
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ÁREA METROPOLITANA DE BUCARAMANGA

Área de apoyo tecnológico y de la información

2021



Contenido

1. INTRODUCCIÓN	3
2. OBJETIVOS DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	4
3. PROCESO DE SEGURIDAD Y PRIVACIDAD DE LA INFORAMCIÓN	4
4. POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL AMB (Adoptada mediante Resolución 000024 del 21 de enero del 2020)	5
4.1 OBJETIVO DE LA PÓLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL AMB (Adoptada mediante Resolución 000024 del 21 de enero del 2020)	5
5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. ...	5
6. OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	6
7. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORAMCIÓN MSPI	6
8. DOCUMENTOS DE REFERENCIA	9
CONTROL DE CAMBIOS	10

1. INTRODUCCIÓN

El Área Metropolitana de Bucaramanga es una entidad administrativa formada por un conjunto de cuatro Municipios, dotada de personería jurídica, de derecho público, autonomía administrativa, patrimonio propio y régimen administrativo, fiscal especial.

De acuerdo con lo establecido por la Ley 1625 de 2013, tiene dentro de sus competencias programar y coordinar el desarrollo armónico, integrado y sustentable de los municipios que la conforman; y en este contexto ha contribuido de forma activa en la conformación del territorio, mediante el liderazgo en los procesos de planificación enmarcados dentro del componente físico territorial del Plan de Desarrollo Metropolitano, estableciendo políticas, planes y proyectos de aumento, mejoramiento, cualificación, del espacio público, parques, zonas verdes y deportivas.

El área metropolitana de Bucaramanga AMB como entidad Pública busca afrontar los diferentes retos con una infraestructura moderna, robusta y segura y competitiva en el nuevo mundo digital. Con ello se busca promover la implementación y ejecución de buenas prácticas de seguridad y privacidad de la información, siendo la información un activo de gran importancia para la entidad que permite el desarrollo continuo de la misión y el cumplimiento del objetivo de la misma.

Por la cual adopta el modelo integrado de gestión MIPG, la política de Gobierno digital (en donde se encuentra como habilitador el modelo de seguridad y privacidad de la información) la política de seguridad digital (Fortalecimiento organizacional, Gestión de TI, Direccionamiento estrategia, Gestión Jurídica), que por medio de la resolución metropolitana 000024 del 21 de enero del 2020 adopta el plan estratégico de tecnologías de la información y las comunicaciones, PETIC 2019 - 2020 y la política general del modelo de seguridad y privacidad de la información del área metropolitana de Bucaramanga.

Teniendo en cuenta lo anterior se actualiza el presente documento para dar cumplimiento a lo establecido en la resolución en mención y continuar mejorando los procesos internos en cuanto a la gestión de la seguridad de la información transversalmente con los planes, procesos y proyectos de TI.

2. OBJETIVOS DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Establecer las actividades que están contempladas en el Modelo de Seguridad de la Información MSPi, alineadas con la NTC/IEC 27001:2013, La política de seguridad de la información y la continuidad del servicio, en el Mapa de procesos de la entidad

3. PROCESO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EL Área Metropolitana Bucaramanga para la actual vigencia adoptará en su modelo de procesos, el proceso de Seguridad y Privacidad de la información en el nivel estratégico que permitirá garantizar de manera continua o reguladas la seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios prestados por el área de apoyo tecnológico y de la información, por medio de la definición de políticas, programas, lineamientos y estrategias y actividades.

