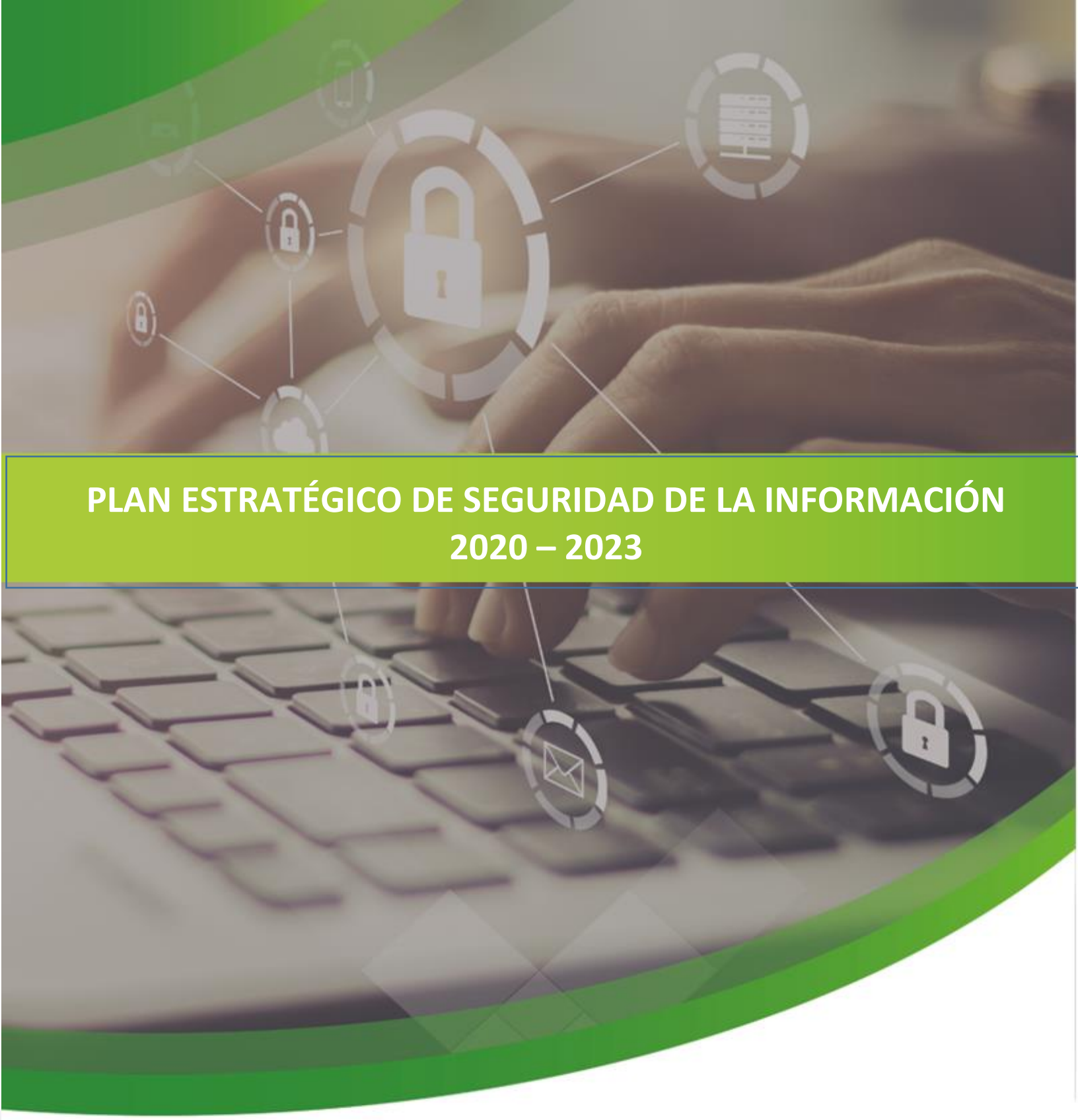

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2020 – 2023

GOBERNACIÓN DE ANTIOQUIA
SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

UNIDOS

Andrés Orlando López Lujan

Secretario de Tecnologías de Información y las comunicaciones

Patricia Restrepo Vélez

Directora de Tecnología e Información

Secretaría de Tecnologías de Información y las Comunicaciones

2020 - 2023

GOBERNACIÓN DE ANTIOQUIA

SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

UNIDOS

Equipo que trabajo y apoyó en la construcción del PESI.

