PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI) 2025 – 2027

GOBERNACIÓN DE ANTIOQUIA
República de Colombia

Maria Cristina Giraldo Ospina
Directora de Tecnología e Información

Dirección de Tecnología e Información

2025 - 2027

GOBERNACIÓN DE ANTIOQUIA
República de Colombia

Equipo que trabajo y apoyó en la construcción del PESI.

Nombre	Rol
Maria Cristina Giraldo Ospina	Directora de Tecnología e Información.
Sergio Andrés Cadavid Echeverry	Equipo y/o Grupo de Seguridad de la Información.
Adriana Ximena Florez Martinez	
John Fredy Borja Carvajal	
Alejandro Ospina Gil	
Yeison Monsalve Sanchez	
Lyda Durley Mona Cardona	

Tabla No.1 - Equipo que trabajo y apoyó en la construcción del PESI.

TABLA DE CONTENIDO

INTRODUCCIÓN. 5
1. GENERALIDADES. 6
2. OBJETIVO. 6
2.1. OBJETIVOS ESPECÍFICOS. 6
3. ALCANCE. 6
4. MARCO NORMATIVO. 7
5. DEFINICIONES. 10
6. ESTADO ACTUAL DE LA ENTIDAD 12
6.1. RESPONSABLES EN SEGURIDAD DE LA INFORMACIÓN. 12
6.2. RESULTADO FURAG 13
6.3. EJECUCIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI). 13
7. ESTRATEGIA DE SEGURIDAD DIGITAL. 15
7.1. DESCRIPCIÓN DE LA ESTRATEGIAS. 16
7.2. PORTAFOLIO DE PROYECTOS Y PRODUCTOS ESPERADOS. 17
7.3. CRONOGRAMA DE PROYECTOS 20
8. DOCUMENTOS DE REFERENCIA. 21

TABLAS 22

IMÁGENES 22

INTRODUCCIÓN.

La Gobernación de Antioquia como Entidad Gubernamental está en la obligación de cumplir con la Política de Gobierno Digital impuesta en el decreto No. 1008 del 14 de junio 2018, por la 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 Decreto 1078 de 2015, Decreto Único Reglamentario del sector de las Tecnologías de Información y Comunicaciones.

Que en la Política de Gobierno Digital en su artículo 2.2.9.1.1.3. – Principios; tiene como prioridad la Seguridad de la Información, el cual dice textualmente: "Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades estatales, y de los servicios que prestan al ciudadano".

Para la realización del documento se tomará como base los lineamientos de Seguridad de la Información establecidos por la Política de Seguridad Digital de junio de 2018. La Gobernación de Antioquia se guiará bajo los lineamientos normativos de la NTC-ISO/IEC 27001, la cual establece los requisitos de la implementación del SGSI, la NTC-ISO 31000; que proporciona un esquema para la gestión de riesgos y las mejores prácticas, tales como la GTC-ISO/IEC 27002, NTC-ISO/IEC 27005, entre otras; buscando mejorar el desempeño y la capacidad de prestar un servicio que responsa a las necesidades y expectativas de las partes interesadas.

Por otra parte, el Plan Estratégico de Tecnología de la Información y Comunicaciones (PETI), es un documento que expresa las intenciones de la organización, en la implementación de iniciativas y acciones que promuevan el uso de las Tecnología de la Información y las Comunicaciones – TIC's como contribución al logro de los Objetivos y Lineamientos Estratégicos enmarcados en el Plan Estratégico Institucional.

El documento PETI define lineamientos para el mejoramiento del nivel de madurez institucional en la implementación de soluciones tecnológicas que generen valor y promuevan el cumplimiento de la misión con sostenibilidad tecnológica. El fortalecimiento y mejoramiento de la infraestructura tecnológica, el fortalecimiento de una mesa de ayuda, la implementación de los Sistemas de Gestión de Seguridad de la Información y la Continuidad de Negocio, la optimización en el procesamiento y análisis de información, el fortalecimiento y mejora de los procesos institucionales Estratégicos, Misionales, de Apoyo y de Evaluación.

El PESI descrito en este documento está alineado completamente con el PETI, en el cual se define estrategias y proyectos con el fin de fortalecer la Seguridad Digital en la Gobernación de Antioquia y dar cumplimiento a la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI y mejorar las prácticas de Gestión de Servicios de TI con el fin de contribuir no solo con el logro de los objetivos institucionales, sino en la generación de confianza en el uso de los mecanismos tecnológicos para una mejor relación Estado – Ciudadano.

1. GENERALIDADES.

El Plan Estratégico de Seguridad de la Información (PESI) constituye una herramienta para la formulación de planes y cronogramas para la implementación, mantenimiento y mejora del Sistema del Gestión de Seguridad de la Información alineado con los objetivos estratégico de la Gobernación de Antioquia en el que se definen estrategias y/o proyectos que permitan mejorar la postura de Seguridad Digital teniendo en cuenta los requerimientos y necesidades actuales de la entidad.

2. OBJETIVO.

Definir un Plan Estratégico de Seguridad de la Información, en adelante PESI, liderada por la Dirección de Tecnología e Información de la Gobernación de Antioquia, en adelante GOBANT, a partir de la vigencia 2024 hasta el año 2027, la cual se detalla desde el 2025 en el presente documento que responde a las necesidades de preservar la Confidencialidad, la Integridad, Disponibilidad y Privacidad de los activos de información.

2.1. OBJETIVOS ESPECÍFICOS.

1. Implementar el Modelo de Privacidad y Seguridad de la Información (MPSI) que permitan mejorar la postura de Seguridad Digital en la Entidad.

2. Actualizar e identificar los activos de información.

3. Identificar los riesgos de Seguridad de la Información.

4. Definir y ejecutar el Plan de Cultura y Sensibilización en Seguridad de la Información.

5. Ejecutar análisis de vulnerabilidades sobre la Plataforma Tecnológica de la Gobernación de Antioquia.

6. Gestionar los Incidentes de Seguridad de la Información identificados y reportados.

3. ALCANCE.

El Plan Estratégico de Seguridad de la Información (PESI) contempla la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) en todos los procesos de la Entidad acorde a las directrices del Modelo de Seguridad y Privacidad de la Información (MSPI) definida por el MINTIC y la norma NTC-ISO-IEC 27001 – Sistema de Gestión de Seguridad de la Información, así como el fortalecimiento de la Infraestructura Tecnológica de la Gobernación de Antioquia.

En la siguiente imagen se muestran los procesos institucionales que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información (SGSI):

Imagen No.1 - Mapa de Procesos de la Gobernación de Antioquia.

4. MARCO NORMATIVO.

El presente documento se soporta en la siguiente normatividad:

TIPO	FECHA	TITULO
Ley 527 de 1999	19 de Agosto 1999	Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
Directivas Presidencial 02 de 2000	28 de Agosto de 2000	Gobierno en Línea.

Ley 1266 de 2008	31 de Diciembre 2008	Habeas data financiera, y seguridad en datos personales. Por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
Ley 1273 de 2009	5 de Enero 2009	Delitos Informáticos y protección del bien jurídico tutelado que es la información. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
CONPES 3650 de 2010	15 de Marzo 2010	Importancia Estratégica de la Estrategia de Gobierno en Línea.
CONPES 3701 de 2011	14 de Julio 2011	Lineamientos de Política para Seguridad y Ciberdefensa.
Ley 1581 de 2012	17 de Octubre 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 1377 de 2013	27 de junio 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley 1712 de 2014	6 de marzo 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 886 de 2014	13 de Mayo 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Decreto 1083 de 2015	26 Mayo 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
CONPES 3854 de 2016	11 de Abril 2016	Política Nacional de Seguridad Digital.
CONPES 3920 de 2018	17 de Abril 2017	Política nacional de explotación de datos (Big Data).