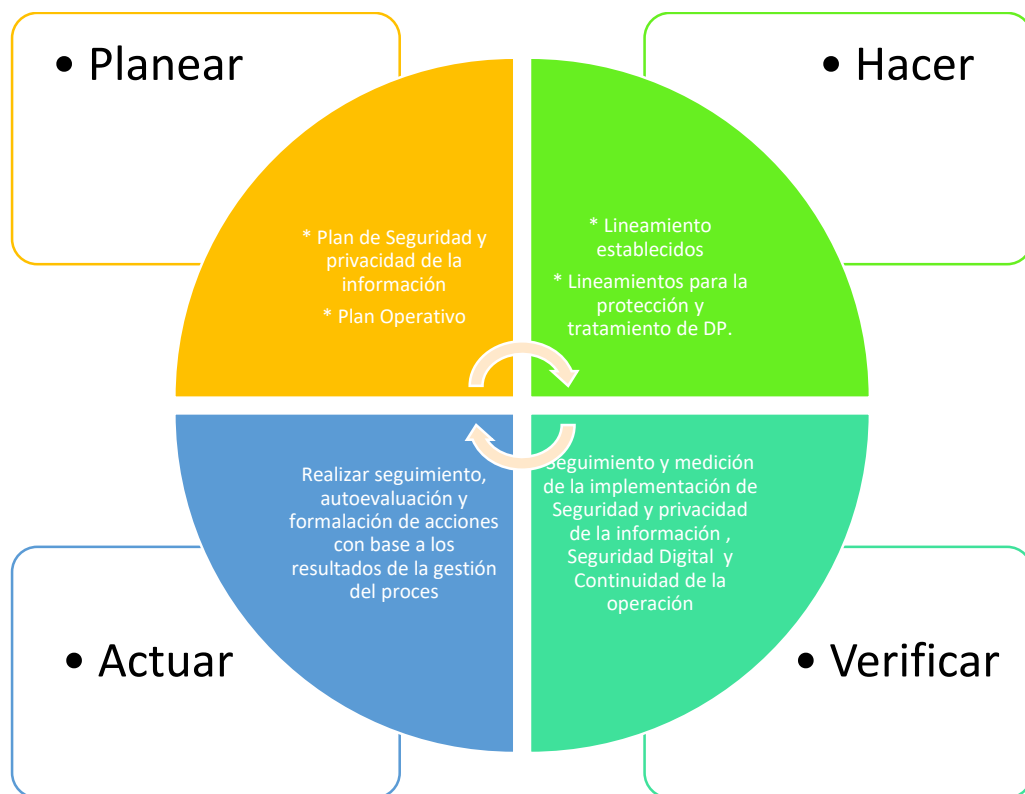


Ilustración 1Ciclo PHVA del proceso de Seguridad y privacidad

4. POLITICA GENERAL DE SEGURIDAD Y PRIVA CIDAD DE LA INFORMACIÓN DEL AMB (Adoptada mediante Resolución 000024 del 21 de enero del 2020)

El Área Metropolitana de Bucaramanga, en su compromiso de generar un ambiente de seguridad de información, opta por crear una política con respecto a la gestión de la seguridad de la información en función de una misión y una visión institucional que permite reducir el riesgo a una mala manipulación de la información única y confidencial, esta política una vez aprobada debe ser publicada y comunicada a todos sus funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan acceso a información a través de los documentos, equipos de cómputo, infraestructura tecnológica.

Para el área metropolitana 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 la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

4.1 OBJETIVO DE LA PÓLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL AMB (Adoptada mediante Resolución 000024 del 21 de enero del 2020)

Para el área metropolitana de Bucaramanga, el establecer políticas y lineamientos de seguridad y privacidad de la información, teniendo en cuenta requisitos legales, operativos, tecnológicos, y dando cumplimiento a la concepción de seguridad en cuanto a confidencialidad, Integridad, disponibilidad y autenticación de la información, ayudara a determinar permitir y conocer las políticas del buen uso y administración de la información dentro de nuestra organización a todos los funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación), bajo el liderazgo del área de sistemas de información y gestión corporativa.

5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Aplica a todos los niveles del Área Metropolitana de Bucaramanga, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la entidad compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación. Así mismo, esta lo dispuesto en este documento y su implementación aplica a toda la información creada, procesada o utilizada por el AMB, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

6. OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN



7. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MSPI

El plan de implementación para la dimensión de Seguridad y privacidad de la información comprende el siguiente cronograma y se hace seguimiento mes a mes.

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE	FECHAS PROGRAMADAS	
				FECHA DE INICIO	FECHA FINAL
Activos de información	Definir lineamientos para el levantamiento de activos de información	Actualización de metodología e instrumentos de	Secretaria General Área de apoyo	01/04/2021	30/07/2021

		levantamiento de activos de información	tecnológico de la información		
		Validar Activos de información en el instrumento levantado en la vigencia anterior	Secretaria General Área de apoyo tecnológico de la información	01/04/2021	30/07/2021
Gestión de riesgos	Actualización de lineamientos de riesgos	Actualizar la política y metodología de gestión del riesgo	Área de apoyo tecnológico de la información	01/05/2021	30/09/2021
	Identificación	Identificación, análisis y evaluación de riesgos – Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la operación	Área de apoyo tecnológico de la información	01/05/2021	30/09/2021
	Seguimiento Fase de tratamiento	Seguimiento Estado de planes de tratamiento de riesgos identificados y verificados de evidencias	Área de apoyo tecnológico de la información	30/09/2021	31/12/2021
Gestión de incidentes de seguridad de la información	Publicar socializar el procedimiento de incidentes de seguridad y privacidad de la información	Elaborar procedimiento actualizado de incidentes de seguridad de la información basado en la norma ISO 27035.	Área de apoyo tecnológico de la información	01/09/2021	31/10/2021
		Socializar el procedimiento a los colaboradores de la Entidad	Área de apoyo tecnológico de la información	01/11/2021	30/11/2021

	Eventos/Vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados al SGSI	Área de apoyo tecnológico de la información	01/10/2021	30/11/2021
Gestión de la continuidad	Documentación del Análisis de Impacto de la operación	Análisis del Impacto del Negocio, valoración de riesgos de interrupción para el Plan de continuidad de la operación	Área de apoyo tecnológico de la información	01/04/2021	30/06/2021
Gobierno Digital	Gobierno Digital	Revisar y alinear la documentación del SGSI de la entidad al MSPI de acuerdo a la normatividad vigente	Área de apoyo tecnológico de la información	01/03/2021	30/06/2021
Gestión de cambio y cultura	Cultura organizacional	Emitir información de buenas prácticas en cuestión de seguridad y privacidad de la información a las diferentes áreas de la entidad.	Área de apoyo tecnológico de la información	01/02/2021	31/12/2021
Protección de datos	Registro y actualización de la base de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Área de apoyo tecnológico de la información	01/05/2021	30/08/2021

8. DOCUMENTOS DE REFERENCIA

- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 527 de 1999. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
- Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se 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, entre otras disposiciones.
- 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 - TICSe crea la agencia Nacional de espectro y se dictan otras disposiciones.
- Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario
- Ley 1955 de 2019. por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad".
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- CONPES 3905 de 2020. Política Nacional de Confianza y Seguridad Digital.

CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
05/01/2021	Versión 1.	Elaboración del Plan

Elaboró

Ing. Freddy Neil Varela Lemus. PU – SAF

Ing. Anderson Favian Mendoza Navas. PU -SPI

Revisó:

Aprobó:

