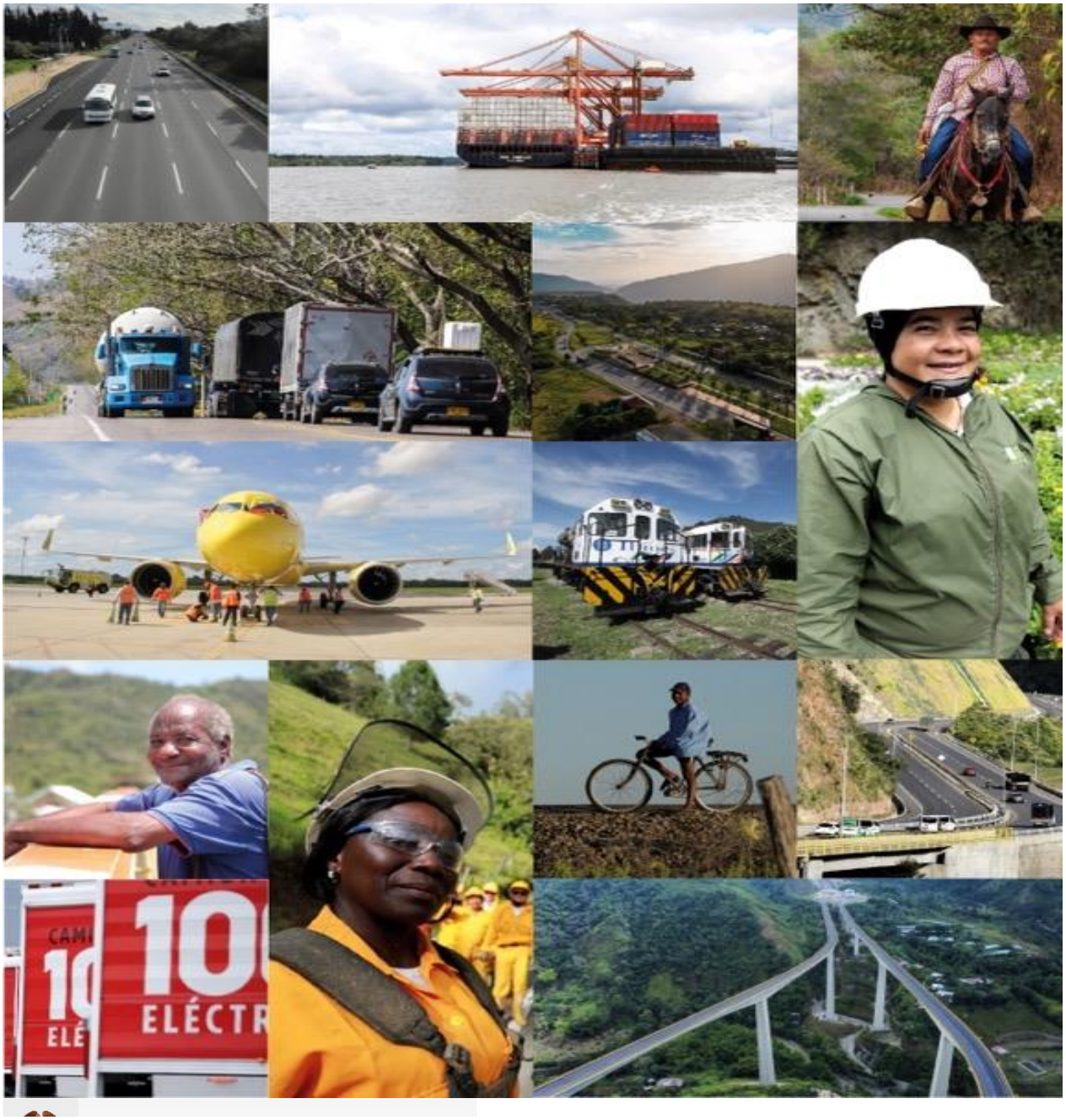


Plan de Seguridad y Privacidad de la Información 2023

1. CONTENIDO

1. INTRODUCCION

El Ministerio de Mintransporte, establece que la información es parte esencial para el logro se sus objetivos estratégicos, por lo cual establece como fundamental, el mantenimiento de su Sistema de Gestión de Seguridad de la Información, que permita asegurar la protección de sus activos de información, y con esto el logro de su misión y visión.

Bajo esta perspectiva, con el fin de mantener y mejorar su Sistema de Gestión de Seguridad de la Información, instituye el Plan de Seguridad y Privacidad de la Información, donde se establecen los aspectos para tener en cuenta para el mantenimiento y mejora continua de su sistema, y que cumple con los mejores estándares a nivel nacional e internacional.

Para lo anterior se establecen por medio de un análisis de la situación actual y deseada, así mismo se plantean las herramientas y diferentes aspectos como proyectos y actividad que se requieren para llevar la entidad, a un nivel adecuado para la protección de la confidencialidad, integridad y disponibilidad de su información, principios fundamentales que constituyen el pilar de la protección de los activos de la información.

2. GENERALIDADES

El Plan de Seguridad y Privacidad de la Información constituye una herramienta para la formulación de planes y cronogramas para el mantenimiento y mejora del Sistema del Gestión de Seguridad de la Información alineado con los objetivos estratégico de la organización, a través del documento se desarrollará la situación actúa del Ministerio y los planes para el logro de la situación deseada.

