CONCEJO
DE MEDELLÍN

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIDAD DE INFORMÁTICA
CONCEJO DE MEDELLÍN

2022-2025

TABLA DE CONTENIDO

PRESENTACIÓN

El Concejo de Medellín se encuentra en la fase de implementación del Modelo de Seguridad y Privacidad de la Información –MSPI-, con el fin de dar cumplimiento a los requisitos establecidos en la Política de Gobierno Digital, la cual establece como uno de los habilitadores transversales la Seguridad de la Información, la cual pretender que las entidades públicas y organismos del Estado implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la Información -MSPI, que contempla 6 niveles de madurez.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. OBJETIVO GENERAL

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información del Concejo de Medellín, para reducir los riesgos a los que está expuesta la Corporación hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2022-2025.

2. OBJETIVOS ESPECÍFICOS.

- Definir y establecer la estrategia de seguridad digital del Concejo de Medellín.
- Definir y establecer las necesidades de la Corporación para la implementación del Sistema de Gestión de Seguridad de la Información.
- Priorizar los proyectos 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 de Seguridad y Privacidad de la Información, al buscar la implementación del Sistema de Seguridad de la Información y la estrategia de Seguridad Digital del Concejo de Medellín, comparte el alcance definido dentro de la Política General de Seguridad de la Información, donde se indica que se tendrán en cuenta todos los procesos de la entidad.

4. DOCUMENTOS DE REFERENCIA

El presente Plan 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.
- PETI, Plan estratégico de tecnologías de la información y las comunicaciones del Concejo de Medellín**,** 2022-2025.

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

En el momento el Concejo de Medellín, presenta el siguiente estado respecto a la implementación de los lineamientos de seguridad de la información requeridos por el MSPI

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	16	100	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	34	100	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	12	100	INICIAL
A.9	CONTROL DE ACCESO	33	100	REPETIBLE
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	40	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	44	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	57	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	36	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	0	100	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	71	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	100	INEXISTENTE
A.18	CUMPLIMIENTO	40	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		**29**	**100**	REPETIBLE

Estado actual respecto al Sistema de Gestión de Seguridad de la Información. Fuente: Propio.