Nombre	Rol
Andrés Orlando López Luján	Secretario de Tecnologías de Información y las Comunicaciones.
Patricia Restrepo Vélez	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	
Mateo Perez Perez	

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

Tabla de Contenido

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 27001:2013, la cual establece los requisitos de la implementación del SGSI, la NTC/ISO 31000:2018; que proporciona un esquema para la gestión de riesgos y las mejores prácticas, tales como la 27002:2015, ISO 27005:2009, 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 Tecnologías 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 Tecnologías de la Información y las Comunicaciones – TIC's como contribución al logro de los Objetivos y Lineamientos Estratégicos enmarcados en el Plan Estratégico Institucional, Plan Diamante 2016-2022. El PESI descrito en este documento está alineado completamente con el PETI.

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 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 y de Apoyo) y de gestión de la información y gobernabilidad de TI, de acuerdo con la Estrategia Gobierno en Línea - GEL del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC (Para mayor información ver PETI).

Finalmente, los lineamientos y proyectos para el desarrollo, optimización e implementación efectiva de los Sistemas de Información, así como las iniciativas que permitirán una adecuada gestión de la Infraestructura de Hardware/Software, basados en el Modelo de Seguridad y Privacidad de la Información – MSPI y en las mejores prácticas de Gestión de Servicios y Proyectos de TI, contribuirán 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 y la protección de los activos de información (PETI).

1. GENERALIDADES.

El Plan de Seguridad y Privacidad de la Información 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 entidad, el presente documento permite plasmar la situación actúa con el fin de trazar estrategias que permiten mejorar la postura de seguridad digital.

2. OBJETIVO.

Definir un Plan Estratégico de Seguridad de la Información, en adelante PESI, liderada por la Dirección de Tecnología Información de la Gobernación de Antioquia, en adelante GOBANT, a partir de la vigencia 2020 hasta el año 2023, que responda a las necesidades de preservar la confidencialidad, la integridad y la disponibilidad sobre los activos de información.

2.1. Objetivos Específicos.

- Comunicar e implementar la Estrategia de Seguridad de la Información.
- Incrementar el nivel de madurez en la gestión de la seguridad de la información.
- Implementar y apropiar el Modelo de Privacidad y Seguridad de la Información MPSI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
- Hacer uso eficiente de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.) para garantizar la continuidad en la prestación de los servicios.
- Definir las responsabilidades relacionadas con el manejo de la seguridad.
- Establecer una metodología de gestión de seguridad de la información clara y estructurada.
- Reducir el riesgo de pérdida, robo o corrupción de información.
- Garantizar que los usuarios tengan acceso a la información a través de medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de esta.
- Cumplir con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Optimizar la seguridad de la información con base en la gestión de procesos.

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 27001:2013 – Sistema de Gestión de Seguridad de la Información, así como el fortalecimiento de la infraestructura de ciberseguridad de la Gobernación de Antioquia.

La Gobernación de Antioquia, define la aplicabilidad de sus requisitos de la norma NTC-ISO/IEC 27001:2013 y todos los controles del Anexo A de la misma norma.

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.
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.
Instrumento MSPI	22 de Febrero 2021	Modelo de Seguridad y Privacidad de la Información. Generado por MinTIC.

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.

- **CIA:** Véase: CID. Acrónimo inglés de Confidentiality, Integrity y Availability, las dimensiones básicas de la seguridad de la información. Acrónimo español (CIA) de Confidencialidad, Integridad y Disponibilidad, las dimensiones básicas de la seguridad de la información.

- **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).

- **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.

- **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.

- **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:** (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.

Para la Gobernación de Antioquia es muy importantes los resultados obtenidos por el Plan Estratégico de Seguridad de la Información (PESI) dado que con él se sustenta:

La implementación del Sistema de Gestión de seguridad de la Información (SGSI) de la entidad.

- El Plan Estratégico de Tecnologías de la Información (PETI) de la entidad, el cual se fundamenta en la metodología de BSC o Cuadro de Mando Integral, debido a su gran utilidad en el direccionamiento de las entidades.

