PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

GESTIÓN TECNOLÓGICA

INSTITUTO MUNICIPAL DE CULTURA Y TURIMSO DE BUCARAMANGA

2024

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El instituto Municipal d cultura y turismo de Bucaramanga como entidad del sector público de orden descentralizado acoge las directrices de la política de gobierno y seguridad digital dados para la integración de sus planes institucionales y estratégicos, y teniendo presente que en el que hacer de sus actividades se utiliza y fomenta la utilización de recursos tecnológicos e informáticos en sus procesos misionales y administrativos en pro de fortalecer la naturaleza pública de sus servicios para el bienestar de los ciudadanos.

La incorporación de determinadas Tecnologías de Información y Comunicación en los procesos misionales y administrativos requieren la aplicación de controles selectivos con el fin de garantizar la integralidad de la información, la confidencialidad de los datos y la disponibilidad de los servicios que se ofrecen por medio de las tecnologías de la información y computación; por lo anterior, requiere implementar un plan de estratégico de seguridad de la información alineado a las políticas y planes del instituto, sus procesos y actividades.

2. OBJETIVO

Definir el plan estratégico de seguridad de la información (PESI) del instituto Municipal de cultura y Turismo de Bucaramanga, para la transformación y fortalecimiento de la seguridad de la información de la entidad alineada a las nuevas tendencias, que permitan la respuesta efectiva y oportuna ante los nuevos retos en esta materia, lo cual permitirá fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2024-2027.

2.1 OBJETIVOS ESPECÍFICOS

- Presentar el estado actual del estado de seguridad de la información basado en el Modelo de Seguridad y privacidad de la información (MSPI) del MinTIC.
- Establecer indicadores que permitan establecer el estado de madurez de la seguridad de la información.
- Definir y establecer la estrategia de seguridad digital de la entidad.
- Definir y establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información.

- Definir y priorizar los procesos a implementar para la correcta implementación del SGSI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.

3. ALCANCE

El Plan Estratégico de Seguridad de la Información tiene como finalidad crear la estrategia y determinar los controles pertinentes para la protección de la información de todos los procesos y activos de información generados por estos, dentro de los marcos de la normatividad vigente, estándares y lineamientos impartidos por el MinTIC.

El instituto Municipal de cultura, cumple con los tres pilares de la seguridad de la información en preservar la integridad, confidencialidad y disponibilidad de la información:

- Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados.
- Confidencialidad: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado.
- Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos.

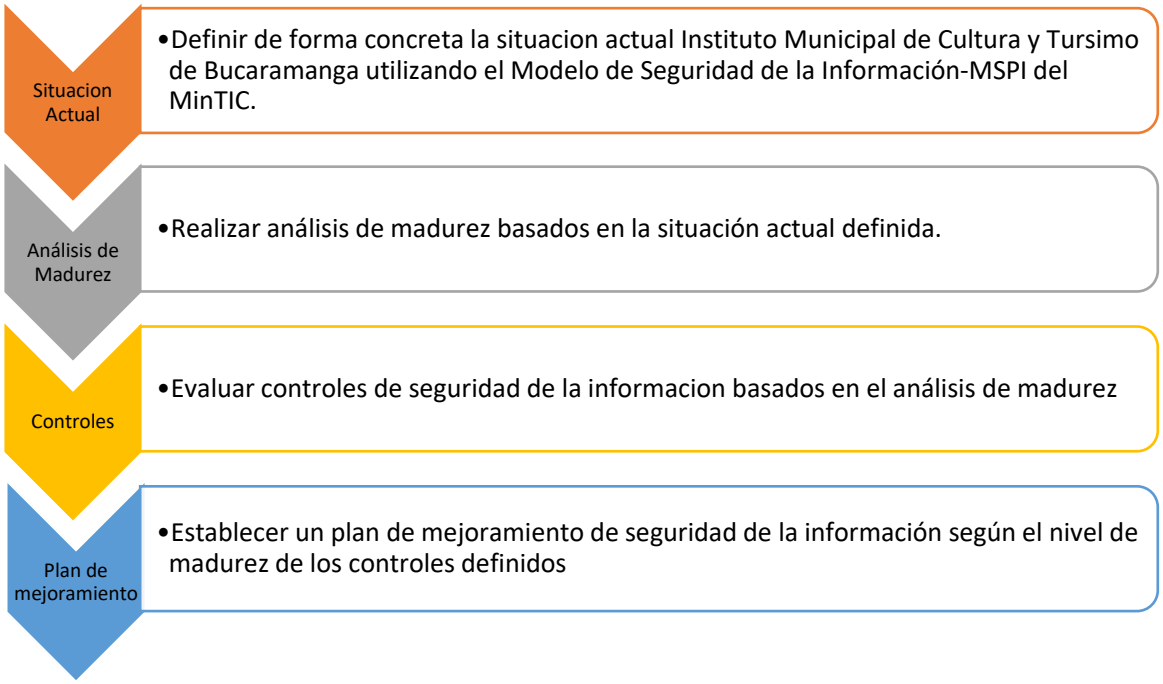
4. DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- 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 (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- Resolución 500 de 2021. "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*".
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.