Decreto 1499 de 2017	2017	Artículo 2.2.22.3.1. Actualiza el Modelo Integrado de Planeación y Gestión - MIPG.
Decreto 612 de 2018	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.
Decreto 1008 de 2018	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.
CONPES 3975 de 2019	8 de Abril 2019	Política Nacional para la Transformación Digital e Inteligencia Artificial.
CONPES 3995 de 2020	01 de julio 2020	Política Nacional de Confianza y Seguridad Digital.
CONPES 4012 de 2020	30 de Noviembre 2020	Política Nacional de Comercio Electrónico.
Resolución 500 de 2021	10 de Marzo 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.
Instrumento MSPI	22 de Febrero 2021	Modelo de Seguridad y Privacidad de la Información. Generado por MinTIC.
Decreto 338 de 2022	8 de Marzo 2022	Por el cual se adiciona el Titulo 21 a la parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la Seguridad Digital.

Tabla No.2 - Normatividad Aplicable.

5. DEFINICIONES.

Alcance:	Ámbito de la organización que queda sometido al SGSI.
Análisis de Riesgos:	Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
Comité de Dirección de Seguridad de la Información-CDSI:	Equipo interdisciplinario conformado por servidores públicos de diferentes áreas de la Gobernación de Antioquia que es presidido por el Director(a) de Tecnología e Información, este comité tiene responsabilidades y funciones generales y operativas definidas. Fue creado mediante resolución No.108373 del 30 de octubre de 2013 y modificado mediante resolución No.030836 del 21 de marzo de 2014.
Confidencialidad:	(Confidentiality). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
Control:	Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de Seguridad de la Información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
Declaración de Aplicabilidad:	(Statement Of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.
Disponibilidad:	(Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
Gestión de Riesgos:	(Risk Management). Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
Incidente de Seguridad de la Información:	(Information Security Incident). Evento único o serie de eventos de Seguridad de la Información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la Seguridad de la Información.
Integridad:	(Integrity). Propiedad de la información relativa a su exactitud y completitud.
ISO:	Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).

NTC-ISO/IEC 27001:	Norma que establece los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial. La nueva versión es del 2022.
NTC-ISO/IEC 27002:	Código de buenas prácticas en Gestión de la Seguridad de la Información. Primera publicación en 2005; segunda edición en 2013. No es certificable. La nueva versión es del 2022.
NIST:	(National Institute of Standards and Technology), Agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.
Parte Interesada:	(Interested Party / Stakeholder). Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
PDCA:	Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.
Plan de Continuidad del Negocio (BCP):	(Bussines Continuity Plan). Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.
Plan de Tratamiento de Riesgos:	(Risk Treatment Plan). Documento que define las acciones para gestionar los riesgos de Seguridad de la Información inaceptables e implantar los controles necesarios para proteger la misma.
Riesgo:	(Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
Seguridad de la Información:	(Information Security). Preservación de la confidencialidad, integridad y disponibilidad de la información.
Selección de Controles:	(Control Selection). Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.
SGSI:	(ISMS). Véase: Sistema de Gestión de la Seguridad de la Información.

Sistema de Gestión de la Seguridad de la Información:	(Information Security Management System). Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de Seguridad de la Información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

6. ESTADO ACTUAL DE LA ENTIDAD.

La Dirección de Tecnología e Información, trabaja en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) definido por MinTIC, el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital[1].

La Gobernación de Antioquia crea el Comité de Dirección de Seguridad de la Información-CDSI mediante resolución No.108373 del 30 de octubre de 2013 y modificado mediante resolución No.030836 del 21 de marzo de 2014, el cual puede ser consultada en el siguiente link: Resoluciones.