- De acuerdo con la expedición del Decreto 2573 de 2014 contenida en el Decreto Único Reglamentario 1078 de 2015 del sector de Tecnologías de la Información y las Comunicaciones y actualizado según el decreto No.1008 del 14 de junio del 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.

La Secretaria de Tecnología de la Información y las Comunicaciones quien en adelante se llamara Secretaria de TIC, 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 el Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital[1].

El modelo se basar en el ciclo PHVA, el cual recomienda la norma NTC-ISO/IEC 27001:2013 y la GTC-ISO/IEC 27002:2015.

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

6.1. Enfoque Organizacional.

La división del enfoque comprende lo siguiente:

- **Estratégico:** Está orientado a definir objetivos claros tanto a: corto, mediano y largo plazo con el fin de prevalecer la Confidencialidad, Integridad, Disponibilidad y Privacidad de la información las cuales pueden ser afectadas por vulnerabilidades de seguridad de informática y el cumplimiento de los lineamientos de seguridad de la información.

- **Táctico:** Está orientado a gestionar e implementar el Modelo de Seguridad y Privacidad de la Información (MSPI) dentro de la entidad y la atención de requerimientos de seguridad de cada uno de los procesos y de los respectivos entes de control, así como la ejecución del Plan de cultura y sensibilización en seguridad de la información a funcionarios, contratistas, terceros y la ciudadanía de la Gobernación de Antioquia.

[1] Fuente de consulta: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

- **Operativo:** Está orientado a gestionar y monitorear las herramientas técnicas adquiridas por la entidad con el fin de blindar la protección necesario para la Confidencialidad, Integridad, Disponibilidad y Privacidad de la información. Este enfoque se soporta por la Mesa de Servicios Tecnológicos quien realiza la atención de los requerimientos de los usuarios en materia de seguridad y el afinamiento de las herramientas existentes.

6.2. 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 Secretaria de TIC.

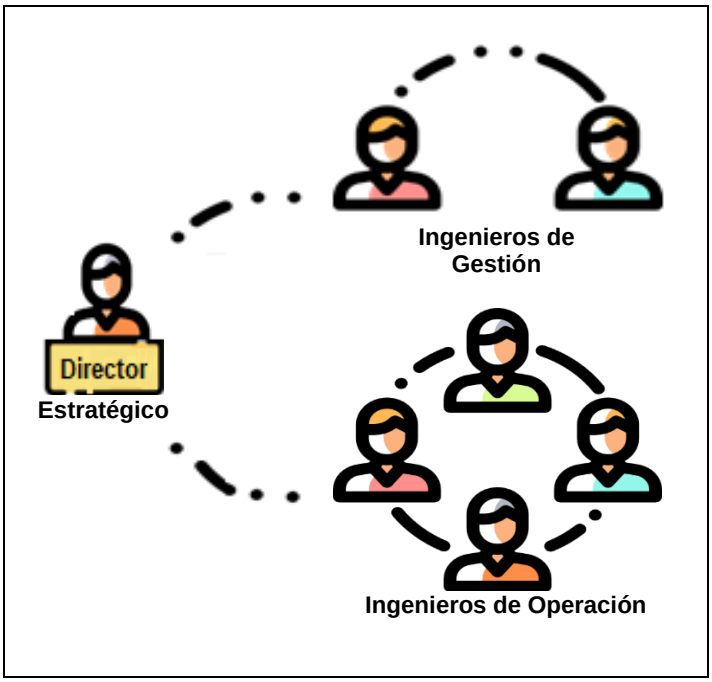

Imagen No.2 - Responsables en Seguridad de la Información.

6.3. 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, se observa en la siguiente imagen los resultados obtenidos en los años 2018,2019, 2020 y 2021 respecto al cumplimiento de las políticas de Gobierno Digital y Seguridad Digital con un desempeño sobresaliente gracias al trabajo realizado en 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 siguiente link: Resultado de desempeño.

III. Índices de las políticas de gestión y desempeño

Índice	2018	2019	2020	2021
POL06: Gobierno Digital	84,0	96,0	97,2	98,1
POL07: Seguridad Digital	83,5	82,5	95,1	96,6

Imagen No.3 - Resultado FURAG Políticas.