- Ley 527/99 “Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos”
- Ley 1266/08 “Por la cual se dictan 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”.
- Ley 1581/12 “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.
- Decreto 1499 del 11 de septiembre de 2017 Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión
- Decreto 612 del 04 de abril 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.
- Decreto 1008 del 14 de junio de 2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

5. METODOLOGÍA



6. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para en análisis de la situación actual, la entidad utilizo la herramienta de autodiagnóstico del modelo de seguridad de la información-MSPI suministrado por el MinTIC, el cual imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital (Gobierno Digital - MSPI, 2013).

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad.

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un

proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

En este sentido, de forma paralela y conjunto con control interno de la entidad se evaluó el nivel de madurez del modelo de seguridad y privacidad de la información del imct, a través de la aplicación del Instrumento de Evaluación del Modelo de Seguridad y Privacidad de la Información – MSPI – anterior mente mencionado.

Respecto a la evaluación de la efectividad de los controles se evidenció la siguiente calificación, teniendo en cuenta la tabla de escala de valoración de controles.

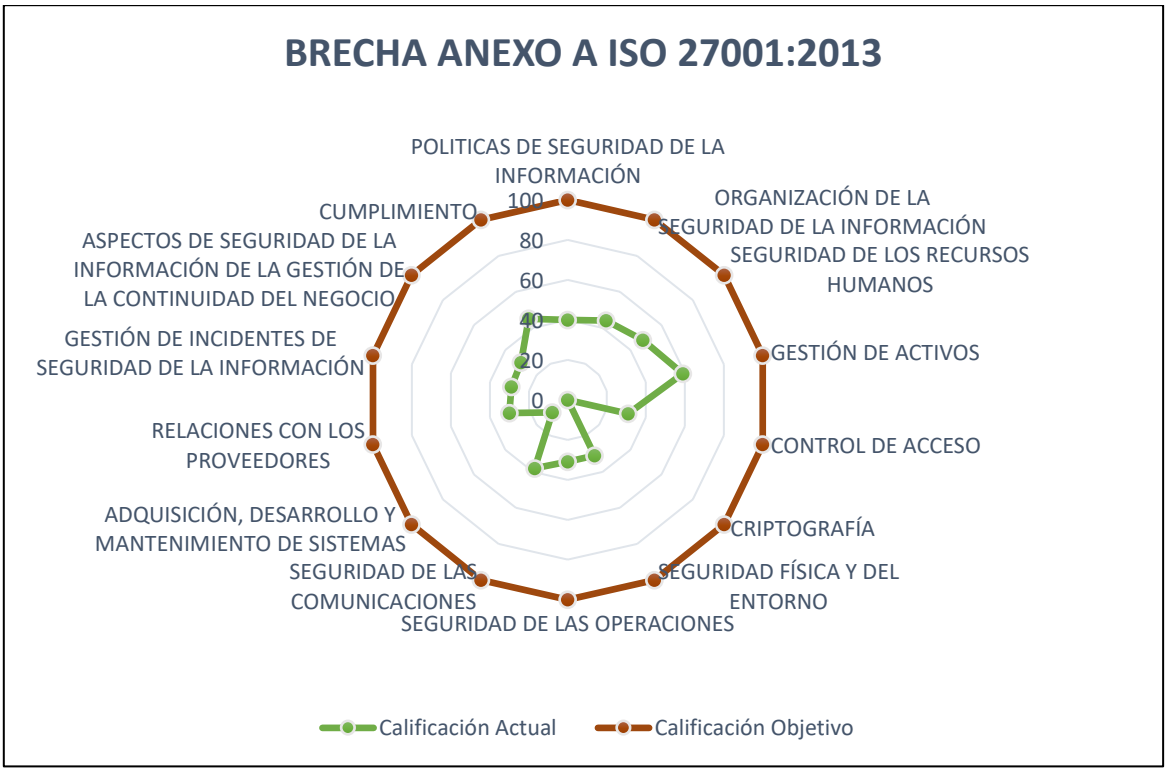
Tabla de Escala de Valoración de Controles ISO 27001:2013 ANEXO A

Descripción	Calificación	Criterio
No Aplica	N/A	No aplica.
Inexistente	0	Total, falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

A continuación, se presentan los resultados obtenidos de acuerdo con las líneas base de seguridad del Modelo de Seguridad de la información – MSPI:

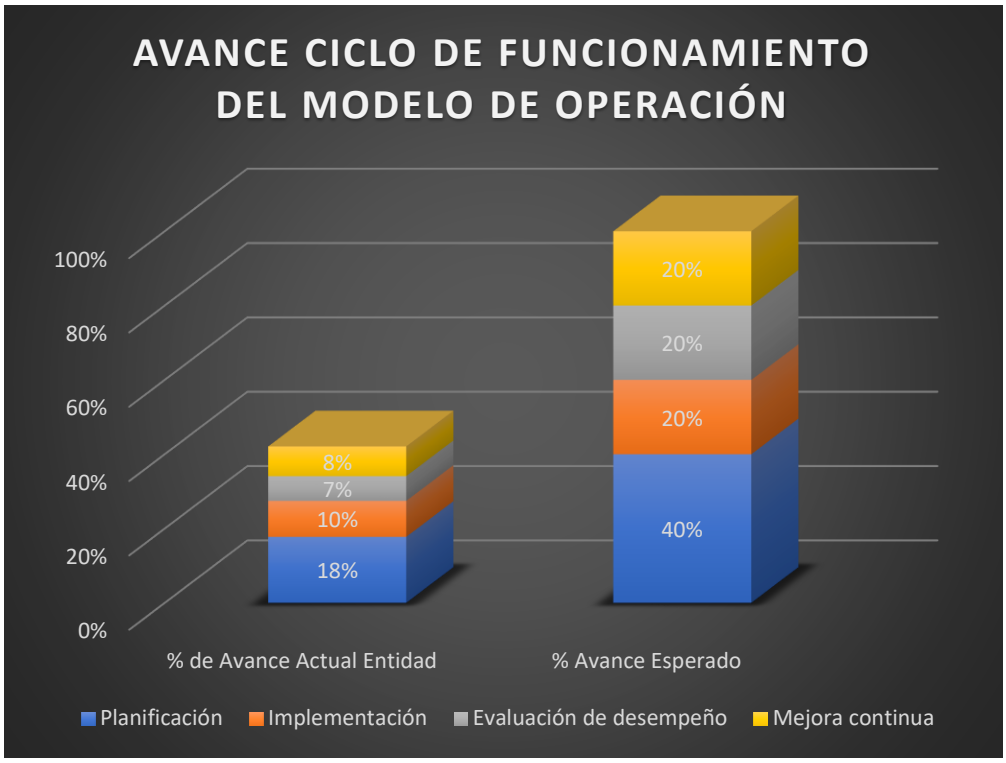
6.1. EVALUACIÓN DE EFECTIVIDAD DE CONTROLES

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	40	100	**REPETIBLE**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	44	100	**EFECTIVO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	48	100	**EFECTIVO**
A.8	GESTIÓN DE ACTIVOS	59	100	**EFECTIVO**
A.9	CONTROL DE ACCESO	31	100	**REPETIBLE**
A.10	CRIPTOGRAFÍA	0	100	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	31	100	**REPETIBLE**
A.12	SEGURIDAD DE LAS OPERACIONES	31	100	**REPETIBLE**
A.13	SEGURIDAD DE LAS COMUNICACIONES	38	100	**REPETIBLE**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	10	100	**INICIAL**
A.15	RELACIONES CON LOS PROVEEDORES	30	100	**REPETIBLE**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	29	100	**REPETIBLE**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	30	100	**REPETIBLE**
A.18	CUMPLIMIENTO	45	100	**EFECTIVO**
PROMEDIO EVALUACIÓN DE CONTROLES		**33**	**100**	**REPETIBLE**



6.2. AVANCE CICLO DE DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**
2023	Planificación	18%	40%
	Implementación	10%	20%
	Evaluación de desempeño	7%	20%
	Mejora continua	8%	20%
TOTAL		**42%**	**100%**



6.3. NIVEL DE MADUREZ DEL MSPI

Respecto del nivel de madurez de modelo de seguridad y privacidad de la información se observó el siguiente resultado, teniendo en cuenta las siguientes escalas de calificación:

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

	NIVEL DE CUMPLIMIENTO
Inicial	SUFICIENTE
Repetible	INTERMEDIO
Definido	CRÍTICO
Administrado	CRÍTICO
Optimizado	CRÍTICO

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

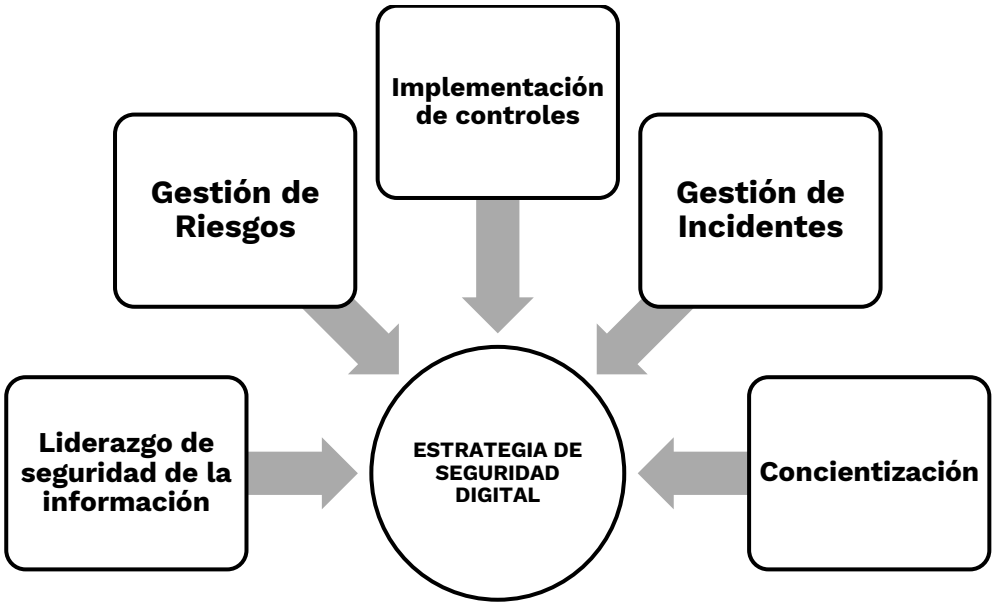
Los Resultados obtenidos referente a al nivel de madurez, se configura de acuerdo con el MSPI que “NO LACANZA EN NIVEL INICIAL”.

De acuerdo con el autodiagnóstico obtenido, se evidencia que, si bien el instituto municipal de cultura y turismo a identificado y reconoce las falencias frente a la seguridad y privacidad de la información, carece de procesos y procedimiento formalmente establecidos los existentes no son debidamente documentados, ni comunicados, hay un alto grado de confianza en los conocimientos de cada persona los controles de seguridad y son principalmente reactivos según la incidencia que se presente.

7. ESTRATEGIA DE SEGURIDAD DIGITAL

El Instituto Municipal de Cultura y Turismo, establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse (*Ver Resolución 500 de 2021*).

Por tal motivo, se define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



7.1. DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
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.
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 tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	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.
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.

7.2. PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, se definen los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	**PROYECTO 1:** Desarrollar e implementar una política de seguridad, en esta se debe incluir políticas de uso de activos de información, controles de acceso y políticas de seguridad física y el entorno. **PROYECTO 2:** Desarrollar e implementar una política de continuidad del negocio.	Política de Seguridad Formalizada e Implementada. Política de continuidad de negocios. Procesos y procedimientos definidos, estandarizados, y formalizados.
Gestión de riesgos	**PROYECTO 1:** Identificar, valorar y clasificar los riesgos asociados a los activos de información **PROYECTO 2:** Definir y/o actualizar planes de tratamiento de riesgos de seguridad	Matriz de riesgos de seguridad digital Planes de tratamiento de riesgos actualizados.
Concientización	**PROYECTO 1:** Establecer desde el inicio de cada año la planeación de sensibilización sobre seguridad para todo el año, la cuales deben quedar en el plan de capacitaciones de la entidad. **PROYECTO 2:** Realizar jornadas de sensibilización a todo el personal.	1. Plan de Sensibilización o plan de capacitaciones. 2. Evidencias de las actividades desarrolladas 3. Certificaciones o listados de asistencias de cursos, charlas, talleres, etc. 4. Resultado de las encuestas de medición

