos de la entidad.
- Ineficacia de la implementación y mantenimiento del SGSI.
- Responsabilidades ambiguas para la implementación del SGSI.

7. HISTORIAL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA
0.0	Se incluye en el SIGC la política de seguridad y privacidad de la información de la Administración Municipal, la cual fue adoptada y adecuada por la Resolución 0489 de 2017.	Mayo-21-2019

1.0	Actualización de la política de seguridad y privacidad de la información por requerimiento del proceso Gestión de las TIC. Adicionalmente es aprobado por el comité de MIPG de la Entidad.	Diciembre-06-2021

ANEXO 2

Política tratamiento datos personales

Alcaldía de Bucaramanga

Construcción Social, Transparencia y Dignidad

RESOLUCION No. 0340 DE 2018

(26 DIC 2018)

"POR LA CUAL SE ADOPTA LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL MUNICIPIO DE BUCARAMANGA SANTANDER"

EL ALCALDE DE BUCARAMANGA

En uso de sus facultades constitucionales y legales conferidas en el numeral 3 del Artículo 315 de la Constitución Política y el numeral 1 literal D del Artículo 91 de la Ley 136 de 1994, y

CONSIDERANDO:

A. Que de conformidad con lo dispuesto en el artículo 315 numeral 3 de la Constitución Política de Colombia, es atribución de los Alcaldes Municipales: *"Dirigir la acción administrativa del municipio; asegurar el cumplimiento de las funciones y la prestación de los servicios a su cargo; representarlo judicial y extrajudicialmente; y nombrar y remover a los funcionarios bajo su dependencia y a los gerentes o directores de los establecimientos públicos y las empresas industriales o comerciales de carácter local, de acuerdo con las disposiciones pertinentes."*; Disposición concordante con lo señalado en el Artículo 91, literal D, numeral 1 de la Ley 136 de 1994, modificado por el Artículo 29 de la ley 1551 de 2012.

A. Que el Congreso de Colombia, expidió la Ley Estatutaria 1581 de 2012, por medio de la cual se dictan disposiciones generales para la protección de datos personales, el cual tiene por objeto "desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma".

B. Que el Presidente de la República de Colombia, en uso de sus atribuciones constitucionales, y en particular las previstas en el numeral 11 del artículo 189 de la Constitución Política y en la Ley 1581 de 2012, expide el Decreto Reglamentario 1377 del 27 de junio de 2013 (hoy compilado por el Decreto 1074 de 2015), con el fin de facilitar la implementación y cumplimiento de la Ley 1581 de 2012.

C. Que el artículo 2° de la Ley 1581 de 2012, establece dentro del ámbito de aplicación, que los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

D. Que de conformidad con lo dispuesto en el artículo 2.2.2.25.6.1. del Decreto 1074 de 2015, los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012, en una manera que sea proporcional a la naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente, por tanto, deberá proceder a implementar la presente Ley, mediante acto administrativo motivado y dando plena aplicación a la Ley.

E. Que la Ley Estatutaria 1581 de 2012, deberá implementarse en el Municipio de Bucaramanga, mediante la adopción de un Manual de Políticas y Procedimientos para la protección de datos personales.

F. El Municipio de Bucaramanga en su calidad de responsable del tratamiento de Información Personal se encuentra comprometido con el cumplimiento de la normatividad referida y, en consecuencia, promoverá el respeto de los principios y normas sobre protección de datos personales por parte de sus trabajadores y Encargados del tratamiento de datos, liderando procesos de mejoramiento continuo y asegurando la conformidad con la Ley.

De conformidad con lo expuesto,

RESUELVE:

ARTICULO PRIMERO: ADOPTAR MEDIANTE LA PRESENTE RESOLUCIÓN, LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL MUNICIPIO DE BUCARAMANGA SANTANDER"

ARTICULO SEGUNDO: Ordenar a las diferentes Secretarias y dependencias del Municipio de Bucaramanga, la implementación y puesta en marcha de la POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES dando aplicación de manera armónica e integral de acuerdo a los principios de conformidad con lo dispuesto en el artículo 4° de la Ley 1581 de 2012.

