PLAN PARA LA IMPLEMENTACIÓN DE LA ESTRATEGIA GOBIERNO EN LÍNEA:

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Lógica Ética & Estética
Gobierno de los Ciudadanos

Municipio de Bucaramanga

Elaboración:

Sergio Oswaldo Cajías Lizcano
Asesor TIC de Bucaramanga

Eder Fernando Bolaño Rocha
Profesional Contratista-Seguridad de la Información

Grupo Asesor:

Alvaro Castilla
Profesional Contratista-Gobierno en Línea

Elkin Albarracín
Profesional Contratista-Sistemas de Información

Hernando Gelvez Díaz
Profesional Contratista-Infraestructura de hardware

Nestor Santos
Profesional Contratista-Planeación estratégica

Revisión:

Nelson Javier Cáceres
Profesional Contratista- Puntos Vive Digital

Sofía Sepulveda
Profesional contratista- Abogada

Uriel Carreño
Profesional Contratista- Calidad

Bernardo Espitia
Técnico Operativo-Centro de Datos

DERECHOS DE AUTOR

El documento ha sido elaborado para el MUNICIPIO DE BUCARAMANGA (se entiende como Municipio de Bucaramanga a la administración central de la ciudad) para la implementación del componente de seguridad y privacidad de la información.

Contiene información de la apropiación de la estrategia de gobierno en Línea, puede ser reproducido siempre y cuando se cite la fuente.

INTRODUCCIÓN

El siguiente documento establece la carta de navegación a seguir para el cumplimiento de la estrategia de Gobierno en Línea para implementación de un sistema de Gestión de seguridad y privacidad de la información (SGSI) basado en las normas internacionales ISO 27000:2013 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 decreto 2573 de 2014 y el decreto 1078 de 2015 establece la estrategia de Gobierno en línea propone para el año 2018 tener implementado en las instituciones territoriales como alcaldía y gobernaciones tener una meta de 100% de implementación de políticas y procedimientos que contribuyan a la gestión de la información pública de manera que se proteja el bien de los servicios ofrecidos por el MUNICIPIO DE BUCARAMANGA. Es importante tener en cuenta la participación del comité de gobierno en Línea, así como también la integración de los sistemas de gestión existentes para lograr una armonización e integración a dichos sistemas.

CONTENIDO

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 a 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 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.

[1] Tomado de: https://cybermap.kaspersky.com/
[2] Tomado de: https://www.sivirtual.gov.co/
http://www.suit.gov.co/

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
- **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.

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

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:

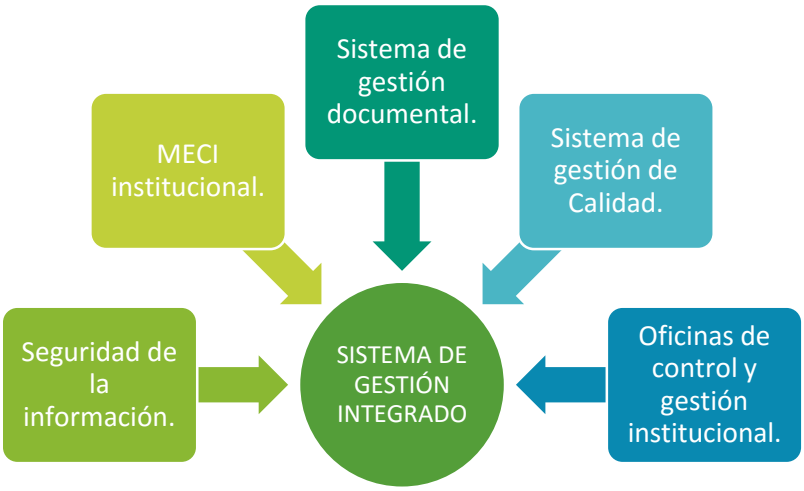

Figura 2. Sistema de gestión integrado
Fuente: Autor

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.

Figura 3. Pantallazo informativo propagado en el mes de marzo de 2016
Fuente: Oficina TIC

- **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.

Figura 4. Ambiente virtual de ARCANA.
Fuente: Autor

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.

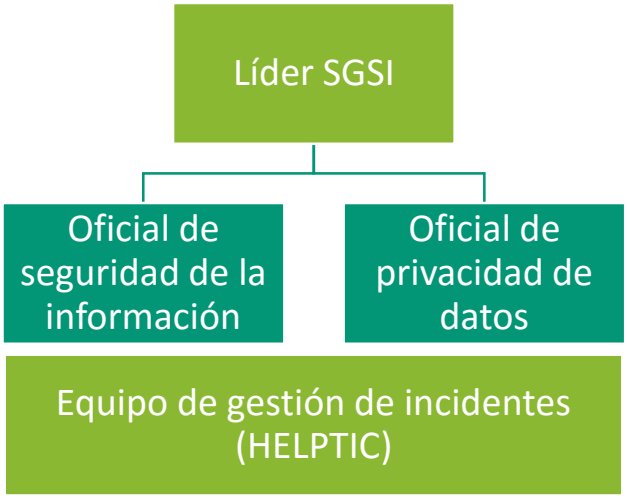

Figura 5. Roles y responsabilidades del SGSI
Fuente: Autor

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)**: La gestión de incidentes debe articularse con la mesa de servicios con el fin de brindar el soporte, garantizar la disponibilidad de los servicios y responder ante cualquier incidencia para reestablecer los servicios del área de TI. Y en casos graves de delitos, mantener la evidencia y articular con las debidas autoridades de reacción, así como la gestión interna en el Municipio.

  - ✓ 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.