3. MARCO NORMATIVO

La normatividad que soporta este documento se encuentra fundamentada en el marco de creación de la Entidad y en las recientes políticas para el uso de la tecnología y la seguridad de la información que a continuación se enuncian:

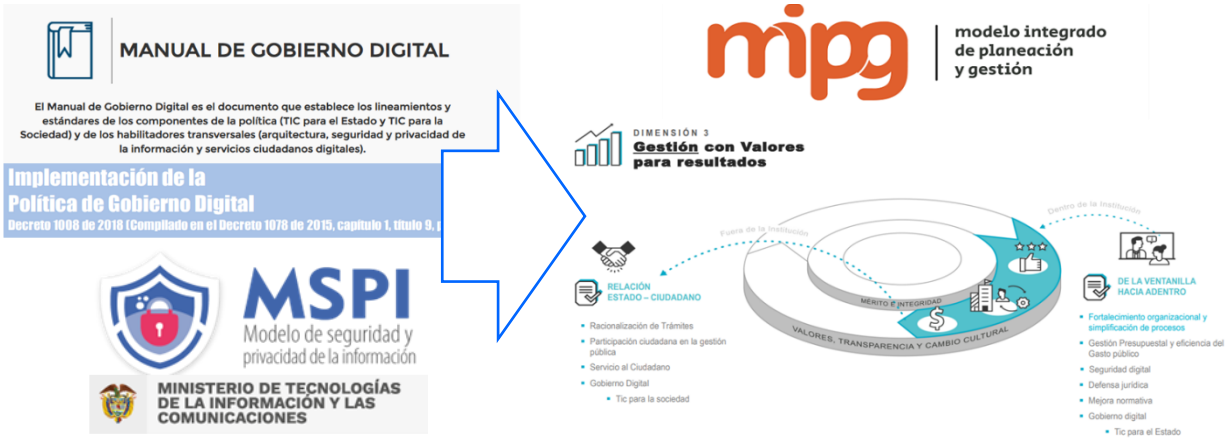
- *Que al otorgarle personería jurídica y asignarle un patrimonio propio a la MINISTERIO DE TRANSPORTE (MINTRANSPORTE), con fundamento en el literal e), del artículo 18 de la Ley 1444 de 2011, se fortalece la entidad y se obtiene una mayor independencia técnica, administrativa y financiera, permitiendo una mayor eficiencia en la prestación del servicio público.*
- *Decreto 415 de 2016, por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones*

- *Ley 1273 de 2009, 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 ".*
- *Decreto 1499 de 2017 Artículo 2.2.22.3.1. Actualiza el Modelo Integrado de Planeación y Gestión - MIPG.*
- *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.*
- *Decreto 1008 de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.*

4. ALINEACIÓN INSTITUCIONAL

El sistema de gestión de seguridad de la información (SGSI) y el presente Plan Estratégico de Seguridad de la Información (PESI), se integran y contribuyen a la consecución del Plan Estratégico Institucional y de los elementos que la componen. Asi mismo, se alinean con el Modelo Integrado de Planeación y Gestión (MIPG) en la dimensión "Gestión con valores para resultados" – Políticas de Gobierno Digital y Seguridad Digital.

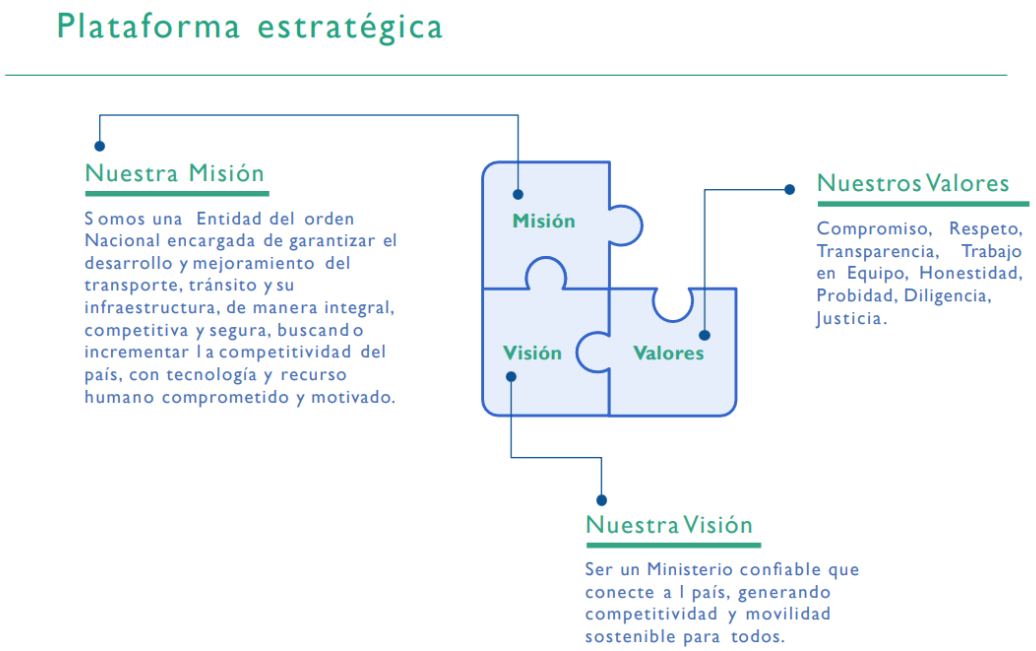
Con lo anterior el presente plan se establece, con el fin de dar cumplimiento a los lineamientos, estándares y acciones a ejecutar para el desarrollo de los componentes y habilitadores transversales de la política de Gobierno Digital, relacionados con seguridad de la Información y el mantenimiento del Modelo de Seguridad y Privacidad de la Información establecido por el MINTIC como cumplimiento de la política de Seguridad Digital y que son de obligatorio cumplimiento.