6.4. Ejecución del Modelo de Seguridad y Privacidad de la Información (MSPI).

En 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 a la norma NTC-ISO/IEC 27001:2013 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	90	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	84	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	80	100	GESTIONADO
A.9	CONTROL DE ACCESO	81	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	90	100	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	82	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	72	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	71	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	77	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	80	100	GESTIONADO
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	95	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		**79**	**100**	GESTIONADO

Imagen No.4 - Seguimiento al MSPI.

Se identifican algunos dominios que se encuentra por debajo del umbral del 75%, 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 ISO 27001:2013.

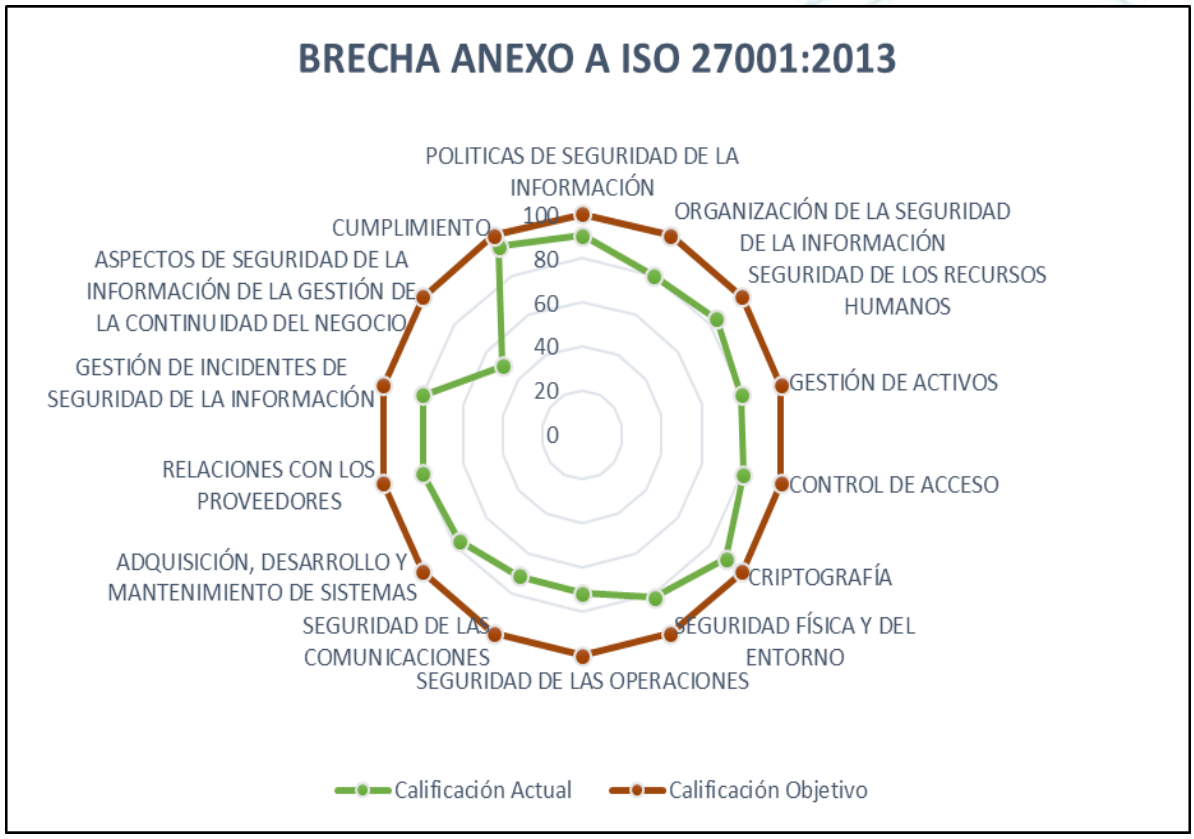

Imagen No.5 - Brechas de Seguridad Digital.

