



PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT



ALCALDÍA DE
BUCARAMANGA

Instituto
de **Cultura y**
Turismo



CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

Contenido

1. INTRODUCCIÓN	4
2. OBJETIVO GENERAL	4
3. OBJETIVOS ESPECIFICOS	4
4. FINALIDAD	5
5. ALCANCE	6
6. DOCUMENTOS DE REFERENCIA	6
7. RECURSOS	7
8. VIGENCIA	8
9. PLANEACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	8
9.1 DESCRIPCIÓN DEL CICLO DE OPERACIÓN	9
9.2 FASE DE DIAGNOSTICO -- ETAPAS PREVIAS A LA IMPLEMENTACIÓN	10
9.3 FASE DE PLANIFICACION	11
9.3.1 Análisis del contexto	11
9.3.2 Plan Estratégico de Seguridad.	12
9.4 Misión TIC	13
9.5 Proyección en materia de Seguridad y Gestión de la Información	13
9.6 Líneas de Acción TIC Sectoriales	13
9.7 Análisis DOFA	15
10. ESTRATEGIA DE SEGURIDAD DIGITAL	16
10.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS	19
10.2 PORTAFOLIO DE PROYECTOS Y ACTIVIDADES	19
11. PROYECCION DE COSTOS	20
12. LIDERAZGO	23
13. PLANEACIÓN	24
14. SOPORTE	24
15. FASE DE IMPLEMENTACIÓN	25
16. CONSULTA, DIVULGACIÓN Y ACTUALIZACIÓN DEL PLAN DE OPERACIONES	26
17. MONITOREO Y REVISIÓN DEL PLAN	26
18. SEGUIMIENTO AL PLAN DE TRABAJO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	27

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

19. GLOSARIO	27
20. REFERENCIAS BIBLIOGRAFICAS	29
20.1 Fuentes Bibliográficas	29
20.2 Fuentes de la Entidad.....	30
21. CONTROL DE CAMBIOS.....	31

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

1. INTRODUCCIÓN

Desde 2024, el Instituto Municipal de Cultura y Turismo de Bucaramanga (IMCT) ha venido implementando acciones estratégicas para garantizar la integridad, confidencialidad y disponibilidad de sus activos de información, mediante la adopción progresiva **del Modelo de Seguridad y Privacidad de la Información**, en concordancia con los lineamientos de la norma ISO/IEC 27001 y la Política de Gobierno Digital.

La planificación de este modelo se ha definido con base en las necesidades institucionales, los objetivos estratégicos y el enfoque de gestión de riesgos del Sistema de Gestión de la Calidad, en coherencia con la estructura organizacional vigente.

El presente Plan Operacional de Seguridad y Privacidad de la Información consolida las acciones estratégicas y operativas necesarias para fortalecer la cultura de seguridad digital en la Entidad; para ello, involucra a todos los funcionarios en procesos de formación y sensibilización, preservando los principios de disponibilidad, integridad, confidencialidad, autenticación y no repudio.

Su implementación se enmarca en un enfoque por procesos, alineado con la norma ISO 9001:2015 y el Modelo Integrado de Planeación y Gestión (MIPG), contribuyendo a optimizar los recursos institucionales y a robustecer las capacidades operativas del Instituto en materia de seguridad digital.

2. OBJETIVO GENERAL

Definir y ejecutar un plan de trabajo que brinda continuidad y sostenibilidad a la implementación del Modelo de Seguridad y Privacidad de la Información en el Instituto Municipal de Cultura y Turismo de Bucaramanga, mediante el cumplimiento de las directrices del Manual de Seguridad Digital, la estrategia de gestión de riesgos y los protocolos de atención a incidentes, asegurando la protección efectiva de los activos de información y fortaleciendo la confianza de los ciudadanos en los servicios institucionales.

3. OBJETIVOS ESPECIFICOS

- a. Asegurar que las acciones en materia de seguridad digital estén alineadas con los principios de mejora continua y los requisitos de la norma ISO/IEC 27001.
- b. Garantizar el cumplimiento del Modelo de Seguridad y Privacidad de la Información bajo la responsabilidad de:
 - Subdirección Administrativa y Financiera – Proceso de Gestión Tecnológica, en la implementación, soporte y gestión de incidentes de seguridad digital.

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

- Oficina Asesora de Control Interno, en la auditoría del modelo y los riesgos de seguridad.
 - Oficina de Talento Humano, en la gestión de la seguridad de los recursos humanos.
 - Funcionarios y contratistas, en la apropiación de la cultura de seguridad y cumplimiento normativo.
 - Promover la cultura institucional y ciudadana en torno a la protección de la información, mediante programas de sensibilización, capacitación y uso responsable de los activos digitales.
 - Fortalecer la seguridad de los activos de información institucionales, reduciendo riesgos a niveles aceptables a través de estrategias de seguridad digital integral.
- c. Definir y consolidar la estrategia de seguridad digital del Instituto Municipal de Cultura y Turismo de Bucaramanga (IMCT), como marco orientador para la protección de la información institucional, la gestión de riesgos y la promoción de una cultura de seguridad en todos los niveles de la Entidad.
- d. Definir y establecer las necesidades del Instituto para la ejecución del Modelo de Seguridad y Privacidad de la información (MSPI).
- e. Priorizar los proyectos a implementar para la correcta implementación del MSPI.
- f. Planificar la evaluación y el seguimiento periódico de los controles y lineamientos establecidos en el marco del Sistema de Gestión de Seguridad de la Información, con el fin de asegurar su efectividad, detectar oportunidades de mejora y garantizar la protección continua de los activos de información del Instituto.

4. FINALIDAD

Establecer directrices claras para la actualización, implementación, cumplimiento y supervisión del Plan Operacional de Seguridad y Privacidad de la Información del Instituto, dirigidas a todos los funcionarios y al personal contratista que tenga acceso a la información y a los activos informáticos. Todos los involucrados deberán velar por la confidencialidad, integridad y disponibilidad de la información, garantizando así la continuidad de las operaciones administrativas, logísticas y misionales de la Entidad. Este enfoque busca reducir los riesgos digitales, proteger los datos de manera efectiva y optimizar el uso de las tecnologías de la información.

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

5. ALCANCE

El alcance del Plan de Seguridad y Privacidad de la Información comprende la implementación y sostenibilidad del Sistema de Gestión de Seguridad de la Información (SGSI) a través de una estrategia integral de seguridad digital, que inicia con un diagnóstico institucional y se desarrolla aplicando el ciclo PHVA (Planear, Hacer, Verificar y Actuar), con énfasis en la mejora continua.