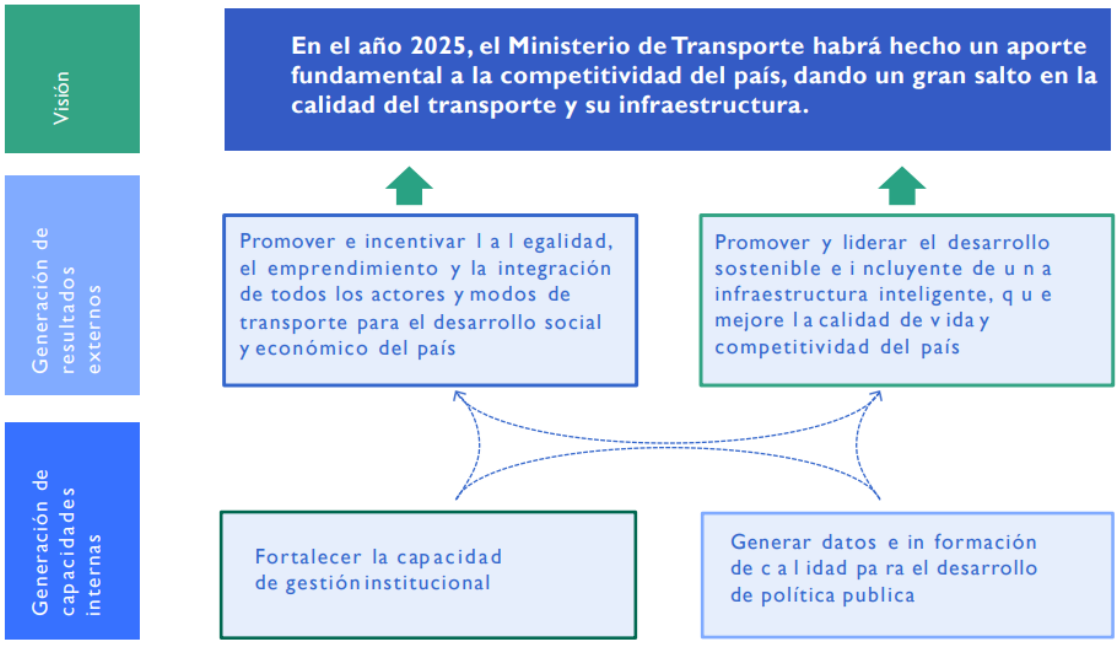
Gestión con Valores para Resultados	DESCRIPCIÓN DE RELACIÓN
Gobierno digital	*La Política de Gobierno Digital es la política del Gobierno Nacional que propende por la transformación digital pública. Con esta política pública se busca fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública y el Estado en general, a través del uso y aprovechamiento de las TIC. Hace parte del Modelo Integrado de Planeación y Gestión - MIPG y se integra con las políticas de Gestión y Desempeño Institucional.* *Dentro de la política se encuentran los habilitadores transversales, que corresponde a las capacidades que les permitan ejecutar las Líneas de Acción de la Política de Gobierno Digital, en los cuales como base de encuentra la Seguridad y Privacidad de la información, de tal forma que se puedan brindar servicios seguros y confiables a la ciudadanía.*
Seguridad Digital	*Esta Política en Seguridad Digital tiene también un fuerte enfoque hacia el ciudadano, ya que el Gobierno busca crear condiciones para que todos gestionemos el riesgo de seguridad digital en nuestras actividades digitales, fomentando la*

	confianza en el entorno digital como medio para alcanzar nuestros objetivos. *para ello las entidades del Estado deben implementar acciones para que los ciudadanos realicen trámites con el Estado y todo tipo de actividades soportadas en medios digitales de forma segura, con lo anterior se vuelve obligatoria la implementación del Modelo de Seguridad y Privacidad de la Información del MINTIC, con el fin de proteger los activos de seguridad de la información de la entidad, y con esto los servicios e información de los ciudadanos.*

Adicional a los aspectos relacionados con el Modelo Integrado de Gestión y Planeación (MIPG), el presente plan se alinea con la plataforma estratégica, la cual está compuesta de 3 componentes: Misión, Visión y Valores, los cuáles se definen en la siguiente gráfica:



El mapa estratégico define 4 objetivos que buscan direccionar a la entidad en el cumplimiento de su visión. Estos objetivos buscan fortalecer a la entidad en dos perspectivas, el primero a través de la generación de resultados externos (Front-Office) y el segundo a través de la generación de capacidades al interior de la entidad (Back-Office).



Para el logro de los objetivos y metas estratégicas, el Ministerio de Transporte establece como plataforma su Sistema de Gestión de Seguridad de la Información, de tal forma que permita la protección de infraestructura y sistemas inteligentes, y con lo anterior se pueda generar datos e información de calidad mitigando los posibles riesgos asociados a la Integridad, confidencialidad y disponibilidad de esta, brindando apoyo a la visión de la entidad y alineado con el objetivo de Gobierno Digital de generar valor público en un entorno de confianza digital.

Para lo anterior se definen varios proyectos con el fin de actualizar y fortalecer los servicios tecnológicos por medio de la adopción de las últimas tendencias tecnologías en seguridad digital y de la información, apoyando el desarrollo de las estrategias del manual de Gobierno Digital y el logro de la visión del Ministerio de Transporte.

4.1. ALINEACIÓN ESTRATÉGICA DEL PESI CON EL PETI DE LA ORGANIZACIÓN

El PESI se encuentra subordinado pajo el PETI de la MINISTERIO DE TRANSPORTE, apoyando los lineamientos y principios de calidad, servicio y mejora continua establecidos en el plan estratégico de seguridad le información, y apoyando el desarrollo tecnológico de la organización bajo la premisa de salvaguardar la integridad, confidencialidad y disponibilidad de la información a través de sistema seguros que brinden confianza a la ciudadanía y demás partes interesadas de la organización.

Con lo anterior el objetivo estratégico en el que se apoya el presente documento de apoyar la implementación del Plan estratégico de Tecnología de la Información de la organización.

5. OBJETIVO GENERAL

Establecer el plan de acción 2023, para el mantenimiento, gestión y mejora del Sistema de Gestión de Seguridad de la Información (SGSI) del MINISTERIO DE TRANSPORTE alineados con la Política de Gobierno Digital y Plan Estratégico institucional PEI de la Organización mediante la implementación de proyectos estratégicos y actividades para la gestión de riesgos, optimización de recursos y entrega de valor en un entorno de confianza digital seguro.

6. OBJETIVOS ESPECIFICOS

- *Actualizar autodiagnóstico del Sistema de Gestión de Seguridad de la información (SGSI) de la organización, identificando las debilidades actuales que deben ser fortalecidas.*
- *Establecer y priorizar los proyectos y acciones de mejora para la gestión de las debilidades identificadas.*
- *Ejecutar las acciones de mejora y proyectos encaminadas a la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).*
- *Realizar la evaluación y auditoría, de la efectividad de las acciones emprendidas para solucionar las debilidades del sistema y verificar el correcto cumplimiento de los controles y lineamientos implementados en el SGSI.*
- *Actualizar el Plan Estratégico de Seguridad de la Información (PESI) para la vigencia 2023.*

7. ALCANCE

El presente plan contempla la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) en todos los procesos de la Entidad acorde al Modelo de Seguridad y Privacidad de la Información (MSPI) definida por el MINTIC y la norma ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información, así como el fortalecimiento de la infraestructura de ciberseguridad del Ministerio de Transporte.