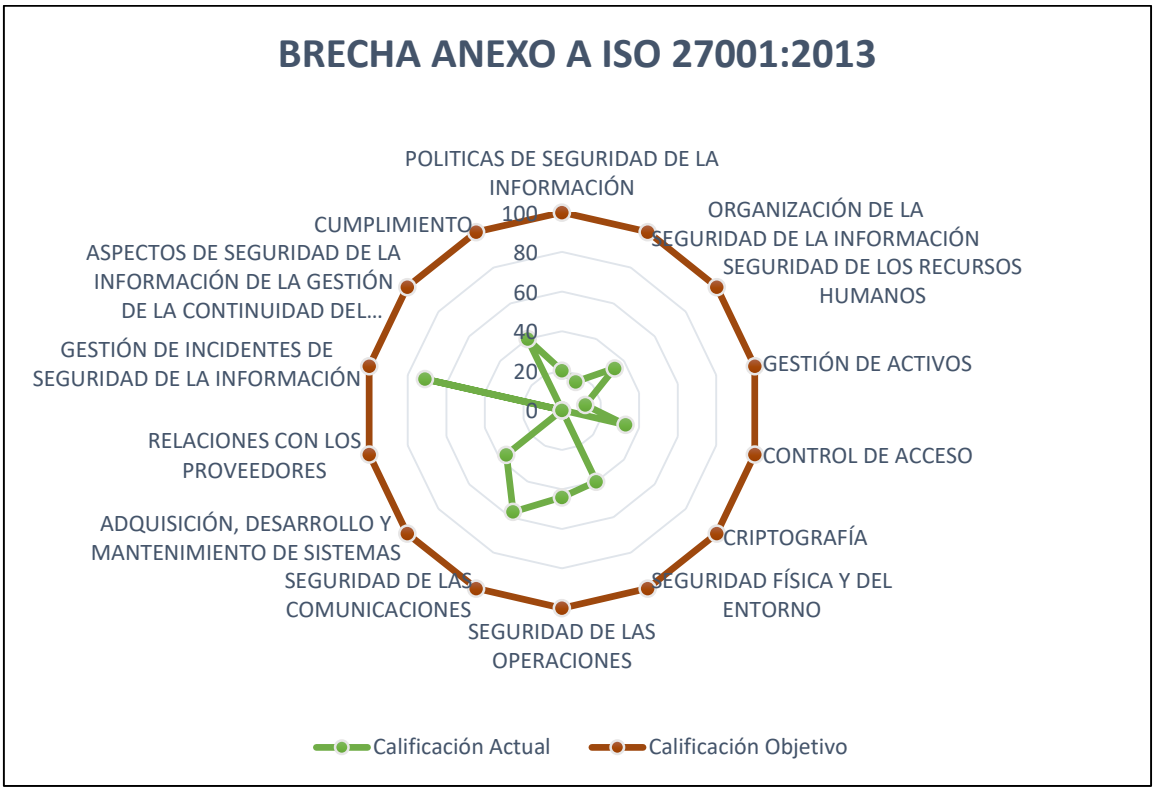


Gráfico brecha. Fuente: Propio.

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2020	Planificación	6,22%	40%
	Implementación	1,44%	20%
	Evaluación de desempeño	0,00%	20%
	Mejora continua	0,00%	20%
TOTAL		8%	100%

Avance en cada fase del ciclo PHVA. Fuente: propio.

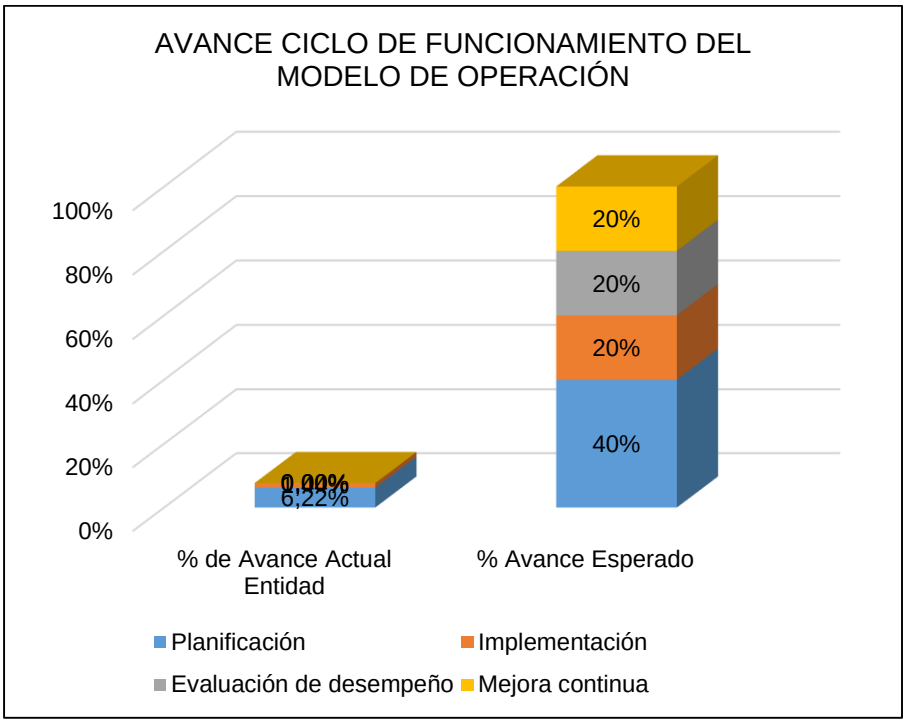


Gráfico avance en cada fase del ciclo PHVA. Fuente: Propio.

NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

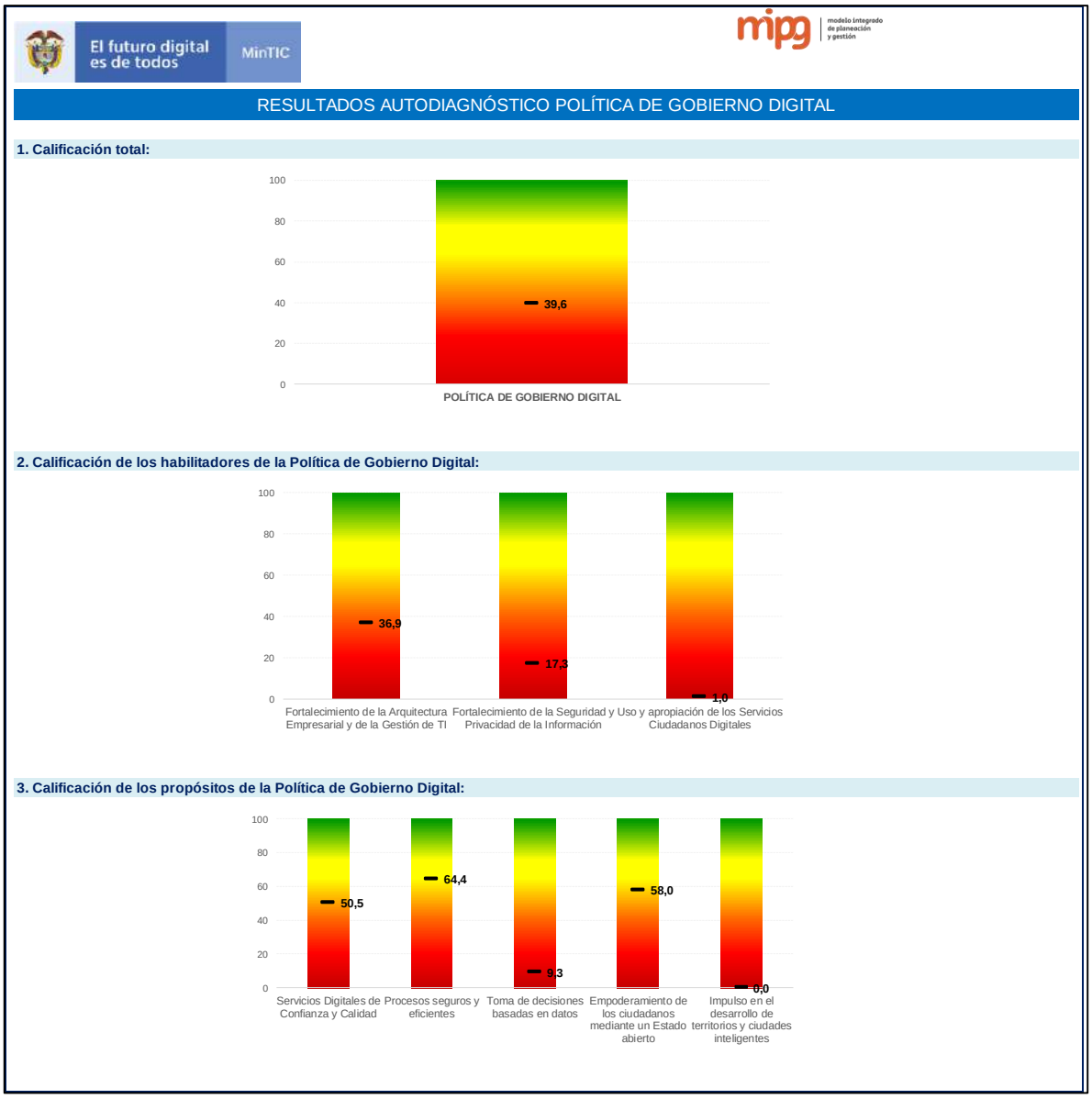
		NIVEL DE CUMPLIMIENTO
NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Inicial	INTERMEDIO
	Repetible	INTERMEDIO
	Definido	CRÍTICO
	Administrado	CRÍTICO
	Optimizado	CRÍTICO

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.

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

Nivel de cumplimiento en cada uno de los niveles de madurez del modelo. Fuente: Propio.

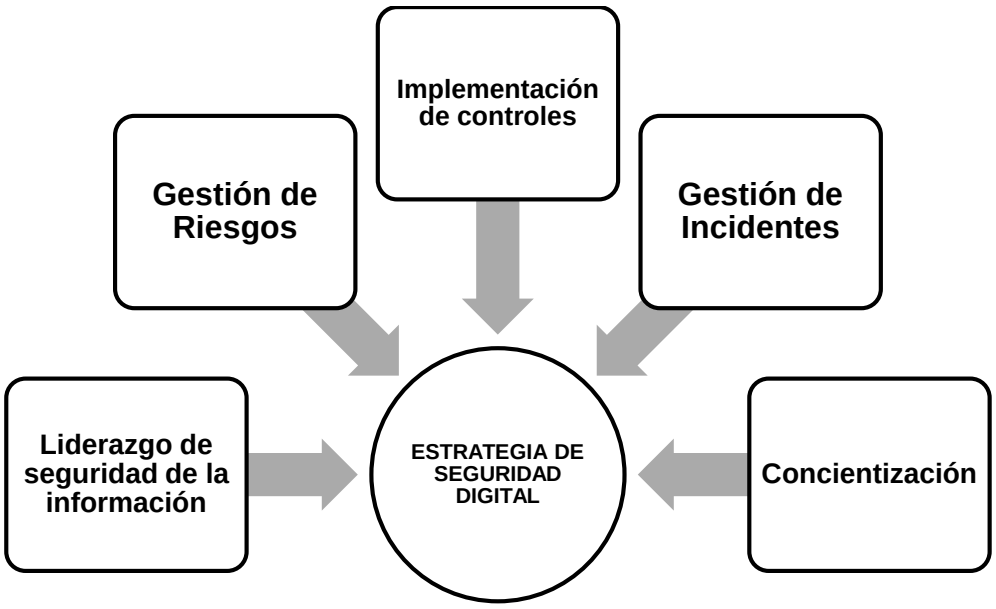
A continuación, se presenta el resultado del autodiagnóstico política de gobierno digital realizado en marzo de 2021.