6.1. RESPONSABLES EN SEGURIDAD DE LA INFORMACIÓN.

La siguiente gráfica representa la estructura organizacional de los responsables en Seguridad de la Información que hacen parte de la Dirección de Tecnología e Información.

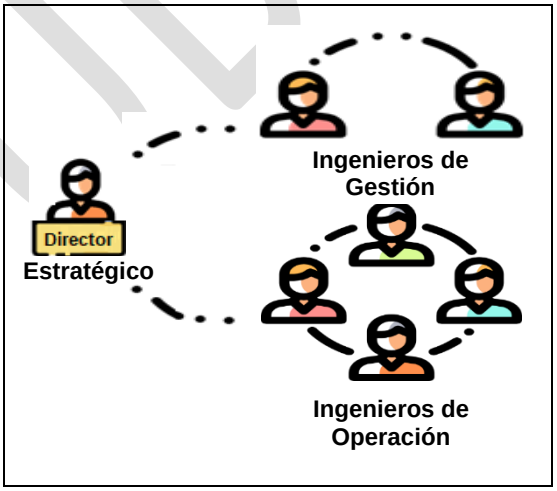

Imagen No.2 - Responsables en Seguridad de la Información.

[1] Fuente de consulta: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

6.2. RESULTADO FURAG.

La Gobernación de Antioquia realiza anualmente la medición de su desempeño en las Políticas de Gobierno Digital y de Seguridad Digital a partir del informe de Gestión y Desempeño Institucional emitido por la función pública denominado FURAG por sus siglas:(Formulario Único de Registro del Avance en la Gestión).

Con el objetivo de tener una visión del trabajo realizado durante las vigencias. Se observa en la imagen No.3 los resultados obtenidos desde el año 2018 al 2023 en el cumplimiento de las Políticas de Gobierno Digital y Seguridad Digital, con base a la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) y el Modelo de Seguridad y Privacidad de la Información (MSPI), esta información puede ser consultada en el link que se encentra cada uno de los años de la siguiente Tabla No.3.

III. Índice de las Políticas de Desempeño y Gestión.						
Índice	2018	2019	2020	2021	2022	2023
POL07: Gobierno Digital	84,0	96,0	97,2	98,1	84,9	89,9
POL08: Seguridad Digital	83,5	82,5	95,1	96,6	90,6	90,3

Tabla No.3 - Resultado FURAG Políticas Gobierno Digital y Seguridad Digital.

6.3. EJECUCIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI).

Con relación a la medición efectuada mediante la aplicación del instrumento del autodiagnóstico del Modelo de Seguridad de la Información (MSPI) en la entidad, se observa la evaluación de efectividad de controles implementados de acuerdo con la norma NTC-ISO-IEC 27001 como se detallan en la siguiente imagen:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	96	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	91	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	51	100	EFECTIVO
A.9	CONTROL DE ACCESO	94	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	90	100	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	87	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	82	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	74	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	79	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	90	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	50	100	EFECTIVO
A.18	CUMPLIMIENTO	97	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		83	100	OPTIMIZADO

Imagen No.3 - Seguimiento al MSPI.

Se identifican algunos dominios que se encuentra por debajo del umbral del 80%, razón por la cual se requiere definir estrategias y proyecto que permita incrementar el % de implementación del MSPI en cada uno de los dominios y reducir la brecha de Seguridad Digital.

En la siguiente grafica radial se observa la situación actual en cada uno de los dominios de NTC-ISO/IEC 27001.

Imagen No.4 - Brechas de Seguridad Digital del Modelo de Seguridad y Privacidad de la Información (MSPI).