Este plan abarca todos los activos de información administrados por los procesos de la entidad y es de obligatorio cumplimiento para funcionarios, contratistas y terceros vinculados. Su aplicación busca asegurar una gestión segura, responsable y eficiente de la información institucional, bajo la coordinación de la Subdirección Administrativa y Financiera – Proceso de Gestión Tecnológica, como dependencia responsable de su implementación y seguimiento.

6. DOCUMENTOS DE REFERENCIA

- a. Decreto 612 de 2018, "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", donde se encuentra el presente Plan Estratégico de Seguridad de la información (PETI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- b. Resolución 500 de 2021. " La presente resolución tiene por objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital "
- c. Manual de Gobierno Digital (El Manual de Gobierno Digital es el documento que establece los lineamientos y estándares de los componentes de la política (TIC para el Estado y TIC para la Sociedad) y de los habilitadores transversales (arquitectura, seguridad y privacidad de la información y servicios ciudadanos digitales).
- d. Modelo de Seguridad y Privacidad de la información – MINTIC “Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digita”.

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

7. RECURSOS

Con el propósito de dar cumplimiento a lo enunciado, se establece la siguiente estructura organizacional en seguridad para dar cumplimiento al Modelo de Seguridad y Privacidad de la información del Instituto.

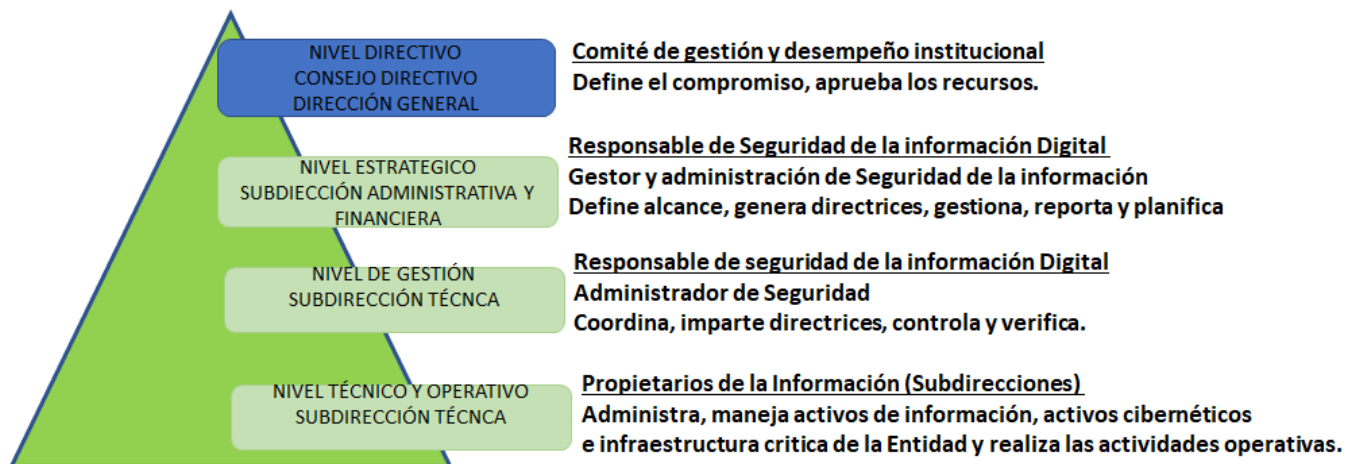


Figura No.1. Estructura Organizacional de Seguridad del Instituto
Fuente: Propia de la Subdirección Administrativa y Financiera

a. El Comité Institucional de Gestión y Desempeño, en su rol como Comité de Dirección de la Política de Seguridad Digital, tiene la misión de impulsar y coordinar las acciones necesarias para fortalecer la seguridad de la información en el Instituto.

Su labor contribuye directamente al desarrollo de las dimensiones del Modelo Integrado de Planeación y Gestión (MIPG), asumiendo la responsabilidad de diseñar y proponer planes, programas, proyectos, metodologías y estrategias en materia de seguridad de la información, para su presentación y validación ante el Comité Institucional de Evaluación y Desempeño

b. Cada líder de proceso de la institución deberá designar a un funcionario de planta que integre el Comité Institucional de Evaluación y Desempeño. Este representante será responsable de cumplir con las directrices establecidas en los espacios de coordinación que se desarrollen a través de mesas técnicas de trabajo, así como de presentar, de forma semestral o cuando sea requerido, la información correspondiente a cada etapa del Modelo de Seguridad y Privacidad de la Información, según las responsabilidades asignadas a las políticas de MIPG.

c. El Instituto adopta una metodología para la administración y gestión del riesgo, basada y alineada con los lineamientos del Departamento Administrativo de la Función Pública

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA Instituto Municipal de Cultura y Turismo
VERSIÓN: 01		
FA: 2/09/2025	GESTIÓN TECNOLÓGICA	

(DAFP), el Estatuto Anticorrupción, la norma ISO 31000 y el Modelo Integrado de Planeación y Gestión (MIPG). Dentro de este marco, los riesgos de seguridad de la información se definen y estructuran para cada proceso institucional, garantizando un enfoque integral y coherente.

d. Para asegurar la continuidad y sostenibilidad del plan de implementación, la institución asigna los recursos necesarios, orientados a garantizar su óptimo funcionamiento y la protección de los activos de información, preservando sus tres pilares fundamentales de seguridad: confidencialidad, integridad y disponibilidad.

8. VIGENCIA

El presente Plan rige a partir de su promulgación hasta la fecha de su actualización.

9. PLANEACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



Figura No.2. Elementos o fases para la Implementación de un SGSI

Fuente: Tornado de: <https://www.normas-iso.com/iso-27001/>

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

9.1 DESCRIPCIÓN DEL CICLO DE OPERACIÓN

El ciclo de funcionamiento del Modelo de Seguridad y Privacidad de la Información se desarrolla en cinco (5) fases. Cada una de ellas incluye objetivos, metas y herramientas (guías) diseñadas para garantizar el cumplimiento efectivo de las disposiciones del modelo y asegurar su correcta implementación.