ARTICULO TERCERO: El Manual de politicas y procedimientos, será parte integral de esta Resolución.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dado en Bucaramanga, a los 26 DIC 2018

RODOLFO HERNANDEZ SUAREZ
Alcalde Municipal

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DEL MUNICIPIO DE BUCARAMANGA
Ley 1581 de 2012
Decreto 1074 de 2015

1. CONSIDERACIONES.

A través de la Resolución 103 de 2017 el Municipio de Bucaramanga (en adelante "la entidad") adoptó el marco institucional de Seguridad y Privacidad de la información, como lineamiento general para la implementación de la Estrategia Gobierno en Línea.

El Municipio de Bucaramanga en su compromiso con el respeto y garantía de los derechos de los ciudadanos, usuarios, contratistas, trabajadores de libre nombramiento y remoción, carrera administrativa, provisionalidad, trabajadores oficiales, aprendices Sena, docentes, directivos docentes, administrativos de instituciones educativas oficiales del municipio y terceros en general, adopta la siguiente política de tratamiento de datos personales de obligatoria aplicación en todas las actividades que involucre, total o parcialmente, la recolección, el almacenamiento, el uso, la circulación y supresión de datos personales.

La presente política es de estricto cumplimiento para la entidad en calidad de responsable del tratamiento de datos personales, así como todos los terceros que obran en nombre de la entidad, o que sin actuar en nombre del Municipio de Bucaramanga tratan datos personales por disposición de ésta como encargados del tratamiento de datos personales.

2. IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO

RAZÓN SOCIAL: Municipio de Bucaramanga
DIRECCIÓN: Carrera 11 No. 34 -52 Fase 2 P2
CIUDAD: Bucaramanga, Santander.
TELÉFONO: (037) 6337000 - 6422110
CORREO: protecciondedatos@bucaramanga.gov.co
PORTAL WEB: www.bucaramanga.gov.co

3. NORMAS QUE RIGEN EL TRATAMIENTO DE DATOS PERSONALES

La Constitución Política de Colombia en su catálogo de derechos fundamentales consagra en su artículo 15 el derecho que tienen todas las personas a su intimidad, buen nombre y al hábeas data. Aunado a lo anterior, se encuentra la Ley Estatutaria 1581 de 2012 como el principal instrumento normativo promulgado en materia de protección de datos personales, norma mediante la cual se establecen las condiciones mínimas que deben observarse para efectuar

un tratamiento adecuado de datos personales por parte de los responsables del tratamiento.

La Ley 1581 de 2012 fue reglamentada posteriormente por el Decreto 1074 de 2015, el cual complemento y aclaró las disposiciones normativas de la Regulación General y precisaron el alcance de los deberes y obligaciones que están llamados a cumplir los responsables y Encargados del tratamiento de datos personales.
Así mismo, la Ley 1712 de 2014, reglamentada parcialmente por el Decreto 103 de 2015 regularon el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información y constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia.
El Municipio de Bucaramanga en su calidad de responsable del tratamiento de Información Personal se encuentra comprometido con el cumplimiento de la normatividad referida y, en consecuencia, promoverá el respeto de los principios y normas sobre protección de datos personales por parte de sus trabajadores y Encargados del tratamiento de datos, liderando procesos de mejoramiento continuo y asegurando la conformidad con la Ley.

4. DEFINICIONES

Conforme a las definiciones dadas en los antecedentes legales expuestos, se tienen como definiciones básicas de los conceptos que implican el manejo de datos personales, los siguientes:

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales[1].

- **Aviso de privacidad:** Comunicación verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.[2]

- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.[3]

[1] Literal a), artículo 3, Ley 1581 de 2012.
[2] Numeral 1, artículo 2.2.2.25.1.3, Decreto 1074 de 2015.
[3] Literal b), artículo 3, Ley 1581 de 2012.

- **Consulta:** Solicitud del titular del dato o las personas autorizadas por éste o por la Ley para acceder a la información que repose en cualquier base de datos, bien sea que esté contenida en un registro individual o que esté vinculada con la identificación del Titular.

- **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[4].

- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables[5].

- **Dato privado:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

- **Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva[6].

- **Dato semiprivado:** Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento y divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas, o a la sociedad en general, como el dato financiero y crediticio[7].