A continuación, se detalla el avance del ciclo PHVA en el modelo de operación:

AVANCE PHVA		
COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
Planificación	33%	40%
Implementación	15%	20%
Evaluación de desempeño	17%	20%
Mejora continua	20%	20%
TOTAL	85%	100%

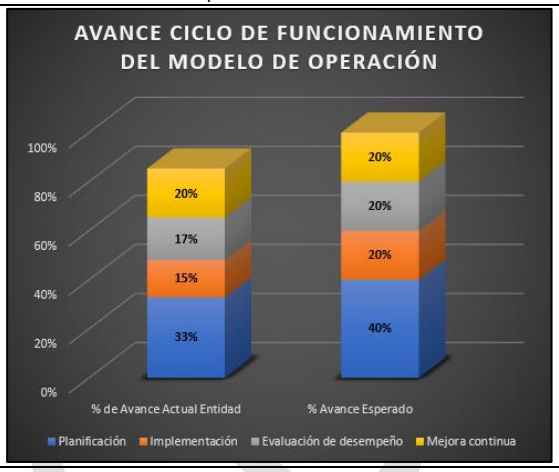

Imagen No.5 - Ciclo PHVA del Modelo de Seguridad y Privacidad de la Información (MSPI).

A continuación, se detalla el avance del modelo del Framework de Ciberseguridad de NIST:

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de f	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	80	100
DETECTAR	84	100
RESPONDER	76	100
RECUPERAR	87	100
PROTEGER	81	100

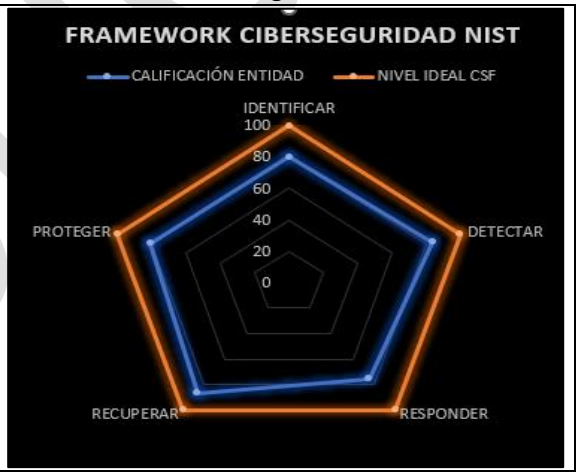

Imagen No.6 - Framework de NIST.

7. ESTRATEGIA DE SEGURIDAD DIGITAL.

La Gobernación de Antioquia adoptara estrategias 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 Digital de acuerdo con las directrices de la resolución No.500 del 2021 de MinTIC.

La estrategia de Seguridad Digital debe definirse en la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI.