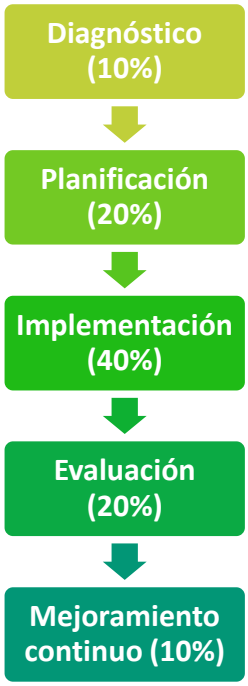

Figura 7. Fases de implementación
Fuente: Manual GEL 3.1

Seguridad y Privacidad de la Información	**30%**	**Definición de marco de seguridad y privacidad de la Entidad:** La Entidad define el estado actual de su nivel de seguridad y privacidad y elabora su plan.	**10%**	**Diagnóstico de Seguridad y Privacidad:** Busca que la entidad determine el nivel de seguridad y privacidad en el cual se encuentra.	**10%**	La Entidad cuenta con un diagnóstico de seguridad y privacidad.	Modelo de Seguridad y Privacidad de la Información para GEL NTC-ISO-IEC 27001:2013 LI.ES.01 LI.ES.02 LI.GO.01
			20%	**Propósito de Seguridad y Privacidad de la Información:** Busca que la entidad organice las acciones a tomar, verificando que estén alineadas a la misión y visión de la entidad y construya de manera objetiva.	**20%**	La Entidad cuenta con un plan de seguridad y privacidad de información.	Modelo de Seguridad y Privacidad de la Información para GEL NTC-ISO-IEC 27001:2013 LI.ES.02 LI.ES.06 LI.ES.08 LI.GO.01 LI.GO.04 LI.GO.09
	40%	**Implementación del plan de seguridad y privacidad:** La entidad desarrolla las acciones definidas en el plan de seguridad y privacidad de información.	**40%**	**Gestión de Riesgos de seguridad y privacidad de la información:** Busca la identificación, valoración, tratamiento y mitigación de los riesgos.	**20%**	La entidad identifica y analiza los riesgos.	Modelo de Seguridad y Privacidad de la Información para GEL NTC-ISO-IEC 27001:2013 Cobit 5 LI.GO.04 LI.ST.14
					20%	La entidad cuenta con un plan de tratamiento de riesgos, clasifica y gestiona controles	Modelo de Seguridad y Privacidad de la Información para GEL NTC-ISO-IEC 27001:2013 LI.INF.15 LI.SIS.22
	30%	**Monitoreo y Mejoramiento continuo:** La Entidad desarrolla actividades para la evaluación y mejora de los niveles de seguridad y privacidad de la información.	**30%**	**Evaluación del desempeño** Busca hacer las mediciones necesarias para calificar la operación y efectividad de los controles, estableciendo niveles de cumplimiento y de protección de los principios de seguridad y privacidad de la información	**20%**	La entidad cuenta con actividades para el Seguimiento, medición, análisis y evaluación del desempeño de la seguridad y privacidad a efecto de generar los ajustes o cambios pertinentes y oportunos	Modelo de Seguridad y Privacidad de la Información para GEL NTC-ISO-IEC 27001:2013 LI.ES.13 LI.GO.03
					10%	La entidad revisa e implementa acciones de mejora continua que garanticen el cumplimiento del plan de seguridad y privacidad de la Información.	Modelo de Seguridad y Privacidad de la Información para GEL NTC-ISO-IEC 27001:2013 LI.GO.13

2. FASE DIAGNÓSTICO

Conocer el estado actual de la entidad es de vital importancia para establecer la línea base del componente de la seguridad y privacidad de la información la gestión realizada en la labor de empalme a finales de 2015 evidencia un cumplimiento del 15% donde el nivel aceptable para el decreto 1078 de 2015 es de un 35% para ese año.

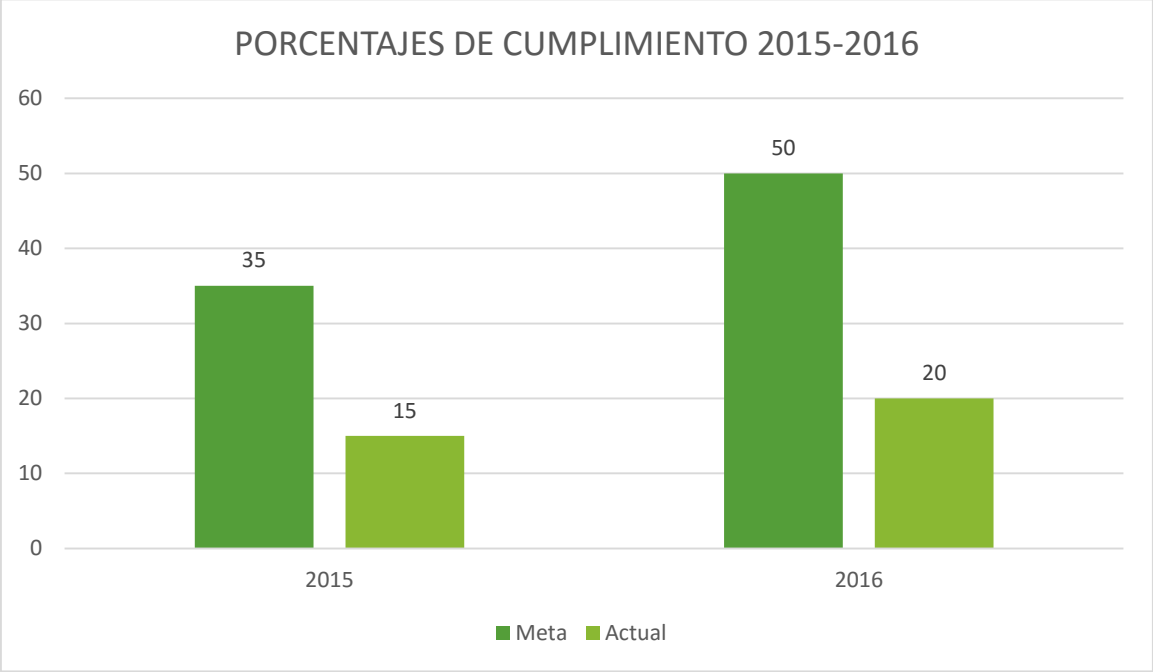

Figura 8. Cumplimiento del componente de seguridad y privacidad
Fuente: Oficina TIC

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.

Los entregables de esta fase serán los siguientes:

FASE	DIAGNÓSTICO	
CANTIDAD DE ENTREGABLES		**3**
FECHAS	1	
	2	
	3	

META	ENTREGABLE
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad, teniendo en cuenta la infraestructura de red de comunicaciones (IPv4/IPv6).	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección.
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.	Documento con el resultado de la herramienta de la encuesta, revisado, aprobado y aceptado por la alta dirección
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.