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%**

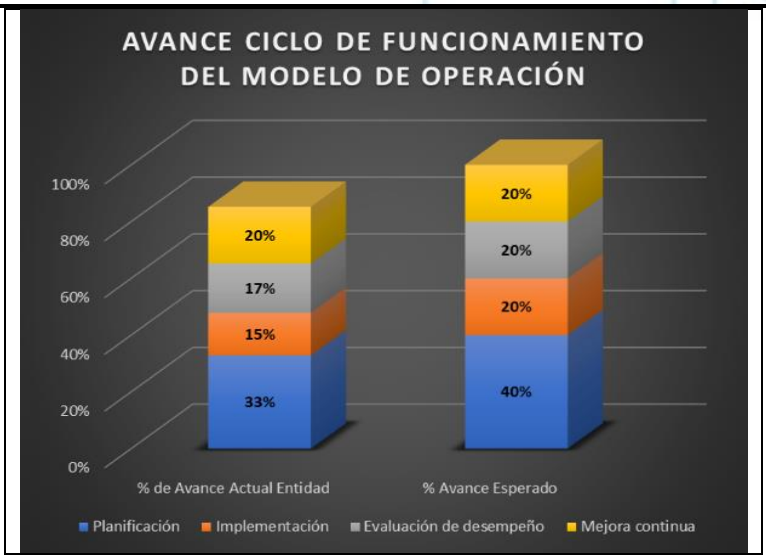

Imagen No.6 - Ciclo PHVA del Modelo de Seguridad y Privacidad de la Información (MSPI).

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

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
	CALIFICACIÓN ENTIDAD	**NIVEL IDEAL CSF**
IDENTIFICAR	78	100
DETECTAR	80	100
RESPONDER	74	100
RECUPERAR	87	100
PROTEGER	76	100

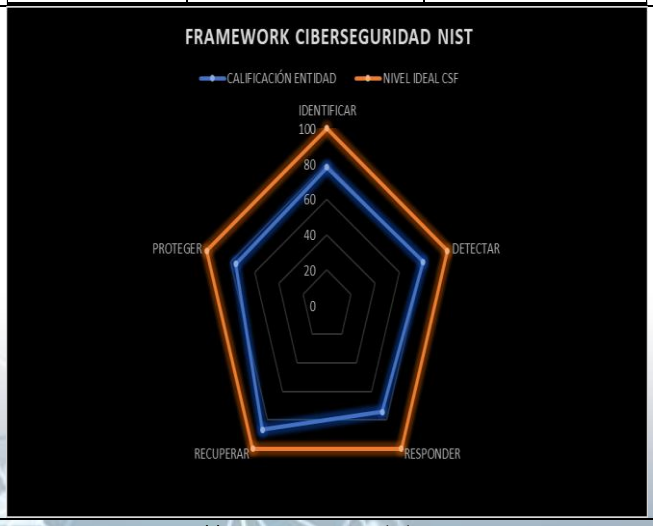

Tabla No. 3 - Framework de NIST.

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 a 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

