PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - PESI 2025

ALCALDIA DE BUCARAMANGA

OFICINA ASESORA TIC

TABLA DE CONTENIDO

1. OBJETIVO

Fortalecer la seguridad de la información para el periodo 2025 del Municipio de Bucaramanga, mediante la implementación de políticas, procesos y controles eficaces que aseguren la confidencialidad, integridad y disponibilidad de los activos de información, garantizando un entorno seguro frente a riesgos y amenazas cibernéticas, y promoviendo una cultura organizacional de gestión responsable de la información.

2. OBJETIVOS ESPECÍFICOS

- Alinear la estrategia de Seguridad de la Información con las metas y objetivos del Municipio de Bucaramanga para el periodo 2025.

- Establecer iniciativas y actividades claras para el cumplimiento y fortalecimiento de la estrategia de Seguridad de la Información.

- Definir e implementar medidas técnicas y administrativas que aseguren la protección continua de los activos de información.

- Planificar y realizar el seguimiento de los controles de seguridad implementados para garantizar la efectividad del plan estratégico.

- Asegurar el compromiso de la alta dirección mediante su apoyo en la implementación de la estrategia de seguridad de la información.

- Identificar, evaluar y gestionar los riesgos de seguridad de la información para mitigar posibles amenazas y vulnerabilidades.

- Asegurar la efectiva implementación y monitoreo del procedimiento de gestión de incidentes, asegurando una respuesta oportuna y eficiente ante cualquier incidente de seguridad.

3. ALCANCE

El Plan Estratégico de Seguridad de la Información abarca todos los procesos de la entidad, cubriendo todas las áreas y niveles operativos. Su objetivo es garantizar la protección de la información mediante la implementación de políticas, procedimientos y controles de seguridad adecuados.

El éxito del plan dependerá del apoyo y compromiso de los diferentes secretarios y líderes de proceso, quienes serán responsables de promover y coordinar la adopción de las estrategias de seguridad en sus respectivas áreas, fomentando una cultura organizacional sólida en seguridad de la información.

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 767 de 2022**, “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”.
- **Resolución 746 de 2022**, ““Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021”
- **Guía DAFP Guía para la Administración del Riesgo**, “Guía para la Administración del Riesgo y el diseño de controles en entidades públicas (Versión 6)”
- **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".
- **CONPES 3995 de 2020, "Política Nacional de Confianza y Seguridad digital"**
- **Manual de Gobierno Digital – MINTIC**.
- **Modelo de Seguridad y Privacidad de la Información – MINTIC.**
- **Ley Estatutaria 1581 de 2012.** Ley de Protección de Datos Personales.

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

Actualmente, la Alcaldía de Bucaramanga está avanzando en diversas iniciativas orientadas a la implementación y adopción del modelo de seguridad y privacidad de la información. Entre estas iniciativas destaca el desarrollo de un plan de capacitación enfocado en fortalecer una cultura organizacional en seguridad y ciberseguridad, así como en la implementación de buenas prácticas para el manejo de la información y los datos institucionales.

Asimismo, se ha consolidado un procedimiento para la gestión de incidentes y se está llevando a cabo la reestructuración del plan de recuperación ante desastres. Se han establecido, además, acciones colaborativas con entes especializados como el MinTIC, orientadas a realizar análisis técnicos sobre los activos críticos de la entidad, con el fin de identificar posibles vulnerabilidades y corregirlas de manera oportuna, previniendo la materialización de riesgos.

Se realizan monitoreos constantes para detectar amenazas en la red corporativa y la infraestructura tecnológica, mientras que la Oficina de Control Interno lleva a cabo auditorías periódicas para evaluar la implementación del modelo de seguridad. Paralelamente, se trabaja en el cumplimiento de un plan de mejoramiento continuo, orientado a alcanzar los objetivos de seguridad y garantizar la protección de los activos de información.

Finalmente, se realiza un seguimiento continuo a la ejecución de iniciativas relacionadas con la implementación del mapa de riesgos de seguridad, con el objetivo de identificar, evaluar y ejecutar acciones de control para minimizar posibles amenazas y proteger los activos de la entidad.

5.1 PARTES INTERESADAS EN SEGURIDAD DE LA INFORMACIÓN.

La gestión de la seguridad de la información involucra a diversas partes interesadas, cada una con un nivel específico de influencia e involucramiento. La Dirección General y el Alcalde tienen un rol clave en la toma de decisiones estratégicas y asignación de recursos. El Comité Institucional de Gestión y Desempeño asegura que las iniciativas de seguridad estén alineadas con los objetivos institucionales.