- **Datos sensibles:** Aquellos datos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos

[4] Literal j), artículo 6, Ley 1712 de 2014
[5] Literal c), artículo 3, Ley 1581 de 2012
[6] Numeral 2, artículo 2.2.2.25.1.3, Decreto 1074 de 2015
[7] Literal g), artículo 3, Ley 1266 de 2008

políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos[8].

- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento[9].

- **Información pública:** Es toda información que el responsable y/o encargado del tratamiento, genere, obtenga, adquiera, o controle en su calidad de tal[10].

- **Información pública clasificada:** Es aquella información que estando en poder de un sujeto responsable 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 la ley[11].

- **Información pública reservada:** Es aquella información que estando en poder de un sujeto responsable en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos[12].

- **Oficial de protección de datos:** Persona(s) que han sido designada(s) internamente por el Municipio de Bucaramanga para ejercer de manera formal la función de coordinar y controlar el cumplimiento de la Ley 1581 de 2012, las quejas, solicitudes o reclamos que los titulares formulen.

- **Persona identificable:** Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona natural no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

- **Reclamo:** Solicitud del titular del dato o de las personas autorizadas por éste o por la Ley para corregir, actualizar, o suprimir sus datos personales o para revocar la autorización en los casos establecidos en la Ley.

[8] Numeral 3, artículo 2.2.2.25.1.3, Decreto 1074 de 2015.
[9] Literal d), artículo 3, Ley 1581 de 2012.
[10] Literal b), artículo 6, Ley 1712 de 2014.
[11] Literal c), artículo 6, Ley 1712 de 2014.
[12] Literal c), artículo 6, Ley 1712 de 2014.

- **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los mismos[13].

- **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento[14].

- **Tratamiento:** Se refiere a cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión[15].

- **Transferencia:** Envío de datos personales que realiza el responsable o Encargado desde Colombia a un responsable que se encuentra dentro (transferencia nacional) o fuera del país (transferencia internacional)[16].

- **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro (transmisión nacional) o fuera de Colombia (transmisión internacional) que tiene por objeto la realización de un tratamiento por el Encargado por cuenta del responsable[17].

5. PRINCIPIOS QUE ORIENTAN EL TRATAMIENTO DE LA INFORMACIÓN

En el desarrollo, interpretación y aplicación del Tratamiento de Datos Personales por parte del Municipio de Bucaramanga, se aplicarán, de manera armónica e integral, los siguientes principios de conformidad con lo dispuesto en el artículo 4º de la Ley Estatutaria 1581 de 2012:

a) **Principio de legalidad en materia de Tratamiento de datos:** El Tratamiento de Datos Personales por parte del Municipio de Bucaramanga es una actividad reglada que debe sujetarse a lo establecido en la presente política y en la Constitución, la ley y las decisiones judiciales adoptadas por el Estado Colombiano.

b) **Principio de finalidad:** El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

[13] Literal e), artículo 3, Ley 1581 de 2012.
[14] Literal f), artículo 3, Ley 1581 de 2012.
[15] Literal g), artículo 3, Ley 1581 de 2012.
[16] Numeral 4, artículo 2.2.2.25.1.3, Decreto 1074 de 2015
[17] Numeral 5, artículo 2.2.2.25.1.3, Decreto 1074 de 2015

c) **Principio de libertad:** El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

d) **Principio de veracidad o calidad:** La información sujeta a Tratamiento del Municipio de Bucaramanga debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

e) **Principio de transparencia:** En el Tratamiento debe garantizarse el derecho del Titular a obtener del Municipio de Bucaramanga, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le concierne.

f) **Principio de acceso y circulación restringida:** El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de ley y la Constitución.

   En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la ley; Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;

g) **Principio de seguridad:** La información sujeta a Tratamiento por el Municipio de Bucaramanga, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

h) **Principio de confidencialidad:** Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

6. DEBERES DEL MUNICIPIO DE BUCARAMANGA COMO RESPONSABLE DEL TRATAMIENTO

El Municipio de Bucaramanga, en cumplimiento a los principios y lineamientos legales para el tratamiento de datos personales, informa a los titulares y terceros interesados que durante el tratamiento de datos personales se dará cumplimiento a los deberes reglamentados en el Artículo 17 de la Ley 1581 de 2012.
Cuando no sea posible poner a disposición del titular la Política de Tratamiento de la Información, el Municipio de Bucaramanga informará por medio de un Aviso de Privacidad, sobre la existencia de tales políticas.