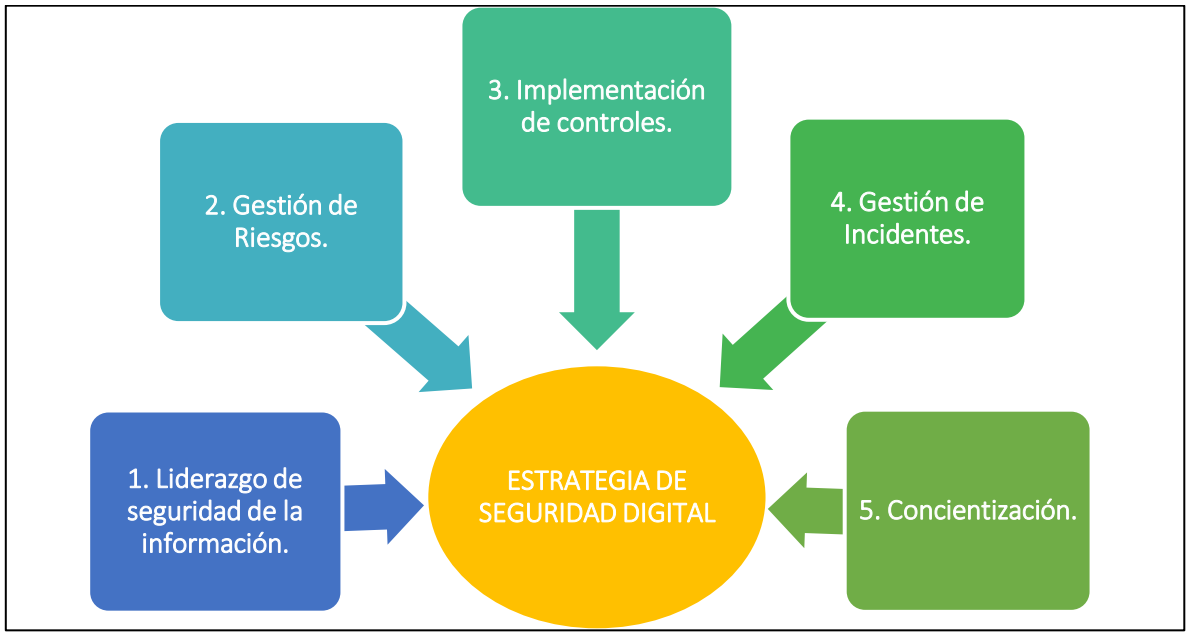

Imagen No.7 - Estrategias.

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

2. Gestión de riesgos.	Determinar los riesgos de seguridad de la información de la Gobernación de Antioquia, 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.
3. Concientización.	Fortalecer la construcción de la cultura organizacional de la Gobernación de Antioquia, 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.
4. Implementación de controles.	Planificar e implementar las acciones necesarias en la Gobernación de Antioquia, para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, a través de la implementación de controles tecnológicos y/o administrativos.
5. Gestión de incidentes.	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Gobernación de Antioquia.

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	PRODUCTOS ESPERADOS
1. Liderazgo de seguridad de la información.	**Proyecto No.1.1:** Actualizar los lineamientos de seguridad de la información.	**Producto No.1.1.1:** Política de Seguridad publicada en el sistema de gestión de la calidad.
	Proyecto No.1.2: Actualizar documentación relacionada con Seguridad de la Información.	**Producto No.1.2.1:** Actualización de la documentación existente en Seguridad de la Información que se encuentra en el sistema de gestión de la calidad. **Producto No.1.2.2:** Definición de nuevos procedimientos, guías, protocolos, formatos e instructivos de seguridad de la información.

2. Gestión de riesgos.	**Proyecto No.2.1:** Participar en la Actualización de la metodología de riesgos de Seguridad Digital en la Entidad.	**Producto No.2.1.1:** Metodología de riesgos aplicando las directrices del DAFP relacionadas con Seguridad Digital.
	Proyecto No.2.2: Identificar los riesgos de Seguridad Digital.	**Producto No.2.2.1:** Matriz de riesgos de Seguridad Digital.
	Proyecto No.2.3: Definir planes de tratamiento de riesgos de Seguridad Digital.	**Producto No.2.3.2:** Definir planes de tratamiento de riesgos de Seguridad Digital.
3. Concientización.	**Proyecto No.3.1:** Establecer Plan de Cultura y Sensibilización en Seguridad de la información para la vigencia.	**Producto No.3.3.1:** Plan de Cultura y Sensibilización en Seguridad de la información para la vigencia.
	Proyecto No.3.2: Realizar la ejecución de las actividades definidas en el Plan de Cultura y Sensibilización en Seguridad de la información para la vigencia.	**Producto No.3.2.1:** Evidencias de registros fotográficos de las charlas efectuadas, infografía, protector de pantalla, cuñas de audio, videos de seguridad.
4. Implementación de controles.	**Proyecto No.4.1:** Realizar seguimiento al instrumento del MPSI implementado en la entidad.	**Producto No.4.1.1:** Actualización del MSPI mensual.
	Proyecto No.4.2: Realizar investigación de nuevas herramientas tecnológicas que mejoren la postura de Seguridad Digital en la Entidad.	**Producto No.4.2.1:** Estudio de mercado de las herramientas tecnológicas que mejoren la postura de Seguridad Digital en la Entidad. **Producto No.4.2.2:** Realizar pruebas de concepto con el fin de identificar necesidades en Seguridad Digital.
	Proyecto No.4.3: Implementar DFA en el correo electrónico para usuarios privilegiados que administran las herramientas tecnológicas de la Entidad.	**Producto No.4.3.1:** Política DFA aplicada a los administradores de las herramientas tecnológicas de la Entidad.
5. Gestión de incidentes.	**Proyecto No.5.1:** Revisar la documentación del procedimiento de incidentes de Seguridad.	**Producto No.5.1.1:** Actualizar la documentación relacionada con el procedimiento de incidentes de seguridad en caso de que se requiera.
	Proyecto No.5.2: Asistir a reuniones de actualización frente a la gestión de incidentes de seguridad de la información.	**Producto No.5.2.1:** Proyecto No.2: Sesiones de capacitación desarrolladas.