2.1. MAPA DE ACTIVIDADES FASE DIAGNÓSTICO

Meta	Recursos Humanos		Costos		Actividades	Tiempo	Entregables
	Interno	Externo	Interno	Externo			
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).					Levantamiento de mapa de red de infraestructura tecnológica.		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.
					Inventario de contraseñas gestionadas y aseguradas.		
					Diagnóstico de auditoría según modelo GEL.		
					Revisión de políticas existentes de seguridad y privacidad.		
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.					Auditoría externa según normas ISO27000 externa.		Documento con el resultado de la herramienta de la encuesta, revisado, aprobado y aceptado por la alta dirección.
Realizar pruebas que permitan a la Entidad medir la efectividad de los controles existentes.					Levantamiento de Controles existentes.		Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la dirección.
					Evaluación de controles aplicados		

3. FASE DE PLANIFICACIÓN

FASE	PLANIFICACIÓN	
CANTIDAD DE ENTREGABLES		8
FECHAS	1	
	2	
	3	
	4	
	5	
	6	
	7	
	8	

META	ENTREGABLE
Objetivos, alcance y límites del MSPI.	Documento con el alcance y límites de la seguridad de la información, debidamente aprobado y socializado al interior de la Entidad, por la alta dirección
Políticas de seguridad y privacidad de la información (Ver anexo 1 y 2) *	Documento con las políticas de seguridad y privacidad de la información, debidamente aprobadas y socializadas al interior de la Entidad, por la alta Dirección.
Procedimientos de control documental del MSPI (Ver anexo 3) *	Formatos de procesos y procedimientos, debidamente definidos, establecidos y aprobados por el comité que integre los sistemas de gestión institucional.
Asignación de recurso humano, comunicación de roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (ó el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección.

Inventario de activos de información.	Documento de inventario de activo de información, revisado y aprobado por la alta Dirección
Acciones para tratar riesgos y oportunidades de seguridad de la información. Identificación y valoración de riesgos de (Metodología, Reportes).o Tratamiento de riesgos (Selección de controles).	Documento con el informe de análisis de riesgos, matriz de riesgos, plan de tratamiento de riesgos y declaración de aplicabilidad, revisado y aprobado por la alta Dirección
Toma de conciencia.	Documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección
Plan y estrategia de transición de IPv4 a IPv6.	Documento con el plan y estrategia de transición de IPv4 a IPv6, revisado y aprobado por la alta Dirección.

3.1. MAPA DE ACTIVIDADES FASE DE PLANIFICACIÓN

Meta	Recursos Humanos		Costos		Actividades	Tiempo	Entregables
	Interno	Externo	Interno	Externo			
Objetivos, alcance y límites del MSPI.					Desarrollo de un marco de seguridad y privacidad de la información para el municipio		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
					Revisión y ajustes del MSPI		
					Aprobación del MSPI		
					Publicación y socialización		
Políticas de seguridad y privacidad de la información					Desarrollo las políticas de seguridad y privacidad de la información para el municipio		Documento con las políticas de seguridad y privacidad de la información, debidamente aprobadas y socializadas al interior de la Entidad, por la alta Dirección.
					Revisión y ajustes de las políticas de SI y PI		
					Aprobación de las políticas SI y PI		
Procedimientos de control documental del MSPI					Actualización y revisión del proceso de gestión, implementación y soporte de las TIC para articular con el MSPI		Formatos de procesos y procedimientos, debidamente definidos, establecidos y aprobados por el comité que integre los sistemas de gestión institucional.
					Generación de formatos, guías, manuales, Instructivos asociados al SGC		
					Publicación y aprobación en el SGC		
Asignación de recurso humano, comunicación de roles y responsabilidades de seguridad y privacidad de la información.					Verificar existencia de personal institucional para la asignación de roles.		Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (ó el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección.
Inventario de activos de información.					Revisión de inventario de activos de información anteriores.		Documento de inventario de activo de información, revisado y aprobado por la alta Dirección
					Verificación y actualización de activos de información.		
					Asociación de riesgos de CID y custodios.		
					Aprobación, publicación y socialización.		

					Diseño de sistema de gestión de activos de información del municipio.		
					Selección de activos de información con riesgo en privacidad de datos personales.		
					Caracterización de información pública para datos abiertos		
Acciones para tratar riesgos y oportunidades de seguridad de la información. Identificación y valoración de riesgos de (Metodología, Reportes). O Tratamiento de riesgos (Selección de controles).					Análisis de metodología de riesgo aplicables al Municipio		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.
					Diseño de matriz de riesgo de seguridad y privacidad de activos de información.		
					Elaboración de aplicabilidad de norma ISO27000 (SoA)		
					Plan de tratamiento de riesgos.		
Toma de conciencia.					Plan de sensibilización de tendencias TI y alertas de virus entre otras.		Documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección
					Plan anual de capacitaciones en seguridad y privacidad de la información		
Plan y estrategia de transición de IPv4 a IPv6.					Estudio de aplicabilidad de Ipv6 para un segmento de la red inalámbrica.		Documento con el plan y estrategia de transición de IPv4 a IPv6, revisado y aprobado por la alta Dirección.

4. FASE DE IMPLEMENTACIÓN

FASE	IMPLEMENTACIÓN	
CANTIDAD DE ENTREGABLES		4
FECHAS	1	
	2	
	3	
	4	

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

4.1. MAPA DE ACTIVIDADES FASE DE IMPLEMENTACIÓN

Meta	Recursos Humanos		Costos		Actividades	Tiempo	Entregables
	Interno	Externo	Interno	Externo			
Planificación y control operacional.					Documento de procedimientos del SGSI.		Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
					Revisión y aprobación del documento de procedimientos y operaciones.		
					Revisión de la declaración de aplicabilidad.		
					Revisión de documentación asociada al SGC.		
					Diseño e implementación del sistema para la gestión de la seguridad de la información ARCANA		
Implementación de controles.					Aplicación de controles por recursos humanos y áreas segura.		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
					Aplicación de controles de red y servidores		
					Aplicación de controles para evaluación y mejora continua.		
					Aplicación de normatividad legal de protección de datos personales		
					Elaboración de la documentación de controles aplicados.		
					Pruebas de efectividad de controles ejecutados para la seguridad y privacidad.		
					Evaluación y acompañamiento a la implementación del servidor de pruebas del Municipio. (Política de desarrollo seguro)		
Implementación del plan de tratamiento de riesgos					Diagnóstico BIA		Indicadores de gestión del MSPI, revisado y aprobado por la alta Dirección
					Elaboración del Plan de contingencia y continuidad del negocio		
					Elaboración de la guía para la gestión de incidentes de seguridad de la información		
					Elaboración e implementación de indicadores del MSPI		
Implementación del plan y estrategia de transición de IPv4 a IPv6					Aplicación del plan de transición a Ipv6 en un segmento de la red inalámbrica.		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

5. FASE DE EVALUACIÓN

FASE	EVALUACIÓN	
CANTIDAD DE ENTREGABLES		3
FECHAS	1	
	2	
	3	

META	ENTREGABLE
Plan de seguimiento, evaluación y análisis del MSPI.	Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.
Auditoria 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.
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

5.1 MAPA DE ACTIVIDADES FASE DE EVALUACIÓN

Meta	Recursos Humanos		Costos		Actividades	Tiempo	Entregables
	Interno	Externo	Interno	Externo			
Plan de seguimiento, evaluación y análisis del MSPI.					Evaluación de indicadores de gestión del MSPI		Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.
					Análisis de cumplimiento de la norma ISO 27000 (GAP)		
Auditoria Interna					Elaboración del plan de auditoria interna al SGSI		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.
					Revisión de activos de información		
					Revisión de activos de información		
					Revisión de políticas de seguridad de la información		
					Revisión de políticas de privacidad y protección de datos		
					Evaluación de documentación y procedimientos.		
Evaluación del plan de tratamiento de riesgos.					Revisión del plan de riesgos.		Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección
					Revisión de riesgos asignados a activos de información.		