Figura No.3. Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

Fuente: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://gobiernodigital.mintic.gov.co/692/articulos-5482_Modelo_de_Seguridad_Privacidad.pdf

La adopción de un Modelo de Seguridad y Privacidad de la Información (MSPI) es una decisión estratégica para el Instituto, orientada a fortalecer la protección de sus datos y garantizar la continuidad de sus operaciones.

Esta decisión se basa en las necesidades y objetivos institucionales, en los requisitos de seguridad establecidos, en la forma en que se desarrollan los procesos y en la estructura general de gestión de la información.

Desde su diseño, los procesos, sistemas de información y controles incorporan criterios de seguridad, asegurando que la protección de la información esté presente desde la planeación hasta la operación diaria.

A continuación, se presentan los elementos o fases clave para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), el cual sirve como base para el MSPI del Instituto.

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

9.2 FASE DE DIAGNOSTICO -- ETAPAS PREVIAS A LA IMPLEMENTACIÓN

En esta fase, la Dirección del Instituto Municipal de Cultura y Turismo de Bucaramanga busca conocer con precisión el estado actual de la institución frente a los requerimientos del Modelo de Seguridad y Privacidad de la Información de Gobierno Digital.

Para ello, se desarrollarán las siguientes actividades:

1. Evaluar el estado actual de la gestión de seguridad y privacidad de la información dentro de la institución:
 - Identificar el nivel de madurez de los diferentes controles de seguridad digital implementados.
 - Determinar el grado de avance en la implementación del ciclo de operación de MSPI.
 - Verificar el nivel de cumplimiento de la legislación vigente en materia de protección de datos personales.
 - Identificar la adopción y aplicación de buenas prácticas en ciberseguridad.
- 2) Identificar vulnerabilidades técnicas y administrativas como insumo para la fase de planificación:
 - a) Evaluar el estado actual de la gestión y la adopción de controles técnicos y administrativos dentro de la institución.
 - b) Detectar vulnerabilidades técnicas y administrativas, así como realizar pruebas de penetración y analizar incidentes de seguridad ocurridos. Estos resultados servirán como base para la fase de planificación y la definición de acciones correctivas.

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

9.3 FASE DE PLANIFICACION

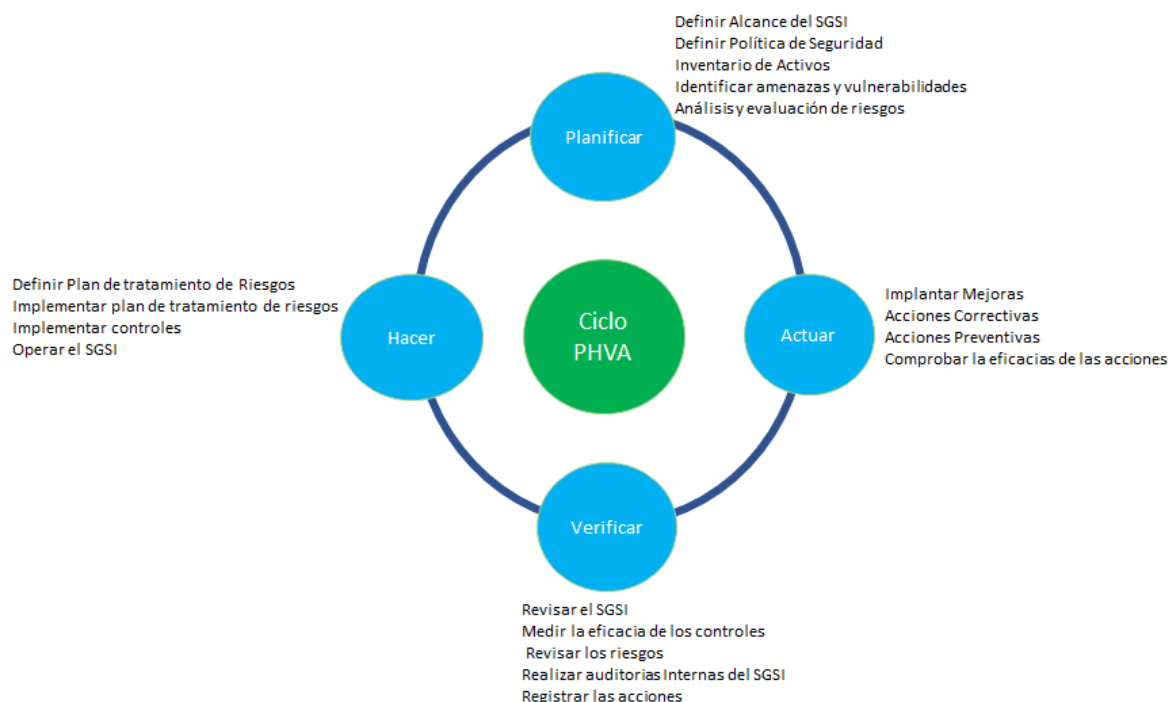


Figura No.4. Ciclo PHVA de Seguridad de la Información.

Fuente: Propia de la Subdirección Administrativa y Financiera

Esta fase comenzará con el análisis de los resultados obtenidos mediante la herramienta de diagnóstico del instrumento de Evaluación MSPI, aplicada por la Dirección del Instituto y alineada con la misión institucional. El propósito es definir las acciones necesarias para fortalecer la seguridad y privacidad de la información, aplicando la metodología de gestión de riesgos establecida en el Sistema de Administración de Riesgos del Instituto.

Las etapas a desarrollar en esta fase son las siguientes:

9.3.1 Análisis del contexto

El análisis interno y externo de la Institución forma parte de la metodología adoptada por la Entidad para la identificación de riesgos, en la cual cada proceso es verificado de manera sistemática. La planificación y ejecución del modelo ISO/IEC 27001 se desarrollará conforme al esquema de procesos establecido. En este sentido, se define una metodología

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

para la implementación del sistema, garantizando el cumplimiento de la normatividad vigente y alineándose con el ciclo PHVA, que comprende sus cuatro fases: planear, hacer, verificar y actuar.

9.3.2 Plan Estratégico de Seguridad.

El Plan Estratégico de Seguridad de la Información 2025 se estructura en cinco ejes estratégicos, cada uno con sus respectivos objetivos específicos. Estos ejes conforman la ruta de trabajo que el Instituto Municipal de Cultura y Turismo de Bucaramanga debe seguir de manera articulada, bajo un direccionamiento unificado, pero a la vez respetando la naturaleza y particularidades propias de cada uno.