Los Secretarios y Líderes de procesos implementan las políticas de seguridad en sus áreas, mientras que la Oficina de Control Interno verifica el cumplimiento mediante auditorías. El equipo de TI, los usuarios finales, proveedores y auditores externos participan activamente en la protección y monitoreo de la información. Además, las entidades gubernamentales y los ciudadanos tienen expectativas sobre el cumplimiento normativo y la protección de sus datos. Este enfoque integral permite una gestión colaborativa y efectiva de la seguridad de la información en la entidad.

A continuación, se presenta la tabla detallada que describe las partes interesadas, su nivel de influencia, expectativas y acciones a tomar en relación con la seguridad de la información.

Parte interesada	Nivel de influencia	Intereses y expectativas	Nivel de involucramiento	Acciones a tomar
Dirección General / Alcalde	Alta	Asegurar la protección de la información, cumplir con normativas y proteger la reputación institucional.	Alta	Apoyo y toma de decisiones clave, asignación de recursos, respaldo a la cultura organizacional.
Comité Institucional de Gestión y Desempeño	Alta	Asegurar la alineación de la seguridad de la información con los objetivos estratégicos de la	Alta	Evaluar el progreso de la implementación del modelo de seguridad, revisar informes de

		entidad, evaluar el desempeño.		desempeño y apoyar en la toma de decisiones.
Secretarios y Líderes de procesos	Alta	Implementar y seguir las políticas de seguridad en sus respectivas áreas.	Alta	Colaborar en la implementación y monitoreo de políticas y procedimientos.
Oficina de Control Interno	Alta	Verificar el cumplimiento del modelo de seguridad, realizar auditorías.	Alta	Realizar auditorías periódicas, seguimiento al cumplimiento de normativas de seguridad.
Usuarios finales (empleados)	Alta	Proteger su información personal y profesional, cumplir con buenas prácticas.	Alta	Capacitación continua en seguridad, sensibilización sobre amenazas y buenas prácticas.
Equipo de TI (Tecnologías de la Información)	Alta	Proteger los sistemas y redes, gestionar incidentes y vulnerabilidades.	Alta	Implementar controles técnicos, monitoreo constante de la infraestructura.
Proveedores externos	Media	Cumplir con los estándares de seguridad al proporcionar servicios o productos.	Media	Asegurar que los proveedores cumplan con las normativas de seguridad de la información.
Auditores Externos	Media	Evaluar el cumplimiento de las políticas de seguridad y privacidad.	Media	Realizar auditorías externas para evaluar la efectividad del modelo de seguridad.
Ciudadanos	Media	Garantizar la confidencialidad y seguridad de su información personal.	Media	Comunicación clara sobre cómo se protege su información, implementar medidas de privacidad.
Entidades gubernamentales (MinTIC, otros)	Alta	Cumplir con normativas nacionales de seguridad y privacidad de la información.	Alta	Colaboración en cumplimiento normativo, análisis de vulnerabilidades.

6. ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN

El Plan Estratégico de Seguridad de la Información de la Alcaldía de Bucaramanga se sustenta en cinco ejes fundamentales: liderazgo en seguridad, gestión de riesgos, implementación de controles, gestión de incidentes y sensibilización. Cada uno de estos ejes se orienta a garantizar una protección efectiva de los activos de información, estableciendo responsabilidades claras y tomando decisiones estratégicas para mitigar amenazas, fortalecer la infraestructura tecnológica y crear una cultura organizacional comprometida con la seguridad.

Además, se busca consolidar una cultura de seguridad mediante la capacitación continua y la sensibilización del personal sobre las mejores prácticas en ciberseguridad. La estrategia también incluye un sistema de gestión de incidentes, que garantiza una respuesta ágil ante cualquier amenaza, y un plan de recuperación ante desastres para asegurar la continuidad operativa. Con un monitoreo constante y la realización de auditorías periódicas por parte de la Oficina de Control Interno, se garantiza que las políticas sean efectivas y que la protección de la información se mantenga alineada con los estándares más altos de seguridad. La colaboración con proveedores externos especializados refuerza esta estrategia, asegurando que la Alcaldía de Bucaramanga mantenga un entorno tecnológico seguro y resiliente.