7. DERECHOS DE LOS TITULARES DE LA INFORMACIÓN.

De conformidad con lo establecido en el artículo 8 de la Ley 1581 de 2012 y el decreto 1074 de 2015, el titular de los datos personales tiene los siguientes derechos frente a el Municipio de Bucaramanga.
a) Conocer, actualizar y rectificar sus datos personales frente al Municipio de Bucaramanga en su condición de responsable del tratamiento.
b) Solicitar prueba de la autorización otorgada al Municipio de Bucaramanga, en su condición de responsable del Tratamiento.
c) Ser informado por el Municipio de Bucaramanga, previa solicitud, respecto del uso que les ha dado a sus datos personales.
d) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.
e) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.
Conforme al último literal, debe atenderse a lo establecido en el artículo 2.2.2.25.4.2 del Decreto 1074 de 2015, el cual determina:

> *(…) El titular podrá consultar de forma gratuita sus datos personales: (i) al menos una vez cada mes calendario, y (ii) cada vez que existan modificaciones sustanciales de las Políticas de Tratamiento de la información que motiven nuevas consultas. Para consultas cuya periodicidad sea mayor a una por cada mes calendario, el responsable sólo podrá cobrar al titular los gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, el responsable deberá demostrar a la Superintendencia de Industria y Comercio, cuando esta así lo requiera, el soporte de dichos gastos.*

En ningún caso el titular de los datos podrá revocar la autorización y solicitar la supresión de los datos, cuando exista un deber legal o contractual que le imponga la obligación de permanecer en la base de datos.

8. TITULARES DE LA INFORMACIÓN PERSONAL

La operación diaria del Municipio de Bucaramanga requiere conocer y tratar datos personales. Los titulares sobre los cuales se trata dicha información son:

- Contratistas
- Asistentes de eventos
- Trabajadores de libre nombramiento y remoción
- Trabajadores de carrera administrativa
- Trabajadores en provisionalidad
- Trabajadores oficiales
- Aprendices Sena
- Docentes de instituciones educativas oficiales del municipio
- Administrativos de instituciones educativas oficiales del municipio
- Proveedores
- Peticionarios
- Visitantes
- Usuarios
- Sujetos procesales

9. FINALIDADES DEL TRATAMIENTO DE DATOS

Las finalidades para las cuales se realizará el tratamiento de sus datos personales, será el siguiente:

- Permitir el ingreso, registro, control y trazabilidad de las solicitudes, quejas y reclamos presentadas a el Municipio de Bucaramanga
- Adelantar acciones de seguimiento, supervisión y control a los procesos contractuales mediante la utilización de las herramientas de gerencia pública, con el fin de garantizar la ejecución de los proyectos y la apropiada ejecución del presupuesto asignado para cada uno de ellos.
- Efectuar acciones de vigilancia y control de ingreso de visitantes mediante captura fotográfica al ingreso de la entidad.
- Dirigir la formulación de planes, programas y proyectos para establecer la política económica y financiera de la entidad, controlando su ejecución.
- Desarrollar planes, programas y proyectos de administración, formación y bienestar del talento humano, para promover el desarrollo integral de los servidores del Municipio de Bucaramanga.
- Dirigir la elaboración e implementación de planes, programas y proyectos que contribuyan a la igualdad de derechos y oportunidades entre los diferentes grupos poblacionales y a la disminución de prácticas

discriminatorias que atenten contra el desarrollo política, social, económico y cultural de los grupos poblacionales y la familia.

- Gestionar planes, programas y proyectos relacionados con el Sistema de Gestión de Seguridad y Salud en el Trabajo, según las normas y procedimientos que apliquen.
- Gestionar planes y programas relacionados con programas sociales y comunitarios, desarrollando las políticas que rigen el sector, conforme a la planeación institucional.
- Desarrollar el objeto y misión de la entidad a través de los diversos programas que para tal fin se establezcan.