1. Liderazgo de seguridad de la información.

Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información, teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad, a través del establecimiento de los roles y responsabilidades en seguridad de la información.

2. Gestión de riesgos.

Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados teniendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.

3. Concientización.

Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información, para que se convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, así como la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.

4. Implementación de controles.

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad; se pueden subdividir en controles tecnológicos y/o administrativos.

5. Gestión de incidentes.

Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

9.4 Misión TIC.

La estrategia TIC del Instituto tiene como misión establecer las directrices que orienten el gobierno y el uso adecuado de las tecnologías de la información y las comunicaciones en la entidad. Su propósito es garantizar la seguridad de los sistemas de información implementados, facilitando la toma de decisiones oportunas y fortaleciendo, la interacción, tanto con la ciudadanía como con las entidades públicas.

9.5 Proyección en materia de Seguridad y Gestión de la Información.

Al 2027, el Proceso de Gestión Tecnológica y Seguridad de la Información del Instituto se consolidará como un referente regional en la administración de las TIC, garantizando la disponibilidad, integridad y confidencialidad de la información institucional. Su gestión se orientará a la interoperabilidad de plataformas existentes en la Institución, la eficiencia en los procesos misionales y estratégicos, y la adopción de estándares tecnológicos, que fortalezcan la confianza ciudadana y la transparencia en la gestión pública.”

9.6 Líneas de Acción TIC Sectoriales.

En cumplimiento de lo dispuesto en la Resolución 1519 del 2020 (MinTIC), se dermina cinco (5) líneas de acción sectoriales orientadas a garantizar el logro de los objetivos estratégicos del sector TIC, que regulan la gestión y gobernanza de las tecnologías en entidades públicas de Colombia.

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 Instituto Municipal de Cultura y Turismo
VERSIÓN: 01		
FA: 2/09/2025	GESTIÓN TECNOLÓGICA	



Figura No. 5 Líneas de acción TIC sectorial.

Fuente: Propia de la Subdirección Administrativa y Financiera

a) En el contexto externo del Instituto se consideran todas aquellas variables externas que puedan afectar la seguridad y privacidad, tales como:

- Marco legal, regulatorio, tecnológico, económico y ambiental.
- Modificaciones o actualizaciones en políticas y normativas.
- Innovaciones y desarrollos tecnológicos.
- Opiniones, expectativas y valores de las partes interesadas externas (contratistas, proveedores, usuarios finales y entidades públicas).
- Contexto interno en materia de Seguridad Digital.

b) El contexto interno del Instituto abarca todos aquellos factores presentes dentro de la entidad que pueden influir en la gestión del riesgo de seguridad de la información. Estos elementos, que forman parte de la dinámica institucional, se detallan a continuación:

- ✓ Misión, visión y políticas institucionales.
- ✓ Estructura de gobierno, administración, organización interna, así como roles y responsabilidades.
- ✓ Políticas, objetivos y estrategias definidas para su cumplimiento.

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

- ✓ Gestión de capacidades, incluyendo recursos y conocimiento.
- ✓ Cultura organizacional.
- ✓ Sistemas, flujos de los sistemas de información y procesos de toma de decisiones.

c) Con relación a las Interfaces y dependencias del Sistema de Gestión de Seguridad de la Información (SGSI), cada proceso deberá identificar las dependencias y actividades que interactúan con otras áreas, con el propósito de garantizar la correcta aplicación del MSPI (Modelo de Seguridad y Privacidad de la Información) en la protección de los activos de información de acuerdo con lo siguiente:

- ✓ La planificación y el desarrollo del modelo ISO/IEC 27001 se llevarán a cabo conforme al modelo de procesos establecido en el Instituto, resultado de la implementación del Sistema de Gestión de la Calidad (SGC) bajo la norma NTC ISO 9001 y del Modelo Integrado de Planeación y Gestión (MIPG).
- ✓ El MSPI adoptará un enfoque basado en procesos, integrándose a la entidad mediante la aplicación del ciclo de mejora continua Planear–Hacer–Verificar–Actuar (PHVA), que establece las fases de establecimiento, implementación, operación, seguimiento, mantenimiento y mejora del sistema en materia de seguridad de la información.

9.7 Análisis DOFA.

Interno		Externo	
FORTALEZAS		OPORTUNIDADES	
F1	Existe compromiso de la Alta Dirección con la gestión y protección de la seguridad de la información.	O1	Mantener actualizada la normatividad y los estándares emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
F2	Monitoreo preventivo y continuo de las plataformas cibernéticas y de las redes que soportan la infraestructura de Tecnologías de la Información y las Comunicaciones (TIC)."	O2	Fortalecer las capacidades de coordinar con las diferentes entidades en Colombia encargados de la ciberseguridad como son el COLCERT (Centro de Respuesta a Emergencias Cibernéticas de Colombia-Grupo de Respuesta a Emergencias Cibernéticas de Colombia del Ministerio TIC y CSIRT (Computer Security Incident Response Teams-Equipos de Respuesta a incidentes de seguridad informática) para la

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

			generación y envíos de Mensajes de alertas y reportes frente a incidentes
F3	Sensibilización y formación de los usuarios finales en materia de seguridad de la información, con el fin de promover la conciencia, responsabilidad y compromiso en la protección de los activos de información institucionales.	03	Promover la adopción de mejores prácticas y controles establecidos en el Sistema de Gestión de Seguridad de la Información (SGSI), para fortalecer la confidencialidad, integridad y disponibilidad de la información de la institución.
	DEBILIDADES		AMENAZAS
D1	Asignación del personal externos para ejecutar actividades y/o obligaciones relacionadas con la creación y desarrollos de sistemas de información, lo que puede afectar la capacidad de gestión y operación del Sistema de Gestión de Seguridad de la Información (SGSI).	A1	Presencia de posibles intentos de intrusión y ciberataques dirigidos a la infraestructura tecnológica de la institución, que representan riesgos para la confidencialidad, integridad y disponibilidad de la información.
D2	Cambios en el entorno institucional que requieran modificaciones en la infraestructura tecnológica o que generen rotación de personal, pudiendo impactar la continuidad y eficacia del Sistema de Gestión de Seguridad de la Información (SGSI).	A2	Actualización o modificación de lineamientos y políticas en materia de Tecnologías de la Información y Comunicaciones (TIC) emitidas por el gobierno, que demanden ajustes en los procesos, controles y procedimientos establecidos.

Tabla No.1 Tabla Análisis DOFA- sistema de seguridad de la información

Fuente: Propia de la Subdirección Administrativa y Financiera

10. ESTRATEGIA DE SEGURIDAD DIGITAL

El Instituto Municipal de Cultura y Turismo implementará, dentro de su plan operacional de seguridad digital, una estrategia integral que articule los principios, políticas, procedimientos, manuales, formatos y plantillas necesarios, para la gestión de la seguridad de la información.

Esta estrategia tendrá como objetivo principal la adopción e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), incorporando además la Guía de Gestión

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

de Riesgos de Seguridad de la Información y los lineamientos para la Gestión de Incidentes de Seguridad, en concordancia con los requisitos establecidos en la norma ISO/IEC 27001.

En este marco, el Instituto define cinco (5) estrategias específicas que, de manera conjunta, conformarán la estrategia general del Plan Operacional de seguridad y privacidad de la información digital, orientada a garantizar la confidencialidad, integridad y disponibilidad de la información institucional.

ESTRATEGIA	DESCRIPCIÓN-OBJETIVO
Gobernanza de la seguridad de la información	El Instituto implementará el Modelo de Seguridad y Privacidad de la Información (MSPI) mediante la aprobación de la política general, el manual de seguridad digital, así como las plantillas, formatos y demás lineamientos establecidos, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de la información. Esta implementación tendrá como pilar fundamental el compromiso de la Alta Dirección, evidenciado en la definición y formalización de roles y responsabilidades en materia de seguridad de la información, asegurando su integración en los procesos institucionales y el cumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI).
Gestión de Riesgos	Determinar los riesgos de seguridad de la información integrados en el Sistema de Administración de Riesgos de la institución, con el objetivo de salvaguardar la confidencialidad, integridad y disponibilidad de la información. Esta gestión se llevará a cabo mediante procesos de planificación, identificación, análisis y valoración de riesgos, orientados a prevenir impactos potenciales. Con base en los resultados de la evaluación de riesgos, se seleccionarán los controles más adecuados para reducir, retener, evitar o transferir dichos riesgos, considerando el costo–beneficio para la institución. Finalmente, se implementará y se supervisará los planes de tratamiento de riesgos, asegurando la mitigación efectiva de las

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

	amenazas identificadas y el cumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI).
Gestión de Vulnerabilidades	Realizar un análisis continuo de vulnerabilidades sobre los sistemas, aplicaciones, redes y demás componentes que soportan los activos de información institucionales, con el fin de identificar debilidades explotables para implementar acciones de mitigación y corrección oportunas que fortalezcan la confidencialidad, integridad y disponibilidad de la información.
Socialización	Sensibilizar a los usuarios para fortalecer su conocimiento sobre las políticas, procedimientos, normas, buenas prácticas y demás lineamientos relacionados con la seguridad de la información, promoviendo una cultura de ciberseguridad sólida en la institución, que se conviertan en hábitos permanentes, asegurando que cada actor comprenda y asuma su rol y responsabilidades dentro del Modelo de Seguridad y Privacidad de la Información
Aplicación de Controles	Implementar las estrategias y actividades necesarias para garantizar el cumplimiento de los controles técnicos y administrativos definidos, orientados a alcanzar los objetivos de seguridad de la información, con el propósito de fortalecer la seguridad institucional, asegurando la protección de la confidencialidad, integridad y disponibilidad de los activos de información.

Tabla No.2 Estrategia de Seguridad de Información Digital

Fuente: Propia de la Subdirección Administrativa y Financiera

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		



Figura No. 6 Estrategia de Seguridad de Información Digital

Fuente: Propia de la Subdirección Administrativa y Financiera

10.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS

A continuación, se presenta el objetivo de cada estrategia específica a implementar, asegurando que las actividades estén alineadas con lo establecido en el Plan de Operación del Modelo de Seguridad y Privacidad de la Información (MSPI).

10.2 PORTAFOLIO DE PROYECTOS Y ACTIVIDADES

Para cada estrategia específica, el Instituto Municipal de Cultura y Turismo define los proyectos, actividades y productos esperados, orientados a garantizar la implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), en conformidad con los principios de confidencialidad, integridad y disponibilidad de la información.

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

ESTRATEGIA	PROYECTO	PRODUCTO
Gobernanza de la seguridad de la información	Generar la documentación relacionada con la seguridad de la Información.	Actualización de procedimientos, manual. plantillas, formatos y/o instructivos de seguridad de la información.
Gestión de Riesgos	Definir planes de tratamiento de riesgos de seguridad	Elaborar un mapa de riesgos de seguridad digital
Gestión de Vulnerabilidades	Formalizar la actualización del procedimiento de Gestión de vulnerabilidad de seguridad de la información.	Elaborar un Análisis de riesgo asociado a vulnerabilidades
Socialización	Realizar jornadas de sensibilización a todo el personal.	Plan de Sensibilización Evidencias de las actividades desarrolladas
Aplicación de Controles	Realizar investigación de nuevas herramientas tecnológicas que mejoren la infraestructura de seguridad digital.	Ejercer monitoreo y revisión de logs de los activos de información. Adquisición de herramientas de protección y actualización de licencias

11. PROYECCION DE COSTOS

Con base en los proyectos definidos dentro de la estrategia para la aplicación de controles, se presenta la estimación de costos elaborada a partir de estudios de mercado, con el fin de facilitar su análisis, consideración y evaluación de viabilidad técnica, financiera y operativa.