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
	PROYECTO 3: Medir el grado de sensibilización a toda la Entidad.	
Implementación de controles	**CONTROL 1** Política de respaldos de información. **CONTROL 2** Procedimiento de Gestión de Cambios. **CONTROL 3** Inventario y clasificación de los activos de la información.	Política de respaldos de información. Procedimiento de Gestión de Cambios. Clasificación de la información.
Gestión de incidentes	**PROYECTO 1:** Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información. **PROYECTO 2:** Capacitar al personal en la gestión de incidentes de seguridad de la información.	1. Procedimiento de gestión de incidentes de seguridad formalizado. 2. Sesiones de capacitación desarrolladas.

7.3. CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

El responsable de seguridad de la información, con base a los proyectos definidos en la sección anterior, se establece un cronograma de actividades donde se evidencie como se llevarán a cabo cada uno de los proyectos previstos. Las actividades se desarrollan de forma secuencial o paralela según se considere.

ESTRATEGIAS	PROYECTOS	AÑOS 2024				AÑO 2025			
		T1	T2	T3	T4	T1	T2	T3	T4
Liderazgo de seguridad de la información	Desarrollar una política de seguridad, en esta se debe incluir políticas de uso de activos de información, controles de acceso y políticas de seguridad física y el entorno.		■			■			
	Desarrollar e implementar una política de continuidad del negocio.			■					
Gestión de riesgos	Identificar, valorar y clasificar los riesgos asociados a los activos de información				■				
	Definir y/o actualizar planes de tratamiento de riesgos de seguridad				■				■
Concientización	Establecer desde el inicio de cada año la planeación de sensibilización sobre seguridad para todo el año, la cuales deben quedar en el plan de capacitaciones de la entidad.	■				■			
	Realizar jornadas de sensibilización a todo el personal			■	■	■	■	■	
	Medir el grado de sensibilización a toda la Entidad.				■				■
Implementación de controles	Política de respaldos de información.				■				
	Inventario y clasificación de los activos de la información.			■		■			
Gestión de incidentes	Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información.				■		■		
	Capacitar al personal en la gestión de incidentes de seguridad de la información			■			■		

Nota: Al finalizar cada vigencia, se realizará una actualización del cronograma, incorporando el estado del avance de los proyectos formulados y si en efecto se cumplieron o se plantean aplazamientos para las vigencias posteriores. Así mismo, el cronograma podrá ser modificado o ajustado de acuerdo con las necesidades o situaciones que surjan en la entidad.

8. ANÁLISIS PRESUPUESTAL

El presupuesto destinado para las actividades y proyectos de seguridad y privacidad de la información de instituto municipal de cultura y turismo de Bucaramanga se define anualmente por medio del plan de adquisiciones, en conjunto con los jefes de área y directivos, por lo cual todo lo relacionado con el presupuesta deberá ser validado en el plan de adquisiciones y que será parte integral del presente documento.

9. RESPONSABLES

1. Representante Legal de la Entidad: Aprobar los documentos de Alto Nivel
2. Subdirección administrativa y financiera: Velar por la implementación del MSPI y garantizar los recursos requeridos.
3. Departamento de sistemas: apoyar la ejecución u apropiación del MSPI.
4. Responsable de departamento de sistemas: Coordinar las actividades de implementación del MSPI

RELACIÓN DE VERSIONES

DOCUMENTO NUEVO		
VERSIÓN	**FECHA**	**CAMBIOS**
01	18/05/2023	Documento anteriormente denominado con el código GAF-O-07
02	31/01/2024	Ajuste auditoria control interno MSPI
DOCUMENTO ANTIGUO		
VERSIÓN	**FECHA**	**CAMBIOS**
01	23/03/2023	Creación del documento.
Para mayor información sobre este documento, dirigirse a la dependencia que lo elaboró:		
Dependencia: Gestión tecnológica.		