6. ESTRATEGIA DE SEGURIDAD DIGITAL

El Concejo de Medellín 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 en torno 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, el Concejo de Medellín define las siguientes cinco estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



Estrategia de seguridad digital. Fuente: Propio.

6.1. 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 Corporación a través del establecimiento de los roles y responsabilidades en seguridad de la información.

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
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 se 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 del Concejo de Medellín. Se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base en 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 Corporación.

6.2. PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, el Concejo de Medellín define 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	Apropiar por parte del Comité Institucional de Gestión y Desempeño la implementación y desarrollo de la política de seguridad digital y de la información	Actas de comité institucional de gestión y desempeño donde se evidencie que se abordan aspectos de desarrollo e implementación de la política de seguridad digital y de la información
Gestión de riesgos	Gestionar los riesgos de TI aplicando la metodología adoptada en el Corporación, especialmente la de riesgos de seguridad y privacidad de la información.	Matriz de riesgos de seguridad digital Definir planes de tratamiento de riesgos
Concientización	Realizar jornadas de sensibilización a todo el personal.	Evidencias de las actividades desarrolladas (Registros de asistencia, convocatorias)
Implementación de controles	Gestionar la implementación de los controles identificados y asociados a los riesgos para minimizar su impacto y ocurrencia.	Evaluación de riesgos con el registro de materialización de riesgos
Gestión de incidentes	Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información.	1. Procedimiento de gestión de incidentes de seguridad formalizado.

6.3. CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

PROYECTO	2022	2023	2024	2025
Apropiar por parte del Comité Institucional de Gestión y Desempeño la implementación y desarrollo de la política de seguridad digital y de la información				
Gestionar los riesgos de TI aplicando la metodología adoptada en el Corporación, especialmente la de riesgos de seguridad y privacidad de la información.				
Realizar jornadas de sensibilización a todo el personal				
Gestionar la implementación de los controles identificados y asociados a los riesgos para minimizar su impacto y ocurrencia.				
Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información				

Nota: Al finalizar cada vigencia, el Concejo de Medellín 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 Corporación.

6.4. ANÁLISIS PRESUPUESTAL:

Con base a los proyectos definidos en el cronograma de actividades, se genera el presupuesto aproximado por cada vigencia según los proyectos establecidos:

	AÑO 2022	AÑO 2023	AÑO 2024	AÑO 2025
PROYECTO	**PRESUPUESTO**	**PRESUPUESTO**	**PRESUPUESTO**	**PRESUPUESTO**
Apropiar por parte del Comité Institucional de Gestión y Desempeño la implementación y desarrollo de la política de seguridad digital y de la información	10.000.000	10.000.000	10.000.000	10.000.000
Gestionar los riesgos de TI aplicando la metodología adoptada en el Corporación, especialmente la de riesgos de seguridad y privacidad de la información.	0	0	0	0
Realizar jornadas de sensibilización a todo el personal	10.000.000	10.000.000	10.000.000	10.000.000
Gestionar la implementación de los controles identificados y asociados a los riesgos para minimizar su impacto y ocurrencia.	240.000.000	298.000.000	310.000.000	324.000.000
Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información	0			
TOTAL PRESUPUESTO	**$ 260.000.000**	**$ 318.000.000**	**$ 330.000.000**	**$ 344.000.000**

7. RESPONSABLES

- Secretario (a) General: Aprobar los documentos de Alto Nivel.
- Secretario (a) General: Asegurar la implementación del MSPI y garantizar los recursos requeridos.
- Líder de programa Unidad de informática: Coordinar las actividades de implementación del MSPI
- Profesionales universitarios – Mesa de ayuda: Ejecutar las actividades relacionadas con la implementación del MSPI.

8. AVANCE VIGENCIA 2022

- Estado de los proyectos definidos.