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

AÑO 2025			
PROYECTO	CANTIDAD	PERIODO DE RENOVACIÓN	INVERSIÓN
Discos duros y Kits de Mantenimiento de la Red de datos	1	Anual	\$15.018.821
DIGICOWEB (EMPRESA Software de Correspondencia)	1	Triannual	\$5.500.000
Software de catalogación Bibliográfica (Janium) (Funcionamiento Vence en noviembre 2025)	1	Anual	\$30.000.000
Sistema Financiero (GD/DELFIN) Nueva Implementación	1	Anual	\$15.500.000
Implementación de nuevas licencias de antivirus (4 Paquetes)	1	Trienio	195.000.000
Suscripción + implantación Fortinet	1	Anual	
Firewall Fortinet	1	Anual	
Licencias Office 365	103	Anual	\$ 20.692.000
Renovación de licencias de Creative cloud (Adobe audition) Versión Empresarial	3	Anual	\$ 12.119.400
✓ Canal de Internet dedicado simétrico 500MB ✓ Internet asimétrico 60M + línea telefónica local CCO-EMA ✓ Línea telefónica ✓ Troncal SIP ✓ Internet asimétrico 60M- Sedes Metrolibro, CCO, Casa L. Perú Valor Mensual \$4.291.891	1	Anual	\$51.502.692
Adquisición de Computadores portátiles para procesos móviles (donados Por la Gobernación)	3	Anual	\$12.000.000
Mantenimiento del Sistemas Alarma Contra Incendio	1	Anual	\$25.900.000
Internet Dedicado 30 Mbps- Estación del tren Café Madrid (V Mensual \$1.677.023.000)	1	Anual	\$20.124.276
Transición IPV4 A IPV6	1	Triannual	

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

AÑO 2026			
PROYECTO	CANTIDAD	PERIODO DE RENOVACIÓN	INVERSIÓN
Adquisición e implementación de switches de última generación, diseñados para garantizar alto desempeño, escalabilidad y administración centralizada de la red, que cumplan con la compatibilidad nativa del firewall Fortinet, que permita integrar de forma segura la segmentación de tráfico, la aplicación de políticas de seguridad, el monitoreo unificado y la optimización del rendimiento en la infraestructura de comunicaciones de la entidad."	1	Triannual	\$90.000.000
Adquisición de puntos de acceso inalámbricos (AP) de última generación, que cumplan con la compatibilidad nativa del firewall Fortinet.	1	Triannual	\$60.000.000
Implementación de un sistema de control de acceso mediante talanqueras y dispositivos en oficinas, orientados al registro seguro de funcionarios y visitantes, así como al control y validación de autorizaciones de ingreso.	1	Triannual	\$50.000.000
DIGICOWEB (EMPRESA Software de Correspondencia	1	Triannual	\$6.050.000
Software de catalogación Bibliográfica (Janium) (Funcionamiento	1	Anual	\$33.000.000
Sistema Financiero (GD/DELFIN) Nueva Implementación	1	Anual	\$15.500.000
Licencias Office 365	103	Anual	\$ 22.761.200
Renovación de licencias de Creative cloud (Adobe audition) Versión Empresarial	3	Anual	\$ 13.331.340
✓ Canal de Internet dedicado simétrico 500MB ✓ Internet asimétrico 60M + línea telefónica local CCO-EMA ✓ Línea telefónica ✓ Troncal SIP ✓ Internet asimétrico 60M- Sedes Metrolibro, CCO, Casa L. Perú Valor Mensual \$4.291.891	1	Anual	\$56.652.962
Internet Dedicado 30 Mbps- Estación del tren Café Madrid (V Mensual \$1.677.023.000)	1	Anual	\$22.136.704
Proyecto de Transformación Digital orientado al proceso de implementación de un sistema de información de gestión documental y	1	Anual	

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

automatización de procesos, que facilita la transición del manejo tradicional en papel hacia un entorno digital, eficiente y seguro en el cumplimiento de la Ley 594 de 2000 (Ley General de Archivos), la Ley 1712 de 2014 (Transparencia y Acceso a la Información Pública) y la política de Cero Papel. ✓ Servidor Laserfiche ✓ Licencia de software ✓ Instalación y capacitación: ✓ Soporte anual			\$117.950.600
Transición IPV4 A IPV6. Adquisición del Pool IP LACNIC Desde a /48 hasta /35 inclusive https://www.lacnic.net/2397/1/lacnic/categorias-y-cuotas-de-asociados	1	Triannual	USD 2.500

12. LIDERAZGO

La Dirección demuestra su compromiso con el Plan Operacional de Modelo de Seguridad y Privacidad de la Información (MSPI), asegurando el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información, mediante las siguientes acciones:

- a) Definición de objetivos y política: Establecer, dentro del Plan Operacional de Seguridad y Privacidad de la Información, los objetivos y la política de seguridad de la información, en coherencia con la dirección estratégica de la institución.
- b) Integración en los procesos: Garantizar que los requisitos del Plan Operacional del MSPI se integren de manera efectiva en los procesos institucionales.
- c) Asignación de recursos: Mantener la disponibilidad de los recursos humanos, técnicos y financieros necesarios para la operación, mantenimiento y mejora del MSPI.

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

- d) Comunicación y concienciación: Promover la importancia de una gestión eficaz de la seguridad digital y del cumplimiento de los requisitos del MSPI en todos los niveles de la institución.
- e) Cumplimiento de resultados previstos: Velar porque el MSPI alcance los objetivos y resultados establecidos.
- f) Dirección y apoyo al personal: Guiar y respaldar a todas las personas involucradas, fomentando su participación activa y contribución a la eficacia y mejora continua del MSPI.
- g) Promover la mejora continua

En el Manual de Seguridad Digital del Instituto Municipal de Cultura y Turismo de Bucaramanga (IMCT) se establecen los lineamientos fundamentales, entre ellos el liderazgo y compromiso de la Dirección, así como la definición de una política de seguridad de la información alineada con el propósito, la dirección estratégica y los objetivos institucionales, en concordancia con los requisitos del Modelo de Seguridad y Privacidad de la Información (MSPI) y del Sistema de Gestión de Seguridad de la Información (SGSI).

13. PLANEACIÓN

El Instituto Municipal de Cultura y Turismo de Bucaramanga, mediante la aplicación del Procedimiento para el Inventario y Clasificación de Activos de Información, implementa una metodología estandarizada para la identificación, clasificación y valoración de dichos activos.

Este proceso se desarrolla de manera unificada con el Formato de Registro de Inventarios para la Gestión y Clasificación de Activos de Información, garantizando la consistencia de los registros, el control de los activos y su adecuada protección en concordancia con los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI).

14. SOPORTE

Para el desarrollo de todas las actividades relacionadas con el Modelo de Seguridad y Privacidad de la Información (MSPI), el Instituto Municipal de Cultura y Turismo de Bucaramanga (IMCT) cuenta con el respaldo de la Alta Dirección y con un proceso

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

sistemático, documentado, el cual es de conocimiento institucional y garantiza su correcta implementación.

15. FASE DE IMPLEMENTACIÓN

a. Planificación y Control

El Instituto, a través de su Sistema de Gestión de Riesgos, planifica, implementa y controla los procesos necesarios para garantizar el cumplimiento de los requisitos de seguridad y privacidad de la información, asegurando la ejecución de las acciones definidas en el Plan de Tratamiento de Riesgos.