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

7.3. Cronograma de Proyectos.

La Gobernación de Antioquia en cabeza de la Secretaria de TIC 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.

<table>
<tr><th colspan="4">AÑO 2023</th><th colspan="2">AÑO 2024</th></tr>
<tr><th>TRIMESTRE 1</th><th>TRIMESTRE 2</th><th>TRIMESTRE 3</th><th>TRIMESTRE 4</th><th>TRIMESTRE 1</th><th>TRIMESTRE 2</th></tr>
<tr><td></td><td></td><td></td><td>Participar en la Actualización de la metodología de riesgos de Seguridad Digital en la Entidad.</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td>Identificar los riesgos de Seguridad Digital.</td><td>Identificar los riesgos de Seguridad Digital.</td><td>Definir planes de tratamiento de riesgos de Seguridad Digital.</td></tr>
<tr><td>Establecer Plan de Cultura y Sensibilización en Seguridad de la información para la vigencia.</td><td colspan="3">Realizar la ejecución de las actividades definidas en el Plan de Cultura y Sensibilización en Seguridad de la información para la vigencia.</td><td>Establecer Plan de Cultura y Sensibilización en Seguridad de la información para la vigencia.</td><td>Realizar la ejecución de las actividades definidas en el Plan de Cultura y Sensibilización en Seguridad de la información para la vigencia.</td></tr>
<tr><td colspan="4">Realizar seguimiento al instrumento del MPSI implementado en la Entidad.</td><td colspan="2">Realizar seguimiento al instrumento del MPSI implementado en la Entidad.</td></tr>
<tr><td>Implementar DFA en el correo electrónico para usuarios privilegiados que administran las herramientas tecnológicas de la Entidad.</td><td></td><td></td><td></td><td>Implementar DFA en el correo electrónico para usuarios privilegiados que administran las herramientas tecnológicas de la Entidad.</td><td></td></tr>
<tr><td></td><td></td><td></td><td>Revisar la documentación del procedimiento de incidentes de Seguridad.</td><td></td><td></td></tr>
<tr><td colspan="4">Asistir a reuniones de actualización frente a la gestión de incidentes de seguridad de la información.</td><td colspan="2">Asistir a reuniones de actualización frente a la gestión de incidentes de seguridad de la información.</td></tr>
</table>

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.

7.4. Proyección de Costos.

Con base a los proyectos definidos en la estrategia de implementación de controles, se debe proyectar costos aproximados tomando como base el estudio de mercado para ser presentados a la Alta Dirección para su consideración y viabilidad pertinente.

Previo al estudio de mercado se realizó RoadMap de adquisiciones de herramientas tecnológicas que mejoran la postura en Seguridad Digital en la Entidad. Los costos están sujetos a la TRM del dólar del día.

Necesidades año 2023	Proyección de costo
Perfilamiento de seguridad para conexiones a redes.	USD 36.792,66
Fortalecimiento de seguridad en Office 365 y Azure.	USD 49.056,88
SOC.	USD 73.585,32
Ethical Hacking.	USD 28.00,00
Fortalecimiento en la plataforma de seguridad perimetral.	USD 9.811,38
MDM.	USD 12.264,22
Capacitación al equipo de seguridad.	USD 2.452,84
Bóveda de contraseñas.	USD 14.717,06
Consultoría BCP-BIA-DRP.	USD 49.056,88

Tabla No.7 - Proyección Costo.

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 Tecnologías de la Información (PETI) de la Gobernación de Antioquia.

TABLAS

IMÁGENES