6. FASE MEJORA CONTINUA

FASE	MEJORA CONTINUA	
CANTIDAD DE ENTREGABLES		2
FECHAS	1	
	2	

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

6.1. MAPA DE ACTIVIDADES FASE DE MEJORA CONTINUA

Meta	Recursos Humanos		Costos		Actividades	Tiempo	Entregables
	Interno	Externo	Interno	Externo			
Plan de seguimiento, evaluación y análisis del MSPI.					Evaluación de resultados de fase de evaluación. Revisión del análisis de cumplimiento de la norma ISO 27000 (GAP)		Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección.
Auditoria Interna					Evaluación de hallazgos		Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta Dirección
					Elaboración de plan de mejoramientos del MSPI		
Comunicación de resultados y plan de mejoramiento					Plan de socialización y capacitación de mejoras y resultados		
Revisión y aprobación por la alta Dirección.					Actualización de documentación y correctivos de hallazgos de auditoría interna.		

CONCLUSIONES

La información es lo más importante para cualquier organización por lo tanto es un factor clave para proteger de incidentes relacionados con la seguridad y privacidad de los mismos abarcando los principios de confidencialidad, disponibilidad e integridad.

Para el Municipio por lo tanto es una meta consagrada en el plan de desarrollo “Gobierno de los ciudadanos y ciudadanas” convertirse en una ciudad modelo en la implementación de la estrategia, con este documento se busca tener como ejemplo para otras entidades relacionadas con el municipio para la implementación de este componente que es fundamental alrededor de los negocios digitales y las tecnologías que se implementan en las entidades. Por lo tanto, este documento tendrá la capacidad de ser adaptado de acuerdo a las necesidades y recursos disponibles para cada entidad en el beneficio de todos los actores y el cumplimento de la Estrategia.

7. ANEXOS

Anexo 1

1. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Para el MUNICIPIO DE BUCARAMANGA la información es un activo valioso para la toma de decisiones, la gestión del cambio y el conocimiento; así como la apropiación de la iniciativa de Gobierno en línea. La necesidad de articular los valores de gobierno “Lógica, Ética y Estética” para establecer una política de seguridad de la información que ha de brindar a los usuarios y ciudadanos las herramientas para la defensa de lo público contenido en los servicios y activos de TI en la entidad. Los tres principios enmarcan lo siguiente:

- **LÓGICA**: Representa los servicios tales como correo electrónico, Base de Datos, servicios Web. Los cuales tienen mayor número de usuarios e impacto en los ciudadanos y funcionarios del MUNICIPIO DE BUCARAMANGA, por lo cual es lógico el funcionamiento continuo de los servicios prestados vistos desde la seguridad de la información para la mitigación de riesgos posibles.

- **ÉTICA**: Representa a los usuarios (Control de cuenta de usuario de dominio, acuerdos de confidencialidad y uso de activos de información, protección de datos personales), considerando la necesidad de fortalecer a los usuarios ante los riesgos de la seguridad de la información a través de la formación y capacitación de los mismo.

- **ESTÉTICA**: Se enfoca en la parte visible de los aplicativos y servicios de información esto es, la infraestructura física como servidores, las redes de comunicación y datos, implicando el buen uso y acceso a los mismos. También incluye la necesidad de una implementación basada en la comunicación y educación en seguridad de la información.

La necesidad de mitigación de riesgos alrededor de la información requiere planes de manejo de incidentes y herramientas para respaldar las actividades ejecutadas en el MUNICIPIO DE BUCARAMANGA considerando que las TIC son un proceso de apoyo a toda la entidad. Además de incentivar la cultura de seguridad de la información a los usuarios ante ataques informáticos, virus y robos o pérdidas de información.

Es de vital importancia la gestión del conocimiento y las revisiones de la política que lleven a una mejora continua para lograr un mejor desempeño de las actividades y la articulación de la normatividad colombiana e internacional en protección de datos, delitos informáticos y seguridad de la información además de tendencias tecnológicas para que puedan ser implementadas entorno a la eficacia de las actividades relacionadas, considerando siempre los tres principios de la seguridad de la información: Confidencialidad, disponibilidad e integridad.

2. OBJETIVO

- Establecer una Política de seguridad de la información junto con los procedimientos, mecanismos, controles y herramientas adecuadas que garanticen la integridad, disponibilidad y confidencialidad de los activos de información en el MUNICIPIO DE BUCARAMANGA.

3. ALCANCE

- La Política de Seguridad de la Información aplica para todos los usuarios internos en todos los niveles jerárquicos, usuarios externos o aquellos que de alguna manera manejen información de la Administración del MUNICIPIO DE BUCARAMANGA.

4. DESCRIPCIÓN DE POLÍTICAS

4.1 PROPIEDAD DE LA INFORMACIÓN

El MUNICIPIO DE BUCARAMANGA establece propiedad sobre los activos de información que están relacionados con su actividad. La información es entregada para su uso, operación o custodia a los servidores públicos, contratistas o terceros, de acuerdo a la función específica y necesidades del trabajo a realizar de acuerdo a lo establecido, además sin alterar en ningún momento la propiedad de los mismos.

Por lo tanto, las personas responsables de los procesos que controlan activos de información, lo hacen para su manejo operativo y de conservación sin perjuicio para el MUNICIPIO DE BUCARAMANGA de perder la propiedad de la información.

4.2 GESTIÓN DE ACTIVOS

Los activos de información en el MUNICIPIO DE BUCARAMANGA se gestionarán de manera que:

1. Se encontrarán inventariados
2. Serán asignados a un responsable
3. Se realizará una valoración de riesgos.
4. Protegidos de acuerdo a su riesgo asignado.