Toda la información deberá ser documentada en el aplicativo del Sistema de Gestión de Calidad, el cual respalda y centraliza los procesos, permitiendo verificar el cumplimiento de lo planificado.

Adicionalmente, la institución cuenta con un procedimiento formal de control de cambios, que establece las acciones necesarias para mitigar efectos adversos cuando sea requerido.

En el Manual de Seguridad se detallan los controles aplicables, en concordancia con los lineamientos establecidos en la norma ISO 27001.

b. Implementación del Plan de Tratamiento de Riesgos

El Instituto Municipal de Cultura y Turismo de Bucaramanga cuenta con un Plan de Tratamiento de Riesgos de Seguridad de la Información, implementado conforme a lo establecido en el Sistema de Administración de Riesgos. Este plan identifica los controles de seguridad requeridos para reducir los riesgos a niveles aceptables, en alineación con la Declaración de Aplicabilidad y la política de seguridad institucional.

c. Indicadores de Gestión

En el marco del Plan de Acción Institucional, se han definido indicadores de gestión que permiten evaluar:

- La disponibilidad y continuidad de los servicios.
- El nivel de madurez del Modelo de Seguridad y Privacidad de la Información del Instituto.

d. Fase de Evaluación del Desempeño

El seguimiento y monitoreo del Modelo de Seguridad de la Información se realiza con base en los resultados de los indicadores definidos, asegurando la verificación de la eficacia de

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

las acciones implementadas. Para garantizar la mejora continua, se establece la obligación de:

- Elaborar un informe semestral de seguimiento y revisión del Modelo de Seguridad.
- Incluir en el Plan Anual las auditorías internas y revisiones independientes.
- Implementar mecanismos de detección y prevención de incidentes de seguridad mediante el uso de indicadores clave.

e. Tareas específicas:

Revisar semestralmente la efectividad del Plan Operacional del Modelo de Seguridad y Privacidad de la Información, considerando:

- ✓ Cumplimiento de la política y objetivos.
- ✓ Resultados de las mediciones (Indicadores y métricas: niveles de cumplimiento)
- ✓ Sugerencias y observaciones de las partes interesadas.
- ✓ Medir la efectividad de los controles en cada proceso, verificando que cumplan con los objetivos de mitigación de riesgos establecidos.
- ✓ Programar auditorías internas del Modelo de Seguridad y Privacidad de la Información, a cargo de la Oficina Asesora de Control Interno de Gestión.
- ✓ Revisar periódicamente el estado de los activos de información, actualizando los procesos institucionales y los formatos de registro de inventario de activos (Gestor de Riesgo de Seguridad de la Información).

16. CONSULTA, DIVULGACIÓN Y ACTUALIZACIÓN DEL PLAN DE OPERACIONES

El Mapa de Riesgos de Seguridad de la Información está integrado al Sistema de Administración de Riesgos del Instituto Municipal de Cultura y Turismo de Bucaramanga, actuando como herramienta clave para facilitar los procesos de gestión de riesgos de seguridad de la información en todas las áreas de la institución.

En el proceso de consulta participan los líderes responsables de la ejecución de los procesos institucionales. Asimismo, todos los documentos asociados al Plan Operacional del Modelo de Seguridad y Privacidad de la Información deben mantenerse publicados en un repositorio controlado de la Entidad, garantizando su disponibilidad para consulta y actualización.

La divulgación del plan se realizará mediante los canales institucionales oficiales, tales como el correo electrónico corporativo y la intranet, asegurando que la información llegue de manera oportuna y segura a todos los funcionarios.

17. MONITOREO Y REVISIÓN DEL PLAN

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

El Plan de Seguridad y Privacidad de la Información del Instituto Municipal de Cultura y Turismo (IMCT) será objeto de revisión semestral, previa a la formulación de los planes anuales por parte de la Subdirección Técnica – Área de Sistemas.

Adicionalmente, el plan podrá ser actualizado en cualquier momento cuando se identifiquen cambios normativos, tecnológicos, organizacionales o de riesgos que lo ameriten, garantizando así su vigencia, pertinencia y efectividad.

18. SEGUIMIENTO AL PLAN DE TRABAJO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Subdirección Técnica del Instituto Municipal de Cultura y Turismo (IMCT), a través del Área de Sistemas, elaborará un informe semestral de seguimiento y control sobre la implementación del Modelo de Seguridad y Privacidad de la Información.

Dicho informe estará dirigido a la Dirección y se sustentará en los reportes de gestión de seguridad de la información emitidos por cada uno de los procesos institucionales, con el fin de evaluar avances, identificar brechas y proponer acciones de mejora.

19. GLOSARIO

- **Activos de la información:** Todo recurso que posea valor para el Instituto y requiera protección. Incluye información en formato físico o digital, tales como bases de datos, documentos, manuales, software, hardware, así como servicios informáticos y de telecomunicaciones. También comprende activos intangibles, como la imagen institucional y el material publicitario.
- **Análisis de riesgos:** Proceso sistemático que utiliza información disponible para identificar amenazas y vulnerabilidades, y estimar el nivel de riesgo que estas representan para la seguridad de la información.
- **Confidencialidad:** Propiedad de la información que garantiza que esta no sea puesta a disposición ni revelada a personas, entidades o procesos no autorizados.
- **Declaración de aplicabilidad (SoA – Statement of Applicability):** Documento que describe los objetivos de control y los controles relevantes para el Modelo de Seguridad y Privacidad de la Información de la organización, determinados con base en los resultados de la evaluación de riesgos, requisitos legales o reglamentarios, obligaciones contractuales y necesidades de la entidad.