7.1. ANÁLISIS DE SITUACIÓN ACTUAL

El Ministerio de Transporte 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 (Formulario Único de Registro del Avance en la Gestión).

Con el objetivo de tener una visión del trabajo realizado en los últimos años, se muestran a continuación los resultados obtenidos en los periodos 2018, 2019 y 2020 respecto a las

políticas de Gobierno Digital y Seguridad Digital, las cuales involucran de manera directa la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) definido por MinTIC, denominado Modelo de Seguridad y Privacidad de la Información (MSPI).

Índice	2018	2019	2020	2021
POL06: Gobierno Digital		75,9	81,4	87,9	95,0
POL07: Seguridad Digital	71,6	88,9	88,7	94,7	

Fuente. *Herramienta Power Bi – Comparativo Medición del Desempeño Institucional 2018,2019, 2020 y 2021.* ***Departamento Administrativo de la Función Pública.***

Teniendo en cuenta los criterios anteriores, se observa que el MINISTERIO DE TRANSPORTE en los ámbitos digitales dirigidos al cumplimiento de Gobierno Digital y Política de Seguridad Digital, ha avanzado de forma sobresaliente, demostrando que la madurez de su sistema en los últimos 3 años ha ido creciendo conforme a la correcta implementación de sus Sistema de Gestión de Seguridad de la Información.

De igual forma, de forma paralela a la medición de FURAG, el Ministerio de Transporte realiza la actualización de su autodiagnóstico del Modelo de Seguridad de la Información del MINTIC, donde con base a los resultados se puede establecer el nivel de madurez del Sistema, a continuación, se presenta, el nivel de madurez, donde se encuentra actualmente la entidad.

2019	
Nivel	**Descripción**
(Nivel 1 de 5) Inicial	• Se han identificado las debilidades en la seguridad de la información. • Los incidentes de seguridad de la información se tratan de forma reactiva. • Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.

2022	
Nivel	**Descripción**
(Nivel 4 de 5) Administrado	• Se revisa y monitorea periódicamente los activos de información de la Entidad. • Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información. • Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro. • La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.

Como se evidencia en la gráfica, la entidad inicia en el nivel 1 de madurez en el 2019, donde se identificó que el Ministerio de Transporte, no contaba con controles de seguridad de la

información y por lo tanto presentada una gran probabilidad de exposición de sus activos de información, lo cual involucraba la necesidad de establecer un Sistema de Gestión de Seguridad de la Información con el fin de proteger sus activos.

Con base a la necesidad, se ejecutó un plan de implementación desde el 2019, hasta el 2022, dando como resultado, que actualmente la Entidad, cuente con un Sistema de Gestión de Seguridad de la Información implementado en el nivel 4 (Administrado) de madurez, lo que evidencia un gran avance y una correcta implementación del sistema.

Sin embargo, en el detalle de calificación del autodiagnóstico, también se identifican algunas debilidades, las cuales deben ser trabajadas, para que el sistema pueda llegar a un nivel optimizado. con el fin de profundizar y evidenciar los puntos críticos o debilidades a trabajar. A continuación, se presentan los resultados comparativos del autodiagnóstico proyectado inicialmente en el año 2019 y los actuales del 2022.:

No.	Evaluación de Efectividad de controles		
	DOMINIO	Punto inicial (2019)	Calificación actual (2022)
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	50	100
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	6	86
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	40	93
A.8	GESTIÓN DE ACTIVOS	11	79
A.9	CONTROL DE ACCESO	32	84
A.10	CRIPTOGRAFÍA	0	80
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	31	80
A.12	SEGURIDAD DE LAS OPERACIONES	14	82
A.13	SEGURIDAD DE LAS COMUNICACIONES	25	87
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	11	75
A.15	RELACIONES CON LOS PROVEEDORES	0	80
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	91
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	17
A.18	CUMPLIMIENTO	32,5	84
PROMEDIO EVALUACIÓN DE CONTROLES		18	80

Año	AVANCE PHVA		
	COMPONENTE	% de Avance inicial Entidad	% de Avance Actual Entidad
2015	Planificación	8%	38%
2016	Implementación	2%	18%
2017	Evaluación de desempeño	3%	17%
2018	Mejora continua	6%	16%
		19%	90%

En la gráfica se evidencia, el avance del sistema en cada uno de los dominios, en los que se podrán identificar algunos puntos que se encuentran por debajo de un 80% de cumplimiento, y en los cuales se han identificado las mayores debilidades del sistema actualmente. Estos puntos específicos deben ser fortalecidos para una adecuada implementación del Sistema de Gestión de Seguridad de la Información.

Para lo anterior, se plantea una descripción de la situación actual y situación deseada de los puntos que presentan debilidad en el sistema de gestión seguridad de la información en las diferentes temáticas, es importante aclarar que el Ministerio de Transporte viene trabajando en estas implementaciones para llegar a la situación deseada en casa escenario:

TEMÁTICA	***SITUACIÓN ACTUAL***	***SITUACIÓN DESEADA***

Establecimiento del Sistema de Gestión de Seguridad de la Información – SGSI	*El sistema, cuenta con Políticas, Procedimientos, Manuales y Formatos. Sin embargo, algunos de estos documentos no son aplicados a cabalidad, por el personal del Ministerio. Asi mismo, algunos se encuentran en proceso de apropiación, ya que el personal encargado inicialmente, ha ido rotando, lo que dificulta una correcta apropiación de los documentos en la entidad.*	*Documentos que componen el SGSI, asignados a un responsable, liberados y divulgados y apropiados en la entidad.*
Riesgos de Seguridad de la Información	*Se tiene implementada una metodología integral de riesgos. Sin embargo, se debe mejorar los aspectos relacionados con la transición de los tratamientos a controles. Con el fin de poder evidenciar la disminución del riesgo a través del tiempo.*	*Sistema de Gestión de riesgos integrada conforme a MIPG con enfoque a los activos de información, para gestión detallada de riesgos de seguridad digital (Seguridad de la Información).*