4.3 CONTROL DE ACCESO

Es de vital importancia el control de acceso a la información mediante sistemas internos, redes externas o internas y activos de información por lo cual, ha de establecerse, mantenerse y actualizarse medidas de control de acceso soportados por una cultura de

seguridad en la entidad y limitar el acceso de los usuarios hacia los activos de información al mínimo requerido para la realización de su trabajo, de acuerdo con el tratamiento correspondiente al nivel de clasificación de cada activo. Además, deben permitir identificar de manera inequívoca cada usuario y hacer seguimiento de las actividades que éste realiza.

4.4 ADMINISTRACIÓN DE REDES Y EQUIPOS

Los recursos tecnológicos del MUNICIPIO DE BUCARAMANGA, son herramientas de apoyo a las labores y responsabilidades de los funcionarios y/o contratistas. Por ello, su uso está sujeto a las siguientes directrices:

- Los bienes de cómputo se emplearán de manera exclusiva y bajo la completa responsabilidad por el funcionario y/o contratista al cual han sido asignados, y únicamente para el correcto desempeño de las funciones del cargo o de las obligaciones contraídas. Por tanto, no pueden ser utilizados con fines personales o por terceros, no autorizados ante la Oficina asesora de TIC mediante solicitud formal por los Directores, Subdirectores, Jefes de Oficina o Coordinadores del MUNICIPIO DE BUCARAMANGA.
- Sólo está permitido el uso de software licenciado por la Entidad y/o aquel que sin requerir licencia sea expresamente autorizado por la Oficina Asesora de TIC. El software generado por el MUNICIPIO DE BUCARAMANGA, en desarrollo de su misión institucional, debe ser reportados a la Oficina Asesora de TIC, para su administración.
- Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional.
- No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren los elementos tecnológicos, además se debe tener organizado el puesto de trabajo para evitar incidentes con estos recursos.
- No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo la disponibilidad de la información por fallas en el suministro eléctrico a los equipos de cómputo.
- Los únicos autorizados para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, son los designados por la Oficina Asesora de TIC para tal labor.
- La Oficina Asesora de TIC realizará monitoreo sobre los dispositivos de almacenamientos externos, con el fin de prevenir o detectar fuga de información.
- La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, debe ser informada de inmediato a la Oficina Asesora de TIC por el funcionario o contratista a quien se le hubiere asignado.
- La pérdida de información debe ser informada con el detalle de la información extraviada a la Oficina Asesora de TIC.
- La Oficina Asesora de TIC es la única dependencia autorizada para la administración del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales.
- Todo acceso a la red de la Entidad mediante elementos o recursos tecnológicos no institucionales deberá ser informado, autorizado y controlado por la Oficina Asesora de TIC previa autorización de la dirección del MUNICIPIO DE BUCARAMANGA.

- Los equipos deben quedar apagados cada vez que el funcionario y/ o contratista no se encuentre en la oficina durante la noche, esto es, con el fin de proteger la seguridad y distribuir bien los recursos de la Entidad, siempre y cuando no vaya a realizar actividades vía remota.
- Se debe evitar guardar documentos sobre el escritorio de trabajo del sistema operativo optando por un lugar seguro dentro del almacenamiento del equipo.

4.5 USO DE SOFTWARE Y SISTEMAS DE INFORMACIÓN

Todos los funcionarios y/o contratistas del MUNICIPIO DE BUCARAMANGA son responsables de la protección de la información que acceden y/o procesan y de evitar su pérdida, alteración, destrucción y/o uso indebido, para lo cual se dictan los siguientes lineamientos:

- Las credenciales de acceso a la red y/o recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible; los funcionarios y/o contratistas no deben revelar éstas a terceros ni utilizar claves ajenas.
- Todo funcionario y/o contratista es responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente.
- Todo funcionario y/o contratista es responsable de los registros y/o modificaciones de información que se hagan a nombre de su cuenta de usuario, toda vez que la clave de acceso es de carácter personal e intransferible.
- En ausencia del funcionario y/o contratista, el acceso a la estación de trabajo le será inactivada con una solicitud a la Oficina Asesora de TIC, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. La Dirección de Recursos Humanos o quien haga sus veces debe reportar, las vacaciones y cualquier tipo de licencia de los funcionarios y la Dirección de Contratación o quien haga sus veces las suspensiones temporales y/o permanentes de los contratistas; no obstante, el funcionario y/o contratista deberá solicitar a la Oficina Asesora de TIC el bloqueo de su usuario por la ausencia temporal o definitiva.
- Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de un contrato con el MUNICIPIO DE BUCARAMANGA, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente; la información del empleado y/o contratista serán almacenados en un repositorio de los servidores de la Entidad.
- Cuando un funcionario y/ o contratista cesa en sus funciones o culmina la ejecución de un contrato con el MUNICIPIO DE BUCARAMANGA, el supervisor o jefe inmediato es el encargado de la custodia de los recursos de información y de informar a la OFICINA TIC la culminación de permisos para los contratistas.

Solo las aplicaciones aprobadas por la Oficina Asesora de TIC serán instaladas o utilizadas en cada dispositivo destinado al procesamiento de información clasificada o sensible, además de garantizar su debida aprobación de uso y licenciamiento de acuerdo a los permisos y controles asignados a los usuarios.

4.5.1 CORREO ELECTRÓNICO

El servicio de correo electrónico institucional es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios y/o contratistas del MUNICIPIO DE BUCARAMANGA, con los siguientes lineamientos:

- El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la Entidad, por lo tanto, la responsabilidad del contenido es netamente del autor.
- Está prohibido el uso de correos masivos tanto internos como externos, salvo con la autorización de la Oficina Asesora de TIC.
- Todo mensaje SPAM o CADENA debe ser inmediatamente reportado a la Oficina Asesora de TIC. No está permitido el envío y/o reenvío de mensajes en cadena.
- Todo mensaje sospechoso respecto de su remitente o contenido debe ser inmediatamente reportado a la Oficina Asesora de TIC y proceder de acuerdo a las indicaciones de esta Oficina, lo anterior, debido a que puede ser contenido de virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif, tengan explícitas referencias no relacionadas con la misión de la Entidad (como por ejemplo: contenidos eróticos, alusiones a personajes famosos).
- La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o a cualquier otra ajena a los fines de la Entidad.
- Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.
- Está expresamente prohibido distribuir información de la MUNICIPIO DE BUCARAMANGA, no pública, a otras entidades o ciudadanos sin la debida autorización de la Dirección.
- El único servicio de correo electrónico autorizado para el manejo de la información institucional en la Entidad es el asignado por la Oficina Asesora de TIC, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.