El propósito principal de esta estrategia es asegurar la integridad, confidencialidad y disponibilidad de la información institucional. Para ello, se enfoca en la adopción progresiva y consolidación del Modelo de Seguridad y Privacidad de la Información, aplicando los lineamientos establecidos en el mismo en todas las áreas de la entidad. Este enfoque implica la implementación de controles efectivos que abarcan todos los procesos y el involucramiento de todos los niveles organizacionales. La alta dirección juega un papel crucial en la asignación de recursos, en la toma de decisiones estratégicas y en el seguimiento del progreso de la adopción del modelo, garantizando que las acciones estén alineadas con los objetivos institucionales.

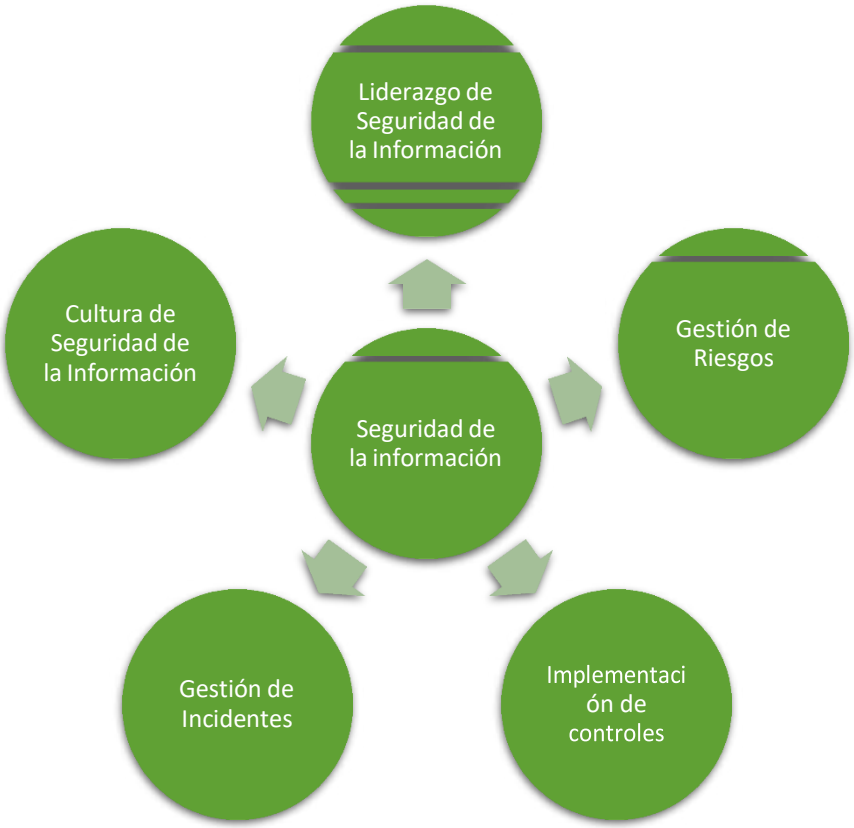

Figura 1. Dimensiones estratégicas de Seguridad de la Información
Fuente: Elaboración propia.

6.1. DIMENSIONES ESTRATEGICAS DE SEGURIDAD DE LA INFORMACIÓN.

A continuación, se detallan las dimensiones que componen la estrategia de seguridad de la información, enfocadas en asegurar la protección de los activos y el cumplimiento de los objetivos establecidos.

DIMENSIÓN	DESCRIPCIÓN / OBJETIVO
Liderazgo de seguridad de la información	El liderazgo en seguridad de la información es esencial para garantizar la protección efectiva de los activos dentro de la entidad. Esta dimensión se enfoca en establecer una estructura clara de responsabilidades, donde la alta dirección, junto con los líderes de las diferentes secretarías y direcciones, asume un papel clave en la toma de decisiones estratégicas, asignación de recursos y respaldo a la implementación de políticas de seguridad. Un liderazgo sólido promueve el compromiso de todos los niveles de la organización, garantizando que la seguridad de la información sea una prioridad constante y que se mantenga alineada con los objetivos estratégicos de la entidad. Además, fomenta una cultura organizacional comprometida con la ciberseguridad, impulsando la adopción de mejores prácticas y el cumplimiento de normativas.
Gestión de riesgos	La gestión de riesgos en seguridad de la información es un proceso fundamental para identificar, evaluar y mitigar las amenazas que puedan afectar los activos de la entidad. Esta dimensión se enfoca en establecer un enfoque sistemático para identificar las vulnerabilidades y riesgos asociados con los sistemas de información, datos y procesos operativos, garantizando su protección frente a incidentes cibernéticos y otros riesgos. Además, se implementan acciones preventivas y correctivas para minimizar el impacto de estos riesgos y asegurar la continuidad de las operaciones. La gestión de riesgos no solo busca proteger la infraestructura tecnológica, sino también promover una cultura organizacional proactiva, que valore la importancia de la seguridad de la información y garantice que todos los niveles de la entidad estén comprometidos con su identificación y mitigación.