Acceso a la Información	*Se cuenta con un inventario genérico de activos de información, dentro de la entidad. Sin embargo, en los mismos no se puede identificar datos relevantes de la hoja de vida, como ubicación, mantenimientos cambios entre otros.*	*Inventario de activos de TIC, documentados con su respectiva hoja devidad.*
Seguridad Perimetral Lógica	*Le entidad, ha iniciado una transición hacia infraestructura en nube. Sin embargo, esta infraestructura no cuenta con los mismos controles perimetrales que la infraestructura local, los sistemas de seguridad On-Premise también deben expandirse a este nivel, con el fin de brindar un adecuado aseguramiento de los sistemas de información alojados en nube.* *Se presentan deficiencias en el control de acceso lógico a la red, por parte de equipos personales del personal. Asi mismo, se presentan debilidades en la posible identificación de fugas de información.*	*Sistemas de seguridad perimetral implementados en nube.* *Sistema de control de acceso a las redes del Ministerio basado en identidades y la política "Trae tu propio dispositivo – BYOD" debidamente desplegado.* *Sistemas de Prevención de Fuga de Información (DLP) incorporados a los servicios de correo y terminales de usuario.*

Seguridad Perimetral Física	*Se evidencian deficiencias de control y aplicación de políticas por parte del personal de seguridad física de la entidad.*	*Áreas seguras plenamente identificadas y documentadas que cuenten con un Sistema de CCTV con cobertura para las mismas.*
		Control de acceso físico a las instalaciones estricto, con verificación de ingreso de equipos propios y de externos documentados y controlados en las bitácoras. *Ejecución y cierre de gestión de vulnerabilidades identificadas como debilidades de seguridad física, en las pruebas de Ethical Hacking.*
Infraestructura Física Data Center	*La organización cuenta con centro de cómputo en un datacenter certificado TIER III, que brinda buenas condiciones a nivel eléctrico y de refrigeración para la infraestructura tecnológica.*	*Centro de cómputo conservando las mismas condiciones TIER III.*
Transferencia Segura de Información	*La entidad, cuenta con herramientas para cifrado de equipo y dispositivos que sean retirados por parte de la entidad.* *Sin embargo, no se realiza las solicitudes por parte de los procesos de la Entidad, para la aplicación de este control a los equipos que presentan este riesgo.*	*Información almacenada o transportada fuera de la organización protegida contra acceso no autorizado.*

Monitoreo de eventos de Seguridad	*La entidad cuenta con procedimientos para monitoreo y gestión de logs, que permiten identificar de forma temprana, eventos de seguridad.* *Si embargo, el personal no cumple con los procedimientos de reporte de eventos y monitore de infraestructura.*	*Personal encargado de infraestructura y sistemas de información, ejecutando tareas periódicas de monitoreo y análisis, asi como herramientas implementadas para correlación de logs que permita identificar posibles eventos o brechas de seguridad y prevenir incidentes.*
Seguridad en redes y comunicaciones	*La Entidad implemento certificados de navegación segura SSL para que las aplicaciones web funcionen sobre HTTPS.* *La entidad no cuenta con controles para el acceso de dispositivos a la red, exponiendo a la entidad a equipos que podrían estar contaminados con malware o ataques de usuario que pueden causar fuga, daños o perdida de información.*	*Renovación de los certificados SSL para los aplicativos de la Entidad.* *solución de control de acceso a la red (NAC – Network Access Control) para blindar de mejor manera la información y servicios de red.* *Solución para gestión de identidades que permita una solución flexible para ingreso de equipos a la red de la entidad aplicando plantillas de seguridad.*
Seguridad en proyectos TI	*La entidad actualmente cuenta con una política de seguridad de la información para la relación con los proveedores. Sin embargo, teniendo en cuenta la rotación del personal directivo de contratos, no ha sido posible apropiarla en su totalidad.*	*Políticas de relación con proveedores y gestión de proyectos acorde al SGSI y apropiada en la entidad.*

Gestión de Vulnerabilidades	*Se realizan pruebas de Ethical Hacking anualmente para análisis de vulnerabilidades de la entidad.* *Sin embargo, se requiere recursos tecnológicos y de personal, para el cierre de algunas brechas de seguridad dentro de la plataforma tecnológica.*	*Sistemas de información con vulnerabilidades remediadas o mitigadas.*
Continuidad de Negocio	*La entidad cuenta con Análisis de Riesgos de Disponibilidad y con un documento de Análisis de Impacto al Negocio. Sin embargo, teniendo en cuenta que no hay infraestructura de redundancia, no cuenta aún con un plan con un plan de continuidad tecnológica (DRP), que permita recuperar los servicios tecnológicos en los tiempos establecidos en el BIA, conforme a las necesidades de los procesos de la entidad. Implicando que en una eventualidad la operación del negocio sea difícilmente restaurada o sus tiempos no sean los adecuados.* *La entidad no cuenta con redundancias o sitio de cómputo alterno, que permita recuperar la operación de la entidad en caso de una eventualidad.*	*Planes de continuidad de tecnología y seguridad de la información establecidos para restaurar la operación del negocio.* *Centro de cómputo alterno con infraestructura suficiente para recuperar los servicios tecnológicos de la entidad y con lo anterior la operación del negocio.*

Capacitación y sensibilización en Seguridad de la Información.	*La entidad cuenta con un plan de concientización para los usuarios, que se actualiza cada vigencia. Sin embargo, no se ha establecido una obligatoriedad del personal en la participación o asistencia a las actividades de seguridad.* *Lo que dificulta la concientización del personal y la evaluación del nivel de concientización de este.*	*Establecimiento de obligaciones de asistencia a actividades y cumplimiento de políticas del Sistema de gestión de Seguridad de la Información.* *Personal concientizado en las política y lineamientos de seguridad de la información que permita un adecuado uso y gestión de los activos de la organización.*
Seguridad en nube	*La entidad actualmente, no cuenta con lineamientos de seguridad de la información, que direccionen las implementaciones de infrestrutura o servicios en nube.* *Por lo cual se requiera la actualización de los procedimientos, manuales y políticas, incluyendo estándares y aspectos de seguridad de la información a tener en cuenta para una correcta implementación en nube.*	*Procedimientos, manuales y políticas actualizados y alineados con estándares de seguridad de la información aplicados a la implementación de infraestructura y sistemas de información seguros en nube.*

Para lo anterior se requiere seguir apropiando los lineamientos en la organización y emprender proyectos para adquirir infraestructura o las redundancias necesarias para la continuidad del negocio y seguridad de la información, renovación de sistemas de información y fortalecimiento de controles de acceso físico y lógica de la Entidad.