4.5.2 USO DE INTERNET

El MUNICIPIO DE BUCARAMANGA a través La Oficina Asesora de TIC establecerá reglas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones, previa validación. De acuerdo al buen uso de los recursos de navegación de la Entidad se deben tener en cuenta los siguientes lineamientos:

- El uso del servicio de Internet está limitado exclusivamente para propósitos laborales.
- Los servicios a los que un determinado usuario pueda acceder desde internet dependerán del rol o funciones que desempeña el usuario en el MUNICIPIO DE BUCARAMANGA y para los cuales esté formal y expresamente autorizado.

- Todo usuario es responsable de informar a la Oficina Asesora de TIC los contenidos o acceso a servicios que no le estén autorizados y/o no correspondan a sus funciones dentro del MUNICIPIO DE BUCARAMANGA.
- Está expresamente prohibido el envío, y/o descarga, y/o visualización, de páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.
- Está expresamente prohibido el envío y/o descarga de cualquier tipo de software o archivos de fuentes externas, y/o de procedencia desconocida que puedan causar cualquier tipo de daños en los equipos y redes.

- Está expresamente prohibido acceder a páginas que agredan la ética y el buen comportamiento.

El MUNICIPIO DE BUCARAMANGA se reserva el derecho de monitorear los accesos, y por tanto el uso del servicio de internet de todos sus funcionarios o contratistas, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines de la Entidad.

4.6 RESPONSABILIDADES Y CONTRASEÑAS

Todos los funcionarios, contratistas y/o colaboradores que hagan uso de los activos de información del MUNICIPIO DE BUCARAMANGA, tienen la responsabilidad de seguir las reglas establecidas en la presente política y sus documentos anexos a la misma, entendiendo que el uso no adecuado de los recursos puede poner en riesgo la continuidad de la misión institucional.

La gestión de usuarios se asignará con previo conocimiento de las funciones a implementar en el MUNICIPIO DE BUCARAMANGA, por lo tanto, el manejo de documentos, cuentas de correo, accesos a sistemas de información y activos de información es responsabilidad de cada usuario, por lo cual la sensibilización de los usuarios frente a sus responsabilidades ha de ser constante.

4.7 SEGURIDAD FÍSICA

El tratamiento a amenazas tales como acceso no autorizado, robo, pérdida, daño, entre otros (riesgos físicos y ambientales) que puedan afectar los activos de información, medios de procesamientos y comunicaciones, así como las instalaciones donde que se encuentran ubicados.

Esto es el control de medios extraíbles, control sobre dispositivos a puertos de red y seguridad del entorno.

4.8 GESTIÓN DE RIESGOS

El MUNICIPIO DE BUCARAMANGA deberá realizar todas las acciones con el fin de minimizar los riesgos de la entidad establecidos en el mapa de riesgo institucional,

especialmente los relacionados con la información de la organización. La gestión del riesgo tendrá en cuenta lo siguiente:

1. Identificación de vulnerabilidades y amenazas sobre los activos de información.
2. Identificación de Riesgos, Evaluación de Riesgos
3. Monitoreo
4. Planes de Acción / Tratamiento
5. Criterios de Aceptación de riesgos

4.9 GESTIÓN DEL CONOCIMIENTO

La documentación relacionada con la seguridad de la información es de vital importancia para el proceso de mejora continua y para cumplir con criterios de calidad propuesto por lo sistema de gestión tanto de calidad y seguridad de la información. Los procesos de mejora continua han de establecer las mediciones y revisiones periódicas de las políticas, manuales y procedimientos para lograr dicho objetivo.

4.10 GESTIÓN DE INCIDENTES

El MUNICIPIO DE BUCARAMANGA mediante la oficina asesora de TIC establecerá los procedimientos de preparación, detección y análisis, contención / respuesta, erradicación y recuperación.

4.11 CONTINUIDAD DEL NEGOCIO

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 y de vínculo con entidades externas, probarse y revisarse de manera periódica.

4.12 NORMATIVIDAD

La política de seguridad de información del MUNICIPIO DE BUCARAMANGA se basa en los lineamientos dados por el decreto 2573 de 2014 para la implementación de Gobierno en Línea, el cual establece el componente de seguridad y privacidad de la información para implementación de la estrategia de gobierno en línea, articulándose con toda la normatividad vigente en la ley colombiana en cuanto a delitos informáticos, protección de datos personales y transparencia. Además, vincula los derechos intelectuales sobre desarrollos de aplicativos y el manejo de la información dentro de la entidad basada en las recomendaciones de la ISO 27000.

5. CONTROL DE CAMBIOS

FECHA	VERSIÓN	JUSTIFICACIÓN	REALIZÓ
	V.0.0	Creación del documento	OFICINA TIC

ANEXO 2

POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES DEL MUNICIPIO DE BUCARAMANGA

1. OBJETIVO

Establecer mecanismos para la obtención, recolección, uso, tratamiento y procesamiento de datos personales en función del cumplimiento de la constitución y las leyes vigentes para el cumplimiento al derecho de todas las personas de conocer, actualizar y rectificar la información encontrada en las bases de datos del MUNICIPIO DE BUCARAMANGA.

2. NORMATIVIDAD

Constitución política de Colombia

Ley 1266 de 2008

Ley 1581 de 2012

Decreto 1377 de 2013

Sentencia C-741

3. DEFINICIONES Y PRINCIPIOS

Las definiciones vinculadas en la siguiente política del MUNICIPIO DE BUCARAMANGA son las siguientes:

a) **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
b) **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.
c) **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
d) **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.
e) **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 datos.
f) **Titular**: Persona natural cuyos datos personales sean objeto de Tratamiento.

g) **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Los principios fundamentales asociados por la ley de protección de datos personales y la política del MUNICIPIO DE BUCARAMANGA enmarcan:

a) **Principio de legalidad en materia de Tratamiento de datos:** El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.
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.
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 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 Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
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 la ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas por la ley 1581 de 2012.
g) **Principio de seguridad:** La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento, 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 por la ley y en los términos de la misma.

4. POLÍTICA DE GENERAL DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

El MUNICIPIO DE BUCARAMANGA administrará los datos de los ciudadanos, servidores públicos, proveedores y demás colaboradores bajo los principios establecidos en la ley 1581 de 2012 para los procesos en los cuales estos actores voluntariamente entregaron para ser gestionados y administrador por el Municipio informando debidamente a los

titulares cualquier cambio o actividad realizada para el tratamiento con el fin de obtener alguna autorización adicional para un servicio o proceso.