De igual manera, se entenderá aceptada cualquier otra información adicional suministrada por los titulares de la información, teniendo en cuenta los principios rectores para el tratamiento de los datos personales, establecidos por la ley, los cuales, podrán ser utilizados por el Municipio de Bucaramanga como responsable del tratamiento de los datos, para el desarrollo de las funciones propias de la entidad.
Sin perjuicio de las disposiciones establecidas por el ordenamiento legal, el Municipio de Bucaramanga conforme a lo dispuesto en el artículo 10 de la ley 1581 de 2012 podrá realizar el tratamiento de datos personales sin requerir de la autorización expresa del titular:

> *Casos en que no es necesaria la autorización: La autorización del Titular no será necesaria cuando se trate de:*
> *a). Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.*
> *b). Datos de naturaleza pública;*
> *c). Casos de urgencia médica o sanitaria;*
> *d). Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;*
> *e). Datos relacionados con el Registro Civil de las Personas*
> *Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley.*

10. TRATAMIENTO DE DATOS SENSIBLES

En términos generales se prohíbe el tratamiento de datos sensibles, exceptuando los casos cuando:

a) El titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
b) El tratamiento sea necesario para salvaguardar el interés vital del titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
c) El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del titular.
d) El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
e) El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

11. TRATAMIENTO DE DATOS DE NIÑOS, NIÑAS Y ADOLESCENTES

De acuerdo con lo establecido en el artículo 12 de la Ley Estatutaria 1581 de 2012, el tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública y que cumpla con los siguientes parámetros y requisitos:

a) Que responda y respete el interés superior de los niños, niñas y adolescentes.
b) Que se asegure el respeto de sus derechos fundamentales.

Todo responsable y encargado involucrado en el Tratamiento de los Datos Personales de Niños, Niñas y Adolescentes, deberá velar por el uso adecuado de los mismos. Para este fin deberán aplicarse los principios y obligaciones establecidos en la Ley 1581 de 2012 y el Decreto 1074 de 2015.

12. MEDIOS Y ACCIONES PARA EL EJERCICIO DE LOS DERECHOS

El Municipio de Bucaramanga cumpliendo con lo reglamentado por la Ley 1581 de 2012 pone en conocimiento el procedimiento para realizar las consultas y reclamos a los usuarios de la siguiente manera:

A) CONSULTAS:

Los titulares, sus causahabientes o representantes podrán consultar la información personal del titular que repose en cualquier base de datos, por lo que el Municipio de Bucaramanga como responsable del tratamiento,

suministrará a éstos, toda la información contenida en el registro individual o que esté vinculada con la identificación del titular.

El Municipio de Bucaramanga garantiza los medios de comunicación electrónica para la formulación de consultas, los cuales serán los mismos utilizados para la recepción y atención de peticiones, quejas y reclamos administrado por los funcionarios de la Entidad dispuestos para la atención de las solicitudes externas.

La consulta será atendida en un término máximo de diez (10) días hábiles, contados a partir de la fecha de recibo de la misma.

De cumplirse el término sin que sea posible atender la consulta, el Municipio de Bucaramanga como responsable del tratamiento de los datos, informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual no podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término. A continuación, se relaciona el diagrama correspondiente:

B) <u>RECLAMOS:</u>

Los reclamos serán atendidos en un término máximo de quince (15) días hábiles contados a partir del día siguiente a la fecha de recibo del mismo. El Municipio de Bucaramanga podrá prorrogar este término en casos especiales dando aviso al interesado. Este nuevo plazo no podrá superar los ocho (8) días hábiles siguientes. A continuación, se relaciona el diagrama correspondiente:

C) CANALES DE ATENCIÓN

El Municipio de Bucaramanga pone a disposición de los ciudadanos los siguientes canales de atención para dar respuesta a las consultas y reclamos presentadas:

Punto de atención personal	Centro de atención municipal especializado -CAME Carrera 11# 34-52 Bucaramanga, Alcaldía de Bucaramanga - Primer piso, Fase II
Correo electrónico	contactenos@bucaramanga.gov.co
Sitio web	www.bucaramanga.gov.co

13. PERSONA O GRUPO RESPONSABLE DE LA ATENCIÓN DE PETICIONES, CONSULTAS, RECLAMOS Y DENUNCIAS

El Área encargada de atender las Quejas, Reclamos, Consultas y Denuncias sobre el tratamiento de datos personales es Centro de Atención Municipal Especializado -CAME en Bucaramanga en el horario de 7:30 a.m. a 12:00 p.m. y 1:00 pm a 5:00 pm.