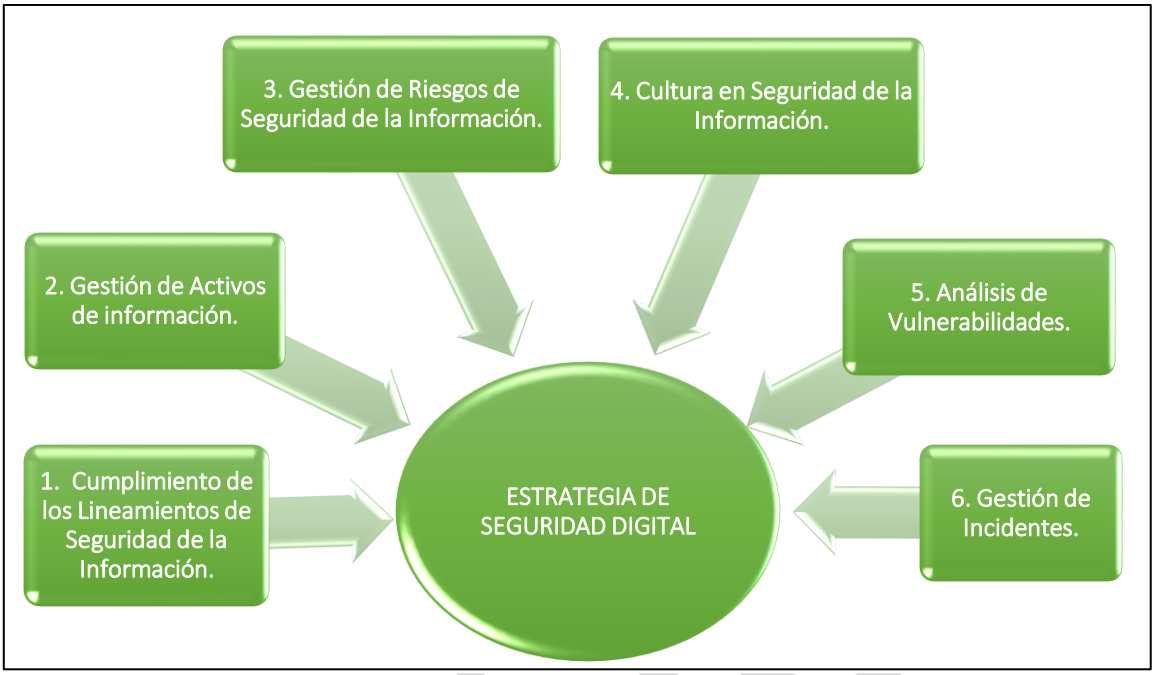

Imagen No.7 - Estrategias.

7.1. DESCRIPCIÓN DE LA ESTRATEGIAS.

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	Descripción / Objetivo
1. Cumplimiento de los lineamientos de Seguridad de la Información.	El cumplimiento de los lineamientos de Seguridad de la Información implica que las personas con las que tiene un vínculo directo o indirecto con la Gobernación de Antioquia que cumplan con las buenas prácticas de seguridad definidas, esto con el fin de garantizar la protección de los activos de información y la preservación Confidencialidad, Integridad y Disponibilidad frente a las amenazas internas o externas, deliberadas o accidentales.
2. Gestión de activos de información.	La gestión de activos de información es una parte fundamental de un Sistema de Gestión de la Seguridad de la Información (SGSI), que es un conjunto de políticas, procedimientos y normas que se basan en el estándar internacional ISO 27001 y que buscan garantizar la Confidencialidad, Integridad y Disponibilidad de la información.

3. Gestión de Riesgos de Seguridad de la Información.	La Gestión de Riesgos de Seguridad de la Información es el proceso de identificar, analizar, evaluar y tratar los riesgos que pueden afectar a la Confidencialidad, Integridad y Disponibilidad de los activos de información. La Gestión de Riesgos de Seguridad de la Información se alinea con la norma internacional ISO 31000 de igual forma toma como referencia la ISO 27005, que proporciona directrices para la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI).
4. Cultura en Seguridad de la Información.	La cultura en seguridad de la información permite fomentar mediante programas de sensibilización, capacitación, comunicación y motivación, que involucren a todos los niveles de la Entidad, desde la alta dirección hasta los usuarios finales.
5. Análisis de vulnerabilidades.	El análisis de vulnerabilidades es un proceso que consiste en identificar, evaluar y priorizar las debilidades y fallas en los sistemas, aplicaciones y redes de la Entidad que podrían ser aprovechadas por un eventual ciberataque, cuya finalidad es detectar las vulnerabilidades que hay antes de que estas sean explotadas por alguna ciber-amenaza.
6. Gestión de Incidentes.	La gestión de incidentes es el proceso de identificar, analizar, evaluar y tratar los eventos no planificados o interrupciones del servicio que afectan a la seguridad, la calidad o el rendimiento de la información, los sistemas y los recursos de una organización. Su objetivo es restablecer el funcionamiento normal lo antes posible, minimizar el impacto negativo y evitar que se repitan los incidentes.

Tabla No.4 - Descripción de los Objetivos de las Estrategias.