8. DETALLE DEL PLAN

Conforme a la alineación estrategita para el cumplimiento de las iniciativas y macroproyectos, a continuación, se detallan el plan, donde se estable el catálogo de proyectos de actividades a ejecutar y se califican teniendo en cuenta su impacto a nivel de Apoyo a los procesos de la Entidad y Gobierno Digital con base en la siguiente tabla:

	Apoyo estratégico: *El proyecto, iniciativa o contrato apoya los objetivos del proceso de forma clara y contundente*
	Apoyo táctico: *El proyecto, iniciativa o contrato apoya al menos un objetivo del proceso en la gestión táctica*
	Apoyo tangencial*: El proyecto, iniciativa o contrato apoya tangencialmente un objetivo o una actividad del proceso*

PROYECTOS	***MOTIVACIÓN U ORIGEN***	***GOBIERNO DIGITAL***								
		TIC para el Estado	***TIC para la sociedad***	***Seguridad y Privacidad (MSPI)***	***Servicios Ciudadanos Digitales***	***Arquitectura TI Colombia***	***Lineamientos impactados (Arquitectura TI)***	***Gobierno Digital – Consolidado***		
Redundancias o centro de cómputo alterno	*La organización no cuenta con un centro de cómputo alterno. En caso de un desastre la recuperación de los servicios tecnológicos no tendría tiempo determinado para su recuperación y restablecimiento.*	*x*	*X*	*x*	*x*	*X*	*5*	*2*	*1*	*2*

PROYECTOS	MOTIVACIÓN U ORIGEN	GOBIERNO DIGITAL								
		TIC para el Estado	TIC para la sociedad	Seguridad y Privacidad (MSPI)	Servicios Ciudadanos Digitales	Arquitectura TI Colombia	Lineamientos impactados (Arquitectura TI)	Gobierno Digital – Consolidado		
	El Ministerio cuenta con Infraestructuras Críticas Cibernéticas, la cuales pueden afectar social y económicamente el país. Estas deben protegerse adecuadamente y garantizar su continuidad en caso de algún incidente o falla crítica. Ej: Registro Nacional de Despachos de Carga (RNDC), RUNT, entre otros.									
Mantenimiento del MSPI	*La entidad se encuentra en un avance del 80% en la implementación del MSPI, y se requiere dar un cumplimiento del*	*x*	*X*	*x*	*x*	*X*	*3*	*3*	*2*	*0*

PROYECTOS	MOTIVACIÓN U ORIGEN	GOBIERNO DIGITAL								
		TIC para el Estado	TIC para la sociedad	Seguridad y Privacidad (MSPI)	Servicios Ciudadanos Digitales	Arquitectura TI Colombia	Lineamientos impactados (Arquitectura TI)	Gobierno Digital – Consolidado		
	100% de avance, lo anterior ya que se constituye un incumplimiento a los decretos establecidos por MinTIC.									
Certificación del SGSI del Ministerio (Fase I)	*Una vez implementado el MSPI, se debe optar por el camino de certificación de la norma ISO 27001, para verificar el nivel de madurez y así mismo demostrar el compromiso del Ministerio con la seguridad de la información.*	-	-	*x*	-	-		*0*	*1*	*0*

PROYECTOS	MOTIVACIÓN U ORIGEN	GOBIERNO DIGITAL								
		TIC para el Estado	TIC para la sociedad	Seguridad y Privacidad (MSPI)	Servicios Ciudadanos Digitales	Arquitectura TI Colombia	Lineamientos impactados (Arquitectura TI)	Gobierno Digital – Consolidado		
Sistema de control de acceso basado en identidades y política BYOD	*No existe control de acceso a las redes del Ministerio para los smartphones, portátiles y demás dispositivos externos que ingresan a la red, por lo tanto, se debe instalar un sistema que permita ingresar estos dispositivos de forma segura sin afectar la red o infraestructura del Ministerio.*	-	-	*x*	-	*X*	*2*	*2*	*0*	*0*
Sistema de prevención de fuga de información (DLP)	*No existen controles para la prevención de fuga de información en la entidad, por lo tanto, se requiere de la implementación de una solución especializada para*	-	-	*x*	-	*X*	*1*	*2*	*0*	*0*

PROYECTOS	MOTIVACIÓN U ORIGEN	GOBIERNO DIGITAL								
		TIC para el Estado	TIC para la sociedad	Seguridad y Privacidad (MSPI)	Servicios Ciudadanos Digitales	Arquitectura TI Colombia	Lineamientos impactados (Arquitectura TI)	Gobierno Digital – Consolidado		
	tratar esta problemática y disminuir su probabilidad de ocurrencia.									
Sistema de detección y visibilidad análisis Y Acción para contener y desarmar ataques cibernéticos con apoyo de inteligencia artificial, asociada a identificación de comportamientos anormales	*La entidad no cuenta con sistemas predictivos que permitan detectar anomalías en la red y posibles ataques internos o externos.* *Conforme a lo anterior, se requiere la implementación de sistemas que permitan tener una visión clara de los sucesos o posibles anomalías que se estén presentando en la red*	*-*	*-*	*x*	*-*	*X*	*1*	*2*	*0*	*0*

PROYECTOS	MOTIVACIÓN U ORIGEN	GOBIERNO DIGITAL								
		TIC para el Estado	TIC para la sociedad	Seguridad y Privacidad (MSPI)	Servicios Ciudadanos Digitales	Arquitectura TI Colombia	Lineamientos impactados (Arquitectura TI)	Gobierno Digital – Consolidado		
	que puedan estar causando degradación en el servicio, o vulnerabilidades o brechas de seguridad que puedan ser aprovechadas para afectar la integridad, confidencialidad o disponibilidad de la información y con lo anterior la operación del negocio.									