14. CAPTURA DE IMÁGENES POR CÁMARAS DE VIDEOVIGILANCIA

El Municipio de Bucaramanga podrá utilizar diversos medios de video vigilancia en diferentes sitios internos y externos de la entidad. Por ese motivo, se informa la existencia de estos mecanismos mediante la difusión en sitios visibles de anuncios de video vigilancia que contendrán como mínimo la información sobre el responsable del tratamiento y sus datos de contacto, se indicará el tratamiento que se dará a los datos y la finalidad del mismo, se incluirán los derechos de los titulares, y finalmente se indicara donde esta publicada la política de tratamiento de la información, dichos anuncios serán ubicados de manera estratégica para su fácil identificación. El sistema de video vigilancia no inspecciona áreas en la que la intimidad del titular prime.

El sistema es utilizado para velar por la seguridad de las instalaciones y las personas. Esta información puede ser empleada como prueba en cualquier tipo de proceso ante autoridades administrativas o judiciales con sujeción y cumplimiento de las normas aplicables.

15. VIGENCIA DE LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

Los lineamientos y directrices contenidos en la presente política tendrán vigencia a partir de su aprobación y promulgación y deja sin efectos cualquier otra Política de Tratamiento de Datos Personales adoptada previamente por el Municipio de Bucaramanga.

16. VIGENCIA DE LA BASE DE DATOS

Las bases de datos que almacene información de titulares que posean relaciones contractuales o deban permanecer por virtud de Ley, se mantendrán vigentes hasta que finalice la necesidad del tratamiento. Lo anterior sin perjuicio del ejercicio de los derechos de supresión que le asisten al Titular.

17. CAMBIOS Y MODIFICACIONES

Los cambios y modificaciones de orden sustancial que se incorporen en la presente política con posterioridad a su entrada en vigor serán comunicados al titular con diez (10) días de anticipación a la implementación de las variaciones. La notificación sobre las modificaciones que serán efectuadas podrá remitirse por los medios de comunicación idónea, tales como: correos electrónicos o en las instalaciones físicas del Municipio de Bucaramanga.

ANEXO 3

Mapa Documental

<table>
<tr><th colspan="7">Marco de seguridad y privacidad de la información del municipio de Bucaramanga (MSPI)</th></tr>
<tr><th colspan="4">Política de seguridad de la información</th><th colspan="3">Política de privacidad y protección de datos personales</th></tr>
<tr><th colspan="2">Propiedad de la información/Gestión de activos/Responsabilidades y contraseñas/Administración de redes y equipos/uso de software y sistemas de información/Correo electrónico/uso de internet.</th><th>Seguridad física y control de acceso</th><th>Gestión de riesgos, conocimiento, incidentes y continuidad del negocio.</th><th>Registro de base de datos.</th><th>Reclamos por parte de los titulares.</th><th>Reporte de incidentes de seguridad en base de datos.</th></tr>
<tr><td>Formato de clasificación de activos (Hardware, software, servicios y Base de datos)</td><td rowspan="2">Guía para la gestión de activos de información</td><td rowspan="6">Formato: registro de equipos y dispositivos externos conectados a la red interna.</td><td rowspan="3">Guía para la continuidad, contingencia y gestión incidentes tecnológicos del municipio de Bucaramanga</td><td>Formato de registro de base de datos y responsables</td><td>Formato: registro de reclamos de titulares de información, actualización, rectificación o supresión de datos</td><td>Formato: gestión de incidentes de seguridad informática</td></tr>
<tr><td>Formato de clasificación de activos: Documental.</td><td colspan="3">Manual para el manejo de bases de datos bajo la ley de protección de datos personales.</td></tr>
<tr><td>Formato: Solicitud de acceso a los activos de información.</td><td rowspan="4">Instructivo de uso de activos de información.</td><td>Formato: gestión de incidentes de seguridad informática.</td><td colspan="3" rowspan="2">Política de privacidad y condiciones de uso de sitio web(www.BUcaramanga.gov.co)</td></tr>
<tr><td>Formato: compromiso de confidencialidad y no divulgación de información.</td><td>Formato: Bitácora de incidentes de servicios de TI.</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Formato de copias de seguridad.</td><td colspan="3" rowspan="2">Guía para el uso de aviso de privacidad y protección de datos del municipio de Bucaramanga.</td></tr>
<tr><td>Formatos de chequeo, monitoreo y control.</td></tr>
</table>