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

- Disponibilidad: Propiedad de la información que asegura que esta sea accesible y utilizable por personas, entidades o procesos autorizados en el momento requerido.
- Entrenamiento: Proceso orientado a desarrollar y reforzar habilidades específicas para que una persona pueda desempeñar eficazmente las funciones asignadas a su cargo.
- Estado de un sistema: Condición o situación en la que se encuentra un sistema en un momento determinado, resultado de su operación, configuración y entorno.
- Evaluación de riesgos: Proceso integral que comprende el análisis y la estimación de los riesgos para determinar su nivel y priorizar su tratamiento.
- Evento de seguridad de la información: Ocurrencia identificada en un sistema o servicio que pueda indicar una posible violación de las políticas o controles de seguridad, o una situación desconocida que pueda ser relevante para la protección de la información.
- Gestión de riesgos: Conjunto de actividades coordinadas para dirigir y controlar la organización con respecto a los riesgos de seguridad de la información.
- Incidente de seguridad de la información: Uno o más eventos de seguridad no deseados o inesperados que tienen una alta probabilidad de comprometer la confidencialidad, integridad o disponibilidad de la información.
- Integridad: Propiedad que salvaguarda la exactitud, consistencia y completitud de los activos de información.
- Mapa de riesgos: Herramienta que permite inventariar y describir de forma ordenada y sistemática los riesgos identificados, sus características, consecuencias y probabilidad de materialización.
- Modelo de Seguridad y Privacidad de la Información (MSPI): Estructura de gestión que asegura la preservación de la confidencialidad, integridad y disponibilidad de la información, así como la privacidad de los datos, mediante la aplicación de procesos de gestión de riesgos que generen confianza en las partes interesadas.
- Plan de mitigación: Plan preventivo que define las acciones necesarias para reducir la probabilidad de ocurrencia o el impacto de un riesgo identificado.
- Política: Declaración de alto nivel que establece los principios, objetivos y directrices de la organización frente a un tema específico.

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

- **Procesos:** Conjunto estructurado de actividades o fases interrelacionadas que transforman insumos en resultados para cumplir un objetivo definido.
- **Riesgo:** Posibilidad de que un evento o circunstancia afecte negativamente el cumplimiento de los objetivos o el desempeño de los procesos institucionales.
- **Seguimiento:** Acción de verificar periódicamente el estado de avance y cumplimiento de las actividades y acciones establecidas en un plan o programa.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, así como de otras propiedades asociadas como autenticidad, trazabilidad, fiabilidad y no repudio.
- **Sensibilización:** Proceso que busca generar conciencia, modificar conductas o reforzar buenas prácticas sobre un tema específico, en este caso, la seguridad de la información.

20. REFERENCIAS BIBLIOGRAFICAS

20.1 Fuentes Bibliográficas

Referencias Bibliográficas

ISO/IEC 27001:2022 – Sistemas de gestión de seguridad de la información (ISMS): marco internacional que define los requisitos para establecer, implementar, mantener y mejorar un SGSI, con énfasis en la protección de la confidencialidad, integridad y disponibilidad de la información.

ISO/IEC 27001 Anexo A – Controles de seguridad (2022): abreviado a 93 controles agrupados en cuatro categorías (organización, personas, físico y tecnológico), permite seleccionar medidas específicas para abordar los riesgos identificados.

Gestión de seguridad de la información: define cómo se gestionan los controles para proteger la confidencialidad, disponibilidad e integridad frente a amenazas y vulnerabilidades mediante la gestión de riesgos, respaldada por estándares como ISO/IEC 27001, 27002 y 27035.

ISO/IEC 27001 – Términos y definiciones (Wikipedia): proporciona una visión general estructural de los componentes del estándar, como cláusulas (contexto, liderazgo, planificación, evaluación del desempeño, etc.)

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

ISO/IEC 27001:2013 – Sistema de Gestión de la Seguridad de la Información (SGSI). Norma internacional que establece los requisitos para implementar, mantener y mejorar de forma continua un sistema de gestión que garantice la confidencialidad, integridad y disponibilidad de la información.

Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas – Modelo Nacional de Gestión de Riesgo de Seguridad de la Información establece directrices para que las entidades públicas en Colombia gestionen de manera integral los riesgos asociados al uso y protección de la información..

ISO/IEC TR 18044:2004– Tecnología de la Información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad de la Información. Informe técnico que establece directrices para la detección, reporte, evaluación y tratamiento de incidentes de seguridad de la información, con el fin de minimizar su impacto, preservar la integridad, disponibilidad y confidencialidad de los activos, y garantizar la continuidad de las operaciones.

ISO/IEC Guide 73 – Gestión de Riesgos – Vocabulario. Guía que proporciona definiciones y términos estandarizados relacionados con la gestión de riesgos, con el objetivo de unificar el lenguaje y facilitar la comprensión y aplicación coherente de los principios y procesos de gestión de riesgos en diferentes organizaciones y sectores.

20.2 Fuentes de la Entidad

Manual de seguridad de la Información de la IMCT

Mapa de Riesgos de Seguridad de Información

TABLA DE REFERENCIA DE DOCUMENTOS CONSULTADOS				
DOCUMENTOS DE REFERENCIA				
TIPO DE DOCUMENTO	TÍTULO DEL DOCUMENTO	CÓDIGO	ORIGEN	
			Externa	Interna
ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems — Requirements		x	
Documento técnico–normativo elaborado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)	Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas		x	
ISO/IEC 18044:2004	Information technology - Security techniques - Information security incident management		x	

CÓDIGO: GT-PL-10	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMCT	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 2/09/2025	GESTIÓN TECNOLÓGICA		

Guía ISO/CEI 73 Gestión de riesgos – Terminología	Gestión de riesgos – Terminología – Líneas directrices para el uso en las normas		x	
--	--	--	---	--

21. CONTROL DE CAMBIOS

CAMBIOS DE VERSIONES						
ELABORACIÓN Y/O ACTUALIZACIÓN DEL DOCUMENTOS CONTROL DE CAMBIOS						
VERSIÓN	FECHA DE APROBACIÓN			DESCRIPCIÓN DEL CAMBIO		
	DD	MM	AAAA			
01	2	09	2025	Elaboración inicial del documento		
ELABORÓ Y/O ACTUALIZÓ			PROCESO RESPONSABLE			
Gabriel Arguello Castro			Gestión Tecnológica			
Alid María Lindarte Rincón			Subdirectora Administrativa y Financiera			
REVISIÓN TECNICA SGC						
NOMBRES Y APELLIDOS			DEPENDENCIA RESPONSABLE			
Yeimis Vásquez Torres			Subdirección Técnica, Proceso de Gestión Integral			
APROBÓ (RESPONSABLE DEL PROCESO)						
NOMBRES Y APELLIDOS			CARGO		FECHA	
					DD	MM
Alid María Lindarte Rincón			Subdirectora Administrativa y Financiera		2	09 2025
APROBÓ POR LA ALTA DIRECCIÓN- COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO “Si aplica”						
NÚMERO DE ACTA			N°.		FECHA	