PROYECTOS	MOTIVACIÓN U ORIGEN	GOBIERNO DIGITAL								
		TIC para el Estado	TIC para la sociedad	Seguridad y Privacidad (MSPI)	Servicios Ciudadanos Digitales	Arquitectura TI Colombia	Lineamientos impactados (Arquitectura TI)	Gobierno Digital – Consolidado		
***Implementación de sistema de EDR* Endpoint Detection Response**	*Con el objetivo de fortalecer la seguridad en los sistemas de información de la entidad con respecto a amenazas avanzadas, en la actualidad ya no es suficiente con la implementación de un software EndPoint, se requiere la implementación denuevas herramientas como lo son el EDR, que permite identificar y analizar de forma detallada los sucesos de EndPoint, asi como la respuesta automática, contra detección de*	-	-	x	-	x	1	2	0	0

PROYECTOS	MOTIVACIÓN U ORIGEN	GOBIERNO DIGITAL								
		TIC para el Estado	TIC para la sociedad	Seguridad y Privacidad (MSPI)	Servicios Ciudadanos Digitales	Arquitectura TI Colombia	Lineamientos impactados (Arquitectura TI)	Gobierno Digital – Consolidado		
	amenazas.									
Implementación de Plan de Recuperación Tecnológica y continuidad de seguridad de la información.	*Las entidades están expuestas a todo tipo de riesgos que atentan contra la seguridad de la información y con lo anterior comprometer la operación del negocio, algunos riesgos tecnológicos pueden ser mitigados, sin embargo, siempre existirá la posibilidad de materialización ya*	*x*	*X*	*x*	*x*	*x*	*4*	*2*	*1*	*2*

PROYECTOS	MOTIVACIÓN U ORIGEN	GOBIERNO DIGITAL								
		TIC para el Estado	TIC para la sociedad	Seguridad y Privacidad (MSPI)	Servicios Ciudadanos Digitales	Arquitectura TI Colombia	Lineamientos impactados (Arquitectura TI)	Gobierno Digital – Consolidado		
	que ningún sistema de información es invulnerable, de la misma forma sucede con los riesgos de desastre naturales, los cuales no pueden ser prevenidos. *Si bien no es factible eliminar el riesgo o prevenir su materialización en su totalidad, se pueden mitigar sus impactos de tal forma que se pueda recuperar los servicios tecnológicos prestados por la entidad rápidamente, pero para lo anterior se requiere el*									

PROYECTOS	MOTIVACIÓN U ORIGEN	GOBIERNO DIGITAL								
		TIC para el Estado	TIC para la sociedad	Seguridad y Privacidad (MSPI)	Servicios Ciudadanos Digitales	Arquitectura TI Colombia	Lineamientos impactados (Arquitectura TI)	Gobierno Digital – Consolidado		
	desarrollo de un Plan de Recuperación Tecnológica que se compone de tres documentos: - *Análisis de Riesgos de Procesos* - *Análisis de Impacto al Negocio* - *Plan de Recuperación Tecnológica* *Estos documentos permiten determinar los procesos, sistemas*									

PROYECTOS	MOTIVACIÓN U ORIGEN	GOBIERNO DIGITAL								
		TIC para el Estado	TIC para la sociedad	Seguridad y Privacidad (MSPI)	Servicios Ciudadanos Digitales	Arquitectura TI Colombia	Lineamientos impactados (Arquitectura TI)	Gobierno Digital – Consolidado		
	y recursos tecnológicos o de información que requieren los procesos críticos de la entidad para recuperarse ante la presentación de un evento, y con lo anterior garantizar la operación del negocio. *El Ministerio cuenta con Infraestructuras Críticas Cibernéticas, la cuales pueden afectar social y económicamente el país. Estas deben protegerse adecuadamente y garantizar su continuidad en caso de algún incidente o falla*									

PROYECTOS	MOTIVACIÓN U ORIGEN	GOBIERNO DIGITAL								
		TIC para el Estado	TIC para la sociedad	Seguridad y Privacidad (MSPI)	Servicios Ciudadanos Digitales	Arquitectura TI Colombia	Lineamientos impactados (Arquitectura TI)	Gobierno Digital – Consolidado		
	crítica. Ej: Registro Nacional de Despachos de Carga (RNDC), RUNT, entre otros.									
Análisis de vulnerabilidades externo de los sistemas de información (Ethical Hacking).	*La entidad debe ejecutar periódicamente análisis de vulnerabilidades a su infraestructura, para detectar brechas de seguridad que puedan ser utilizadas para causar ataques cibernéticos.*	-	-	x	-	x	2	2	0	0
Renovación anual de licenciamiento y soporte de infraestructura tecnológica de	*Se requiere mantener un presupuesto definido para la renovación de los licenciamientos de la*	x	x	x	x	x	3	2	0	3

PROYECTOS	MOTIVACIÓN U ORIGEN	GOBIERNO DIGITAL								
		TIC para el Estado	TIC para la sociedad	Seguridad y Privacidad (MSPI)	Servicios Ciudadanos Digitales	Arquitectura TI Colombia	Lineamientos impactados (Arquitectura TI)	Gobierno Digital – Consolidado		
seguridad del Ministerio de Transporte.	*infraestructura para evitar brechas de seguridad o posibles incidentes de seguridad, a causa de fallas de los equipos o falta de actualización de los mismos.*									
Entrenamiento y capacitación en seguridad de la información.	*La seguridad de la información es una temática en constante evolución, por lo que se requiere que el personal reciba capacitaciones relacionadas que aumente las capacidades de respuesta a posibles incidentes o nuevas amenazas a la seguridad de la*	-	-	-	-	*x*	*1*	*1*	*0*	*0*