7.2. PORTAFOLIO DE PROYECTOS Y PRODUCTOS ESPERADOS.

La Gobernación de Antioquia, defines para cada estrategia, proyectos y productos esperados, que tienen como objetivo aumentar el % de implementación del MSPI y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

Estrategia	Proyecto	Producto Esperado
1. Cumplimiento de los lineamientos de Seguridad de la Información.	Proyecto No.1.1.: Implementar de controles de Seguridad de la Información.	Producto Esperado No.1.1.1.: Afinamiento a los dispositivos de Seguridad Informática.
		Producto Esperado No.1.1.2.: Cumplimiento de los controles de seguridad definidos.

		Producto Esperado No.1.1.3.: Contratación de Bienes y Servicios de Seguridad Informática para mitigar riesgos sobre la Infraestructura Tecnológica de la Entidad.
		Producto Esperado No.1.1.4.: Definición y actualización de la documentación en materia de Seguridad de la Información.
2. Gestión de activos de información.	**Proyecto No.2.1.:** Actualizar e identificar los activos de información.	**Producto Esperado No.2.1.1.:** Socializar los Lineamientos e instrumentos para el registro de los activos de información.
		Producto Esperado No.2.1.2.: Mesas de trabajo con los procesos para la actualización e identificación de activos de información.
		Producto Esperado No.2.1.3.: Consolidación y entrega de los activos de información para la emisión del Concepto Jurídico.
		Producto Esperado No.2.1.4.: Socialización de los activos de información definitivos a cada proceso.
		Producto Esperado No.2.1.5.: Presentación de los instrumentos públicos de: Registro de Activos de información. Índice de Información Clasificada y Reservada, Esquema de Publicación de Información, al Comité Institucional de Gestión y Desempeño del Gobernación de Antioquia para su aprobación mediante acto administrativo.
		Producto Esperado No.2.1.6.: Publicación de los instrumentos públicos de: - Registro de Activos de información. - Índice de Información Clasificada y Reservada. - Esquema de Publicación de Información.

3. Gestión de Riesgos de Seguridad de la Información.	**Proyecto No.3.1.:** Identificar, evaluar y realizar seguimiento de los riesgos de Seguridad de la Información.	**Producto Esperado No.3.1.1.:** Solicitar la identificación y valoración de riesgos de Seguridad de la Información con cada proceso de la Entidad.
		Producto Esperado No.3.1.2.: Seguimiento al plan de tratamiento de riesgos de Seguridad de la Información.
4. Cultura en Seguridad de la Información.	**Proyecto No.4.1.:** Definir y ejecutar un Plan de Cultura y Sensibilización en Seguridad de la Información.	**Producto Esperado No.4.1.1.:** Definir el Plan de Cultura y Sensibilización en Seguridad de la Información 2025.
		Producto Esperado No.4.1.2.: Realizar la ejecución y seguimiento al Plan de Cultura y Sensibilización en Seguridad de la Información 2025.
5. Análisis de vulnerabilidades.	**Proyecto No.5.1.:** Ejecutar análisis de (test y re-test) de vulnerabilidades técnicas a la Plataforma Tecnológica.	**Producto Esperado No.5.1.1.:** Ejecución de análisis de vulnerabilidades técnicas sobre la Plataforma Tecnológica.
		Producto Esperado No.5.1.2.: Elaboración y entrega del informe de análisis de vulnerabilidades a los responsables de los Servicios TI para que efectúen su remediación con el fin de mitigar brechas de seguridad.
		Producto Esperado No.5.1.3.: Ejecución de re-test de vulnerabilidades técnicas sobre la Infraestructura Tecnológica.
		Producto Esperado No.5.1.4.: Elaboración y entrega del informe de re-test de vulnerabilidades a los responsables de los Servicios TI para que efectúen su remediación con el fin de mitigar brechas de seguridad.
6. Gestión de Incidentes.	**Proyecto No.6.1.:** Atender los incidentes de seguridad identificados y reportados.	**Producto Esperado No.6.1.1.:** Atención de los casos reportados e identificados de incidentes de seguridad.

Tabla No.5 - Portafolio de Proyectos y Productos Esperados.