Concientización	Una de las dimensiones clave del Plan Estratégico de Seguridad de la Información de la Alcaldía de Bucaramanga es el fomento de una cultura organizacional robusta en torno a la seguridad. Esta dimensión busca garantizar que todos los colaboradores, desde la alta dirección hasta los empleados de nivel operativo, comprendan la importancia de proteger los activos de información y adopten prácticas responsables en su manejo. Para ello, se implementarán programas continuos de capacitación y sensibilización, con el objetivo de educar a los empleados sobre los riesgos cibernéticos y las amenazas a las que se enfrentan. Las campañas de sensibilización serán diseñadas para promover buenas prácticas de seguridad, reforzar las políticas internas y asegurar el cumplimiento de los procedimientos establecidos. Además, se realizarán ejercicios prácticos, como simulaciones de ingeniería social, que permitirán a los colaboradores reconocer y actuar frente a intentos de phishing y otras técnicas de ataque. Esta dimensión, enfocada en la formación y concientización constante, fortalecerá la capacidad de la Alcaldía de Bucaramanga para prevenir incidentes de seguridad y proteger sus activos más valiosos.
Implementación de controles	Esta dimensión se centra en la aplicación de medidas tecnológicas y administrativas para garantizar la protección de los activos de información. Esta dimensión abarca tanto la adopción de soluciones de seguridad tecnológicas, como la creación de políticas y procedimientos internos que aseguren el cumplimiento de las normativas de seguridad. Además, se establecerán controles de acceso que restrinjan el uso de la información de acuerdo con los roles y necesidades de cada usuario dentro de la Alcaldía. El propósito es crear un entorno seguro donde los datos y sistemas estén protegidos frente a amenazas, reduciendo la vulnerabilidad ante posibles

	incidentes. A través de esta implementación, se busca no solo asegurar la confidencialidad, integridad y disponibilidad de la información, sino también facilitar una respuesta ágil y eficiente ante cualquier eventualidad que pueda comprometer la seguridad de los recursos institucionales.
Gestión de incidentes	Se busca establecer un proceso integral para manejar de manera eficiente los incidentes de seguridad. Este proceso abarca desde la identificación y notificación de un incidente hasta su resolución y análisis post-incidente. En primer lugar, se establecen mecanismos claros para que los empleados y usuarios puedan reportar cualquier actividad sospechosa, asegurando una detección rápida. Una vez reportado, el equipo técnico de seguridad evalúa la situación, establece la gravedad del incidente y toma las medidas necesarias para mitigar cualquier daño, involucrando a los líderes de cada área según sea necesario. Además, se activan protocolos de comunicación internos que aseguran una respuesta coordinada entre las áreas involucradas, como el equipo de TI y la alta dirección. Después de la resolución, se realiza un análisis exhaustivo para identificar las causas raíz y aplicar mejoras preventivas. Este enfoque asegura que la Alcaldía de Bucaramanga pueda responder de forma ágil, eficaz y coordinada ante cualquier incidente, protegiendo la integridad de sus activos de información.

7. DEFINICIÓN DE ACTIVIDADES ASOCIADAS AL PLAN ESTRATEGICO DE SEGURIDAD DE LA INFORMACIÓN

La Alcaldía de Bucaramanga define los siguientes proyectos y actividades con el propósito de avanzar en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

ESTRATEGIA / EJE	ACTIVIDAD	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	1. Velar por el cumplimiento de las normativas y regulaciones en seguridad de la información, además de revisar y aprobar las actualizaciones del Modelo de Seguridad y Privacidad de la Información (MSPI), incluyendo sus políticas, procedimientos y otros mecanismos necesarios para su efectiva implementación.	1.1. Informe de políticas definidas y aprobadas por el Comité de Gestión y Desempeño MIPG y el CICCI, detallando las actualizaciones y ajustes realizados.
	2. Destinar los recursos financieros, tecnológicos y humanos requeridos para garantizar el éxito de las iniciativas en Ciberseguridad y Seguridad de la Información.	2.1. Implementación de proyectos asociados a Seguridad de la información y Ciberseguridad ejecutados al interior de la entidad.
	3. Apoyar las estrategias, iniciativas y proyectos de seguridad de la información, garantizando que estén alineados con los objetivos de la organización y contribuyendo a su implementación exitosa.	3.1. A continuación, se detallan los entregables que se generarán según el contexto y las necesidades de cada proyecto: • Informes de Supervisión de Proyectos. • Planes de Alineación Estratégica. • Actas de Reuniones de Supervisión. • Evaluaciones de Proyecto y Cumplimiento. • Actas de Reunión de Avance de Proyecto.