PROYECTOS	MOTIVACIÓN U ORIGEN	GOBIERNO DIGITAL								
		TIC para el Estado	TIC para la sociedad	Seguridad y Privacidad (MSPI)	Servicios Ciudadanos Digitales	Arquitectura TI Colombia	Lineamientos impactados (Arquitectura TI)	Gobierno Digital – Consolidado		
	información del Ministerio.									
SOC - Centros de Operaciones de Seguridad /NOC - Centros de Operaciones de Redes	*El Ministerio cuenta con Infraestructuras Críticas Cibernéticas, la cuales pueden afectar social y económicamente el país. Estas deben protegerse y monitorearse las 24 horas con el fin de detectar posibles intentos de ataques,*	*x*	*x*	*x*	*X*	*X*	*2*	*4*	*1*	*0*

PROYECTOS	MOTIVACIÓN U ORIGEN	GOBIERNO DIGITAL								
		TIC para el Estado	TIC para la sociedad	Seguridad y Privacidad (MSPI)	Servicios Ciudadanos Digitales	Arquitectura TI Colombia	Lineamientos impactados (Arquitectura TI)	Gobierno Digital – Consolidado		
	degradaciones y con lo anterior evitar incidentes de seguridad que puedan tener un impacto económico la nación y de imagen para el ministerio. *. Ej: Registro Nacional de Despachos de Carga (RNDC), RUNT, entre otros.*									

PROYECTOS	MOTIVACIÓN U ORIGEN	GOBIERNO DIGITAL								
		TIC para el Estado	TIC para la sociedad	Seguridad y Privacidad (MSPI)	Servicios Ciudadanos Digitales	Arquitectura TI Colombia	Lineamientos impactados (Arquitectura TI)	Gobierno Digital – Consolidado		
Implementación de escritorios virtuales	*La entidad esta en proceso de implementación de la modalidad de teletrabajo, pero para lo anterior, se debe tener en cuenta los aspectos relacionados en los estándares internacionales como la norma ISO 27001:2013 y el Modelo de Seguridad y Privacidad de la Información del MINTIC, numeral A.6.2.* *Donde es necesario proteger la información que es consultada, procesada y evitar su*	-	-	*x*	-	-	-	*1*	*0*	*0*

PROYECTOS	MOTIVACIÓN U ORIGEN	GOBIERNO DIGITAL						
		TIC para el Estado	TIC para la sociedad	Seguridad y Privacidad (MSPI)	Servicios Ciudadanos Digitales	Arquitectura TI Colombia	Lineamientos impactados (Arquitectura TI)	Gobierno Digital – Consolidado
	almacenamiento en equipos de propiedad privada.							

Conforme a lo anterior los proyectos u actividades relacionadas o que puedan ser afectados con la Modernización de centro de datos y monitoreo, estarán sujetos a variaciones según los tiempos definidos por la entidad para el estudio y ejecución del macroproyecto de renovación, adecuación de sus instalaciones físicas y de la disponibilidad presupuestal, que supone una condición para priorizar la ejecución de unos proyectos sobre los demás

9. CRONOGRAMA

Con base en los proyectos de actividades propuestas y ruta crítica para la ejecución de estos, se planifica la ejecución de estos para la vigencia 2023 como se muestra a continuación:

Plan Estratégico de Seguridad de la Información (PESI)					
OBJETIVOS	**PRODUCTOS**	**ACTIVIDADES**	**RESPONSABLE**	**CORTO PLAZO [1 AÑO]**	
				Inicio dd/mm/aaaa	**Fin dd/mm/aaaa**
Actualizar autodiagnóstico del Sistema de Gestión de Seguridad de la información (SGSI) de la organización, identificando las debilidades actuales que deben ser fortalecidas.	Actas e informes de revisión de los roles y aplicación de lineamientos.	Seguimiento de aplicación de políticas, lineamientos y procedimientos del Sistema de gestión de Seguridad de la Información, con los diferentes responsables de los procedimientos.	Coordinador del Grupo TIC Jefe Oficina de Planeación	01/02/2023	30/06/2023
Ejecutar las acciones de mejora y proyectos encaminadas a la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).	Formatos de acción, correctiva, preventiva y de mejora. Asi como informes de avance y gestión de las actividades que no puedan ser ejecutadas por recursos financieros o de personal.	Establecimiento de acciones correctivas de y de mejora para documentos del Sistema que por recursos de personal o infraestructura no están pudiendo ser ejecutados.	Coordinador del Grupo TIC Jefe Oficina de Planeación	01/02/2023	30/06/2023

Ejecutar las acciones de mejora y proyectos encaminadas a la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).	Actas de capacitación y apropiación de documentos firmadas por los responsables adignados.	Fortalecimiento y apoyo en la apropiación de documentos del Sistema de Gestión de Seguridad de la Información que no se estén aplicando.	Coordinador del Grupo TIC Jefe Oficina de Planeación	01/02/2023	30/06/2023
Establecer y priorizar los proyectos y acciones de mejora para la gestión de las debilidades identificadas.	Plan para actualización de documentos e inclusión de lineamientos de seguridad en nube	Establecimiento de documentos a actualizar para inclusión y adaptación de lineamientos a seguridad en nube.	Coordinador del Grupo TIC Jefe Oficina de Planeación	01/02/2023	30/04/2023
Ejecutar las acciones de mejora y proyectos encaminadas a la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).	Documentos actualizados y liberados en Daruma	Actualización de políticas procedimientos y manuales identificados para inclusión de lineamientos y buenas prácticas de seguridad en nube.	Coordinador del Grupo TIC Jefe Oficina de Planeación	01/02/2023	30/06/2023
Ejecutar las acciones de mejora y proyectos encaminadas a la mejora continua del Sistema de Gestión de	Anexos técnicos y actas de ejecución e implementación.	Adquisición e implementación de infraestructura para gestión de copias de respaldo de información.	Coordinador del Grupo TIC Jefe Oficina de Planeación	01/02/2023	31/12/2023

Seguridad de la Información (SGSI).					
Realizar la evaluación y auditoría, de la efectividad de las acciones emprendidas para solucionar las debilidades del