ANEXO 4

Política Seguridad de la información

TABLA DE CONTENIDO

1. OBJETIVO, ALCANCE Y USUARIOS 2

2. DOCUMENTOS DE REFERENCIA 2

3. TERMINOLOGÍA BÁSICA SOBRE SEGURIDAD DE LA INFORMACIÓN 2

4. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 3

4.1. OBJETIVOS Y MEDICIÓN **3**
4.2. REQUISITOS PARA LA SEGURIDAD DE LA INFORMACIÓN 4
4.3. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN 4
4.4. RESPONSABILIDADES 4
4.5. COMUNICACIÓN DE LA POLÍTICA 5
4.6. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN 5

5. APOYO PARA LA IMPLEMENTACIÓN DEL SGSI 6

6. VALIDEZ Y GESTIÓN DE DOCUMENTOS 6

7. HISTORIAL DE CAMBIOS 6

1. OBJETIVO, ALCANCE Y USUARIOS

La ALCALDÍA MUNICIPAL DE BUCARAMANGA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para la ALCALDÍA MUNICIPAL DE BUCARAMANGA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, capítulos 5.2 y 5.3
- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Disponible en https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Versi%C3%B3n+5+-+Diciembre+de+2020.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=1611247032238&download=true
- Modelo de Seguridad y Privacidad de la Información. Disponible en https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

3. TERMINOLOGÍA BÁSICA SOBRE SEGURIDAD DE LA INFORMACIÓN

- **Confidencialidad**: característica de la información por la cual solo está disponible para personas o sistemas autorizados.
- **Integridad**: característica de la información por la cual solo que es modificada por personas o sistemas autorizados y de una forma permitida.
- **Disponibilidad**: característica de la información por la cual solo pueden acceder las personas autorizadas cuando sea necesario.
- **Seguridad de la información**: es la preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Sistema de gestión de seguridad de la información**: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

4. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.1. Objetivos y medición

Esta política aplica a la ALCALDÍA MUNICIPAL DE BUCARAMANGA según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

a. Minimizar el riesgo en las funciones más importantes de la entidad.
b. Cumplir con los principios de seguridad de la información.
c. Cumplir con los principios de la función administrativa.
d. Mantener la confianza de sus clientes, socios y empleados.
e. Apoyar la innovación tecnológica.
f. Proteger los activos tecnológicos.
g. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
h. Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la ALCALDÍA MUNICIPAL DE BUCARAMANGA.
i. Garantizar la continuidad del negocio frente a incidentes.
j. La ALCALDÍA MUNICIPAL DE BUCARAMANGA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

La ALCALDÍA MUNICIPAL DE BUCARAMANGA medirá el cumplimiento de todos los objetivos. El Líder de Seguridad y Privacidad de la Información es el responsable de definir el método para medir el cumplimiento de los objetivos; la medición se realizará al menos al menos una vez al año y el Líder de Seguridad y Privacidad de la Información analizará y evaluará los resultados y los reportará al Líder de Planeación como material para la revisión por la Dirección. El Líder de Seguridad y Privacidad de la Información es responsable de registrar los detalles sobre los métodos de medición, periodicidades y resultados en el Informe de Medición.

4.2. Requisitos para la seguridad de la información

Esta Política, y todo el SGSI, deben cumplir los requisitos legales y normativos importantes para la organización en el ámbito de la Seguridad y Privacidad de la información, como también con las obligaciones contractuales.

En la Lista de obligaciones legales[1], normativas y contractuales se detalla una lista de requisitos contractuales y legales.

4.3. Controles de seguridad de la información

El proceso de elegir los controles (protección) está definido en la metodología de evaluación y tratamiento de riesgos.

Los controles seleccionados y su estado de implementación se detallan en la Declaración de aplicabilidad.