	4. Realizar un autodiagnóstico de seguridad de la información para evaluar controles, políticas y vulnerabilidades, con el fin de identificar áreas de mejora.	4.1. Autodiagnóstico de seguridad de la información debidamente diligenciado.
Gestión de riesgos	5. Realizar seguimiento continuo y monitoreo activo del mapa de riesgos de seguridad de la información.	5.1. Mapa de riesgos de seguridad de la información actualizado, con el avance detallado de las acciones implementadas.
	6. Monitorear el inventario de activos de información y actualizarlo cuando sea necesario.	6.1. Mapa de Riesgos de Seguridad de la Información actualizado.
Cultura de Seguridad de la Información	7. Desarrollar un programa de formación continua en seguridad de la información, dirigido a sensibilizar a empleados, contratistas y directivos sobre la protección de datos y el cumplimiento de las políticas de seguridad.	7.1. Plan de Capacitación en Seguridad de la Información
	8. Impartir sesiones de capacitación y llevar a cabo campañas de sensibilización periódicas dirigidas a empleados, líderes de proceso, aliados estratégicos y alta dirección, enfocadas en las políticas y buenas prácticas de seguridad de la información.	8.1. Los productos o entregables esperados para esta actividad pueden ser: • Informe de sesiones de capacitación realizadas. • Materiales de sensibilización (presentaciones, folletos, videos).

		• Registros de asistencia a las sesiones de capacitación. • Evaluación de efectividad de las campañas de sensibilización. • Encuestas de retroalimentación de los participantes.
Implementación de controles	9. Realizar anualmente un análisis de vulnerabilidades en los activos críticos de la infraestructura tecnológica para identificar debilidades y fortalecer la seguridad.	9.1. Informe de análisis de vulnerabilidades técnicas y recomendaciones de mejora.
	10. Definir e implementar un plan de remediación para abordar las vulnerabilidades y debilidades identificadas en los activos críticos de la infraestructura tecnológica, priorizando las acciones correctivas según su impacto y riesgo.	10.1. Plan de remediación con acciones correctivas implementadas, y seguimiento de su efectividad.
	11. Avanzar en la implementación del modelo de seguridad y privacidad de la información, ejecutando los controles establecidos y asegurando su integración en los procesos organizacionales, con monitoreo continuo y actualización periódica para proteger los activos de información.	11.1. Informe de Monitoreo y Actualización del Modelo de Seguridad de la Información.

	12. Realizar el seguimiento y ejecución de las acciones correctivas derivadas de la auditoría realizada por la Oficina de Control Interno, asegurando el cumplimiento de las recomendaciones y la implementación de los ajustes necesarios dentro de los plazos establecidos.	12.1. Informe de avance del plan de mejoramiento.
	13. Monitorear y actualizar de manera continua los indicadores del Modelo de Seguridad y Privacidad de la Información.	13.1. Informe actualizado de indicadores del Modelo de Seguridad y Privacidad de la Información.
	14. Implementar soluciones de seguridad (antivirus, firewalls, copias de seguridad) y realizar su seguimiento y monitoreo continuo para proteger la infraestructura tecnológica y los datos críticos.	14.1. Informe de implementación y monitoreo de soluciones de seguridad.
Gestión de incidentes	15. Formalizar e implementar el procedimiento para la identificación, notificación, clasificación y resolución de incidentes de seguridad, asegurando su correcta aplicación.	15.1. Documento formal que confirma la aprobación del procedimiento de gestión de incidentes.
	16. Capacitar a los actores clave en el procedimiento de gestión de incidentes, aclarando sus roles y responsabilidades, y entrenar a los usuarios sobre	16.1. Registro de asistencia. Materiales de capacitación.

	la importancia de reportar incidentes oportunamente.	
	17. Registrar y dar seguimiento a los eventos e incidentes de seguridad en una bitácora para garantizar su trazabilidad y resolución efectiva.	17.1. Bitácora o registro actualizado de eventos e incidentes de seguridad, o alternativamente, informe de seguimiento de los incidentes ocurridos.

8. CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

Teniendo en cuenta los proyectos y actividades definidos en la sección anterior, se establece el siguiente cronograma con el propósito de definir los tiempos estimados para la realización de las actividades planteadas.

CRONOGRAMA 2025				
ACTIVIDAD	**Trimestre 1**	**Trimestre 2**	**Trimestre 3**	**Trimestre 4**
Velar por el cumplimiento de las normativas y regulaciones en seguridad de la información, además de revisar y aprobar las actualizaciones del Modelo de Seguridad y Privacidad de la Información (MSPI), incluyendo sus políticas, procedimientos y otros mecanismos necesarios para su efectiva implementación.				

Destinar los recursos financieros, tecnológicos y humanos requeridos para garantizar el éxito de las iniciativas en Ciberseguridad y Seguridad de la Información.				
Apoyar las estrategias, iniciativas y proyectos de seguridad de la información, garantizando que estén alineados con los objetivos de la organización y contribuyendo a su implementación exitosa.				
Realizar un autodiagnóstico de seguridad de la información para evaluar controles, políticas y vulnerabilidades, con el fin de identificar áreas de mejora.				
Realizar seguimiento continuo y monitoreo activo del mapa de riesgos de seguridad de la información.				
Monitorear el inventario de activos de información y actualizarlo cuando sea necesario.				
Desarrollar un programa de formación continua en seguridad de la información, dirigido a sensibilizar a empleados, contratistas y directivos sobre la protección de datos y el cumplimiento de las políticas de seguridad.				

Impartir sesiones de capacitación y llevar a cabo campañas de sensibilización periódicas dirigidas a empleados, líderes de proceso, aliados estratégicos y alta dirección, enfocadas en las políticas y buenas prácticas de seguridad de la información.				
Realizar anualmente un análisis de vulnerabilidades en los activos críticos de la infraestructura tecnológica para identificar debilidades y fortalecer la seguridad.				
Definir e implementar un plan de remediación para abordar las vulnerabilidades y debilidades identificadas en los activos críticos de la infraestructura tecnológica, priorizando las acciones correctivas según su impacto y riesgo.				
Avanzar en la implementación del modelo de seguridad y privacidad de la información, ejecutando los controles establecidos y asegurando su integración en los procesos organizacionales, con monitoreo continuo y actualización periódica para proteger los activos de información.				

Realizar el seguimiento y ejecución de las acciones correctivas derivadas de la auditoría realizada por la Oficina de Control Interno, asegurando el cumplimiento de las recomendaciones y la implementación de los ajustes necesarios dentro de los plazos establecidos.				
Monitorear y actualizar de manera continua los indicadores del Modelo de Seguridad y Privacidad de la Información.				
Implementar soluciones de seguridad (antivirus, firewalls, copias de seguridad) y realizar su seguimiento y monitoreo continuo para proteger la infraestructura tecnológica y los datos críticos.				
Formalizar e implementar el procedimiento para la identificación, notificación, clasificación y resolución de incidentes de seguridad, asegurando su correcta aplicación.				
Capacitar a los actores clave en el procedimiento de gestión de incidentes, aclarando sus roles y responsabilidades, y entrenar a los usuarios sobre la importancia de reportar incidentes oportunamente.				

Registrar y realizar seguimiento a los eventos e incidentes de seguridad en una bitácora para garantizar su trazabilidad y resolución efectiva.				

9. RESPONSABLES

- Alcalde: Aprobar los documentos de Alto Nivel y destinar los recursos necesarios.
- Comité Institucional de Gestión y Desempleo – MIPG, Comité Institucional de Coordinación de Control Interno - CICCI.: Aprobar documentos asociados al Modelo de Seguridad y Privacidad de la Información y realizar seguimiento a la ejecución de las iniciativas.
- Responsable de Seguridad Digital / CIO / Asesor TIC Despacho Alcalde: Coordinar las actividades de implementación del MSPI

10. HISTORIAL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA	RESPONSABLE
0.0	Original Documento desarrollado por el Proceso Gestión de TIC con el fin de establecer la primera versión del PLAN ESTRATÉGICO DE	Diciembre-12-2023	
1.0	Se actualizaron las actividades a ejecutar asociadas al	Enero-30-2025	Ing. Jaime Otero