Los datos suministrados al base de datos serán registrados a plena voluntad del titular para el acceso a trámites o servicios del MUNICIPIO DE BUCARAMANGA cuya administración seguirá los principios de la seguridad de la información en especial la confidencialidad y la integridad. A su vez el titular garantiza al MUNICIPIO DE BUCARAMANGA, que los datos suministrados son veraces y completos para el buen fin de trámites o servicios solicitados. Estos datos podrán ser transferidos a un tercero en virtud del cumplimento de la ley ante investigaciones de carácter administrativo o judicial ante el debido trámite para dicho fin.

La administración de la información en el MUNICIPIO DE BUCARAMANGA podrá ser encargada a contratistas y proveedores para su tratamiento bajo el estricto cumplimiento del principio de confidencialidad. En caso de que el titular registre datos incompletos o no veraces el MUNICIPIO DE BUCARAMANGA tendrá la autonomía de eliminar estos registros de las bases de datos, también en caso de que finalice algún proceso y no se considere pertinente mantener dicho registro activo.

El MUNICIPIO DE BUCARAMANGA adoptará los niveles de seguridad para sus bases de datos según la política de seguridad de la información, sin embargo, no se responsabiliza por cualquier consecuencia derivada del ingreso indebido de terceros a la base de datos y/o por alguna falla técnica en el funcionamiento y/o conservación de datos en el sistema en cualquiera de los menús de su página web. Igualmente, no garantiza la disponibilidad de los servicios en línea y de la información que los usuarios requieran en determinado momento. Por lo tanto, el MUNICIPIO DE BUCARAMANGA no responderá en ningún caso y bajo ninguna circunstancia, por los ataques o incidentes contra la seguridad de su sitio web o contra sus sistemas de información; o por cualquier exposición o acceso no autorizado, fraudulento o ilícito a su sitio web y que afecten la confidencialidad, integridad o autenticidad de la información publicada o asociada con los contenidos y servicios que se ofrecen en él. El MUNICIPIO DE BUCARAMANGA podrá utilizar cookies durante la prestación de servicios en su sitio web con el objetivo de gestionar y mejorar los servicios ofrecidos a través del portal institucional.

5. DERECHOS DE LOS TITULARES DE LA INFORMACIÓN

El Titular de los datos personales tendrá los siguientes derechos:

a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a

error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.

b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la ley 1581 de 2012.
c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que les ha dado a sus datos personales.
d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto por la ley.
e) 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.
f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

6. PROCEDIMIENTOS Y RESPONSABILIDADES

El MUNICIPIO DE BUCARAMANGA cumplirá con los deberes previstos en la ley para el tratamiento de datos personales garantizando al titular su pleno derecho de *habeas data* además de los recursos disponibles para ejercer dicho derecho. Así mismo creará y gestionará los procedimientos y formatos para la atención al titular para hacer valer sus derechos, ya sea de consulta, actualización, rectificación, supresión y revocación de la autorización de los datos, el titular lo solicitará a través de los diferentes canales dispuestos para tal fin.

El titular es responsable de suministrar la información veraz y completa al MUNICIPIO DE BUCARAMANGA, así como el buen uso de informático para la protección de sus datos personales. Por otra parte, el Municipio de Bucaramanga no se responsabiliza de ataques informáticos o código malicioso en sus sistemas de hardware o software o cualquier documento digital alojado en los servicios web, sin embargo, se compromete a gestionar y minimizar los riesgos asociados a través la política de seguridad de la información.

6.1. CANALES DE ATENCIÓN A TITULARES

El MUNICIPIO DE BUCARAMANGA atenderá los requerimientos de los titulares a través de la oficina de atención al ciudadano para atención de reclamos de los titulares en su derecho de la ley de protección de datos 1581 de 2012 y su normatividad vigente.

También el titular podrá ejercer su derecho mediante el uso de las direcciones electrónicas relacionadas:

Correo protección de datos: **datospersonales@bucaramanga.gov.co**

En el caso del registro de hojas de vida para el Municipio a través de la plataforma tu talento es lo que vale será:

Tu talento es lo que vale: **info@bucaramanga.gov.co**

7. AVISO DE PRIVACIDAD

En cualquier caso, el Municipio de Bucaramanga manejará el siguiente aviso de privacidad para sus bases de datos que sean protegidas y gestionadas como datos personales:

"El MUNICIPIO DE BUCARAMAGA, identificado con el NIT 890.201.222-0 y con domicilios Fase I: Calle 35 # 10-43 y Fase II: Carrera 11 # 34-52 ubicado en la ciudad de Bucaramanga (Santander) y como responsable del manejo de recolección, almacenamiento, utilización, circulación y suprimir datos de carácter personal bajo la ley 1581 de 2012 se compromete a garantizar el buen uso de los datos de los titulares para el cumplimiento de las funciones institucionales y procesos misionales del Municipio. Los titulares podrán ejercer sus derechos mediante los canales dispuestos en la presente política."

8. CONTROL DE CAMBIOS

FECHA	VERSIÓN	JUSTIFICACIÓN	REALIZÓ
	V.0.0	Creación del documento	Oficina TIC

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="2">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="3">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></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></td><td>Formatos de chequeo, monitoreo y control.</td></tr>
</table>

Otros Entregables

1. POLITICA DE PRIVACIDAD DE SITIO WEB DEL MUNICIPIO DE BUCARAMANGA

El sitio web del MUNICIPIO DE BUCARAMANGA es un espacio para la divulgación oficial de información de interés para la ciudadanía y los actores interesados en conocer las diferentes actividades que realiza la administración central de la Alcaldía de Bucaramanga**.**

La privacidad y confidencialidad de la información del usuario registrada en el sitio web es entregada a plena voluntad del titular y en ningún caso esta información podrá cederse a terceros sin la autorización previa articulada con la legislación vigente para la protección de datos personales (Ley 1581 de 2012, Decreto 1377 de 2013). Se recomienda que el uso de claves y usuarios este bajo su responsabilidad y debe ser exclusivamente para el uso personal en los trámites en línea a través de este sitio.

El sitio web utiliza cookies para el registro de las visitas y actividad del sitio con el fin de mejorar las características del mismo; en cualquier momento el usuario puede autorizar o configurar su navegador con el fin de no permitir la utilización de las mismas en los dispositivos que utilice para acceder al sitio web del MUNICIPIO DE BUCARAMANGA.