4.4. Responsabilidades

Las responsabilidades para el SGSI son las siguientes:

- El Líder de Seguridad y Privacidad de la Información es el responsable de garantizar que el SGSI sea implementado y mantenido de acuerdo con esta Política y de garantizar que todos los recursos necesarios estén disponibles.
- El Líder de Seguridad y Privacidad de la Información es el responsable de la coordinación operativa del SGSI, como también de informar su desempeño.
- El alcalde Municipal o a quien designe, debe revisar el SGSI al menos una vez por año o cada vez que se produzca una modificación significativa; y debe elaborar actas de dichas reuniones. El objetivo de las verificaciones por parte de la dirección es establecer la conveniencia, adecuación y eficacia del SGSI.
- El Líder de Seguridad y Privacidad de la Información implementará programas de formación y concienciación de empleados sobre seguridad de la información.
- La protección de la integridad, disponibilidad y confidencialidad de los activos es responsabilidad del propietario de cada activo.
- Todos los incidentes o debilidades de seguridad deben ser informados al Líder de Seguridad y Privacidad de la Información.
- El Líder de Seguridad y Privacidad de la Información definirá qué información relacionada con la seguridad y privacidad de la información será comunicada a qué parte interesada (tanto interna como externa), por quién y cuándo.

[1] Ley 1581 de 2012 , Política de Gobierno Digital

- El Líder de Seguridad y Privacidad de la Información es el responsable de adoptar e implementar el Plan de formación y concienciación, que corresponde a todos los funcionarios que participan en la gestión de la seguridad de la información.

4.5. Comunicación de la Política

El Líder de Seguridad y Privacidad de la Información debe asegurarse de que todos los funcionarios de la ALCALDÍA MUNICIPAL DE BUCARAMANGA, como también los participantes externos correspondientes, estén familiarizados con esta Política.

4.6. Principios de Seguridad de la Información

A continuación, se establecen once principios de seguridad que soportan el SGSI de La ALCALDÍA MUNICIPAL DE BUCARAMANGA:

i. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
ii. La ALCALDÍA MUNICIPAL DE BUCARAMANGA protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
iii. La ALCALDÍA MUNICIPAL DE BUCARAMANGA protegerá la información creada, procesada, transmitida o resguardada por sus procesos internos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
iv. La ALCALDÍA MUNICIPAL DE BUCARAMANGA protegerá su información de las amenazas originadas por parte de orígenes internos o externos.
v. La ALCALDÍA MUNICIPAL DE BUCARAMANGA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
vi. La ALCALDÍA MUNICIPAL DE BUCARAMANGA controlará la operación de sus procesos internos garantizando la seguridad de los recursos tecnológicos y las redes de datos.
vii. La ALCALDÍA MUNICIPAL DE BUCARAMANGA implementará control de acceso a la información, sistemas y recursos de red.
viii. La ALCALDÍA MUNICIPAL DE BUCARAMANGA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
ix. La ALCALDÍA MUNICIPAL DE BUCARAMANGA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

x. La ALCALDÍA MUNICIPAL DE BUCARAMANGA garantizará la disponibilidad de sus procesos internos y la continuidad de su operación basada en el impacto que pueden generar los eventos.
xi. La ALCALDÍA MUNICIPAL DE BUCARAMANGA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

5. APOYO PARA LA IMPLEMENTACIÓN DEL SGSI

A través del presente, el ALCALDE MUNICIPAL DE BUCARAMANGA declara que en la implementación y mejora continua del SGSI se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta Política, como también para cumplir con todos los requisitos identificados.

6. VALIDEZ Y GESTIÓN DE DOCUMENTOS

Este documento es válido hasta el 31 de diciembre de 2022

El propietario de este documento es el Líder de Seguridad y Privacidad de la Información, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de funcionarios y participantes externos que cumplen una función en el SGSI pero que no están familiarizados con el presente documento.
- No cumplimiento del SGSI con las leyes y normas, las obligaciones contractuales y con los demás documentos internos de la entidad.
- Ineficacia de la implementación y mantenimiento del SGSI.
- Responsabilidades ambiguas para la implementación del SGSI.

7. HISTORIAL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA
0.0	Se incluye en el SIGC la política de seguridad y privacidad de la información de la Administración Municipal, la cual fue adoptada y adecuada por la Resolución 0489 de 2017.	Mayo-21-2019

1.0	Actualización de la política de seguridad y privacidad de la información por requerimiento del proceso Gestión de las TIC. Adicionalmente es aprobado por el comité de MIPG de la Entidad.	Diciembre-06-2021