7.3. CRONOGRAMA DE PROYECTOS.

La Gobernación de Antioquia en cabeza de la Dirección de Tecnología e Información toma como base los proyectos anteriormente definidos y establece un cronograma de donde se evidencie como se llevarán a cabo cada uno de los proyectos.

AÑO 2024				
Proyecto	Actividades	2025	2026	2027
No.1.1.	Revisión y actualización de políticas a las herramientas de seguridad informática.	X	X	X
	Revisión del cumplimiento de los Controles de Seguridad.	X	X	X
	Contratación de Bienes y Servicios, de acuerdo con los recursos asignados.	X	X	X
	Actualización de la documentación de Seguridad de la Información.	X	X	X
No.2.1.	Socializar los lineamientos de los activos de información.	X	X	X
	Identificación de activos de información.	X	X	X
	Entrega del consolidado de activos de información.	X	X	X
	Presentación de los activos de información identificados.	X	X	X
	Entrega de los instrumentos públicos (activos de información) al comité para aprobación.	X	X	X
	Publicación de los instrumentos públicos de los activos de información.	X	X	X
No.3.1.	Solicitar la identificación y valoración de riesgos de Seguridad de la Información con cada proceso de la Entidad.	X	X	X
	Seguimiento al plan de tratamiento de riesgos de Seguridad de la Información.	X	X	X
No.4.1.	Definir el Plan de Cultura y Sensibilización en Seguridad de la Información para la vigencia.	X	X	X
	Realizar ejecución y seguimiento a las actividades definidas en el Plan de Cultura y Sensibilización en Seguridad de la Información para la vigencia.	X	X	X
No.5.1.	Ejecución de análisis de vulnerabilidades técnicas.	X	X	X
	Elaboración y entrega del informe de vulnerabilidades.	X	X	X
	Ejecución de re-test de vulnerabilidades técnicas.	X	X	X
	Elaboración y entrega del informe del re-test vulnerabilidades.	X	X	X
No.6.1.	Atención de los casos por incidentes de seguridad.	X	X	X

Tabla No.6 - Cronograma de Proyectos.

Nota: La Gobernación de Antioquia, al finalizar cada vigencia realizará una actualización del cronograma, incorporando el estado del avance de los proyectos formulados y si estos cumplieron o si se requiere ajustar tiempos 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. DOCUMENTOS DE REFERENCIA.

EL Plan Estratégico en Seguridad de la Información (PESI) toma como base los siguientes documentos para su estructura:

- Manual de Gobierno Digital MinTIC.
- MSPI - Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Modelo Integrado de Planeación y Gestión (MIPG) del DAFP.
- Plan Estratégico de Tecnología de la Información (PETI) de la Gobernación de Antioquia.
- Manual de Lineamientos de Seguridad de la Gobernación de Antioquia.

TABLAS

Tabla No.1 - Equipo que trabajo y apoyó en la construcción del PESI. 3
Tabla No.2 - Normatividad Aplicable. 9
Tabla No.3 - Resultado FURAG Políticas Gobierno Digital y Seguridad Digital. 13
Tabla No.4 - Descripción de los Objetivos de las Estrategias. 17
Tabla No.5 - Portafolio de Proyectos y Productos Esperados. 19
Tabla No.6 - Cronograma de Proyectos. 20

IMÁGENES

Imagen No.1 - Mapa de Procesos de la Gobernación de Antioquia. 7
Imagen No.2 - Responsables en Seguridad de la Información. 12
Imagen No.3 - Seguimiento al MSPI. 14
Imagen No.4 - Brechas de Seguridad Digital del Modelo de Seguridad y Privacidad de la Información (MSPI). 14
Imagen No.5 - Ciclo PHVA del Modelo de Seguridad y Privacidad de la Información (MSPI). 15
Imagen No.6 - Framework de NIST. 15
Imagen No.8 - Estrategias. 16