El Municipio de Bucaramanga no se responsabiliza del uso abusivo de la información publicada por otros usuarios en espacio de opinión, ni los archivos adjuntos estén libre de software malicioso. Además, no se garantiza la disponibilidad del sitio por fallas técnicas o ataques cibernéticos a bases de datos. Sin embargo, la mitigación de estos riesgos estará definidos bajo la política de seguridad de la información.

2. CONDICIONES DE USO

EL MUNICIPIO DE BUCARAMANGA, es la entidad territorial que tiene como fin administrar y gestionar las políticas públicas para el beneficio ciudadano de la ciudad de Bucaramanga, la información contenida en su sitio web (www.bucaramanga.gov.co) es para el beneficio de toda la ciudadanía en general, sus clientes y/o proveedores u otras entidades de carácter público de control y gestión.

La función principal del sitio web es difundir los temas y actividades que tienen que ver con su misión, su visión, objetivos y las funciones que le corresponden. Adicionalmente, por este medio la entidad da a conocer información sobre Políticas, planes, programas y proyectos institucionales, Trámites; Servicios; Indicadores de Gestión; Planes y Programas; Publicaciones; Normas; Convocatorias; Información presupuestal y de contratación; páginas recomendadas, y, en general, información relacionada con el gobierno y la entidad

o de los programas que desarrollan las entidades si es el caso. Adicionalmente, permite la opción de solicitar trámites en línea y ofrece herramientas de interacción para los usuarios del sitio.

El MUNICIPIO DE BUCARAMANGA solicita al Usuario de esta página, que lea detallada y juiciosamente estas condiciones de uso y la política de privacidad de este Sitio Web, antes de iniciar su exploración o utilización. Si el Usuario no está de acuerdo con estas Condiciones de Uso o con cualquier disposición de la Política de Privacidad, le sugerimos que se abstenga de acceder o navegar por el Sitio Web de nuestra entidad.

2.1. ACEPTACIÓN DE CONDICIONES DE USO Y POLÍTICA DE PRIVACIDAD

El usuario es responsable del conocimiento de las condiciones y políticas de privacidad del sitio, el MUNICIPIO DE BUCARAMANGA se reserva el derecho de modificar, actualizar sin aviso alguno la información contenida en el sitio. El acceso al sitio es carácter libre y gratuito para todos los usuarios.

2.2. CONTENIDO DEL SITIO

El sitio web y todos sus contenidos están alineados para la misión, visión y objetivos institucionales de la entidad en virtud de favorecer con la publicación de la información a los ciudadanos u otros entes de participación con el Municipio. La información publicada es de carácter informativo de manera que no se considera completa o exhaustiva para satisfacer necesidades propias de cada usuario.

Pueden existir otros enlaces web a diferentes entidades externas al municipio con el fin de facilitar la gestión y la integración de otros entes territoriales y nacionales, por lo cual el MUNICIPIO DE BUCARAMANGA no se hace responsable por el contenido ni la administración de los mismos.

2.2.1. RESPONSABILIDAD DEL CONTENIDO

El municipio no se responsabiliza por publicaciones en los espacios de opinión ciudadana, ni garantiza que los contenidos de los archivos estén libres de contenidos maliciosos, por lo cual el MUNICIPIO DE BUCARAMANGA no se hará responsable en daños de equipo o perdida de información por contenidos alojados en el sitio.

Debido a que en la actualidad los medios técnicos no permiten garantizar la absoluta falta de injerencia de la acción de terceras personas en el Sitio Web, el MUNICIPIO DE BUCARAMANGA de ninguna manera asegura la exactitud y/o veracidad de todo o parte de la información contenida en su página, ni su actualización, ni que dicha información haya sido alterada o modificada en todo o en parte, luego de haber sido publicada en la página, ni cualquier otro aspecto o característica de lo publicado en el sitio o en los enlaces,

respectivamente. En ningún momento los contenidos alojados serán de carácter sexista, racista, discriminatorios u obscenos o algún otro atentado de los derechos fundamentales consagrados en la ley.

2.2.2. DERECHOS INTELECTUALES

El contenido del sitio es netamente exclusivo del MUNICIPIO DE BUCARAMANGA, por lo tanto, los logos y otros elementos de la identidad corporativa estará bajo la protección de la ley. De igual manera el uso de la identidad de otras entidades se realiza sin la necesidad de perder el control y los derechos por parte de las entidades que sean mencionadas.

Cualquier uso o publicación debe ser autorizada por el MUNICIPIO de BUCARAMANGA.

2.2.3. REGISTRO, PARTICIPACIÓN Y PUBLICACIONES DE LOS USUARIOS.

Al ingresar al sitio Web y para garantizar el buen y adecuado uso de la misma, el Usuario deberá cumplir con lo siguiente:

- Ser responsable por cualquier actividad que se lleve a cabo bajo su registro.
- Ser responsable de la seguridad de su contraseña.
- No abusar, acosar, amenazar o intimidar a otros usuarios del Sitio Web ya sea a través de los chats, foros, blogs o cualquier otro espacio de participación.
- No usar el Sitio Web como medio para desarrollar actividades ilegales o no autorizadas tanto en Colombia, como en cualquier otro país.
- Ser el único responsable por su conducta y por el contenido de textos, gráficos, fotos, videos o cualquier otro tipo de información de la cual haga uso o incluya en el Sitio Web.
- Abstenerse de enviar correo electrónico no deseado (SPAM) a otros usuarios de este Sitio Web, así como también de transmitirles virus o cualquier código de naturaleza destructiva.

El usuario reconoce que su participación en cualquier foro, chat, comentario, blog y/o cualquier otro espacio de participación del Sitio Web, será bajo su exclusiva responsabilidad, y que de igual forma, las opiniones y/o acciones y/o comportamiento de otros usuarios en tales espacios son responsabilidad exclusiva de quienes las emiten o realizan, por lo cual el MUNICIPIO DE BUCARAMANGA no se hace responsable ni garantiza la calidad o idoneidad de tales conductas u opiniones, ni por las consecuencias que ellas pudieren acarrear a favor y/ o en contra de otros usuarios o de terceros.

3. ACTUALIZACIÓN DE LA POLÍTICA DE PRIVACIDAD DEL SITIO WEB Y CONDICIONES DE USO Y NORMATIVIDAD VIGENTE

El municipio de Bucaramanga se reserva el derecho de actualizar sus políticas de forma unilateral, por lo tanto, el usuario es responsable de revisar y leer las condiciones de uso y privacidad. Las políticas definidas se articularán con la legislación vigente tanto para la protección de datos personales como los lineamientos de la estrategia de gobierno en línea.