ESTRATEGIA / EJE	PROYECTO	AVANCE 2022
Liderazgo de seguridad de la información	Apropiar por parte del Comité Institucional de Gestión y Desempeño la implementación y desarrollo de la política de seguridad digital y de la información	Se incluyó en el orden del día del Comité Institucional de Gestión y Desempeño los avances alcanzados en materia de seguridad y privacidad de la información. Actas 21, 25, 29, 30 y 35 del 2022
Gestión de riesgos	Gestionar los riesgos de TI aplicando la metodología adoptada en el Corporación, especialmente la de riesgos de seguridad y privacidad de la información.	Matriz de riesgos de seguridad digital actualizada conforme a la metodología adoptada en el Corporación. Se formuló el Plan de tratamiento de riesgos de seguridad y privacidad de la información 2023.
Concientización	Realizar jornadas de sensibilización a todo el personal.	Se realizaron dos jornadas de sensibilización los días 13 y 15 de diciembre
Implementación de controles	Gestionar la implementación de los controles identificados y asociados a los riesgos para minimizar su impacto y ocurrencia.	Se realizó evaluación de los riesgos y controles identificados, de manera trimestral en el Comité Institucional de Gestión y Desempeño.

ESTRATEGIA / EJE	PROYECTO	AVANCE 2022
		La materialización y tratamiento se registró en el Reporte de Mejoramiento de Isolución (Acciones 619, 620 y 621).
Gestión de incidentes	Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información.	Se formalizó el procedimiento de gestión de incidentes de seguridad.

- Avance en la implementación del MSPI.

Se aumentó en un 39% la 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	90	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	100	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	92	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	50	100	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	40	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	44	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	57	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	36	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	100	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	71	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	27	100	REPETIBLE
A.18	CUMPLIMIENTO	50	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		**68**	**100**	GESTIONADO

La implementación del MSPI aumentó en un 32%:

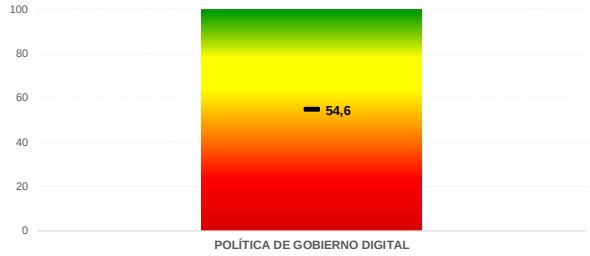
Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2022	Planificación	36,44%	40%
	Implementación	3,42%	20%
	Evaluación de desempeño	0,00%	20%
	Mejora continua	0,00%	20%
TOTAL		40%	100%

- Resultados Autodiagnóstico Gobierno Digital de MIPG

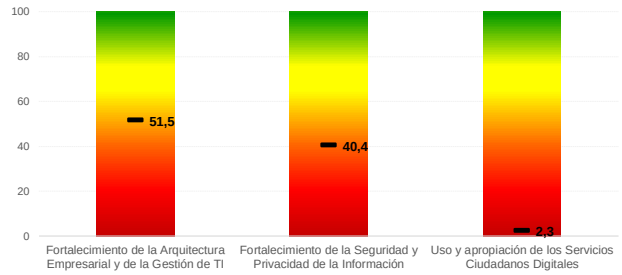
Respecto al año 2021, el resultado del autodiagnóstico aumentó en 15 puntos porcentuales.

RESULTADOS AUTODIAGNÓSTICO POLÍTICA DE GOBIERNO DIGITAL

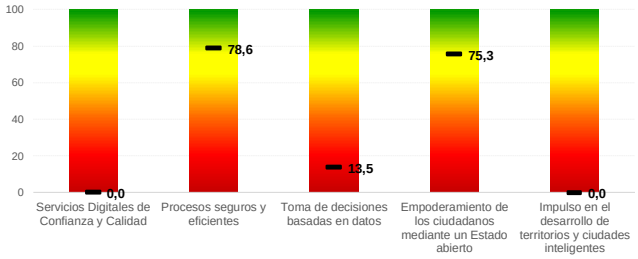
1. Calificación total:



2. Calificación de los habilitadores de la Política de Gobierno Digital:



3. Calificación de los propósitos de la Política de Gobierno Digital:



9. SEGUIMIENTO

Se realizará seguimiento trimestral a las acciones propuestas en el presente Plan y se presentará el avance en el Comité Institucional de Gestión y Desempeño, conforme al Calendario de Obligaciones Legales y Administrativas - COLA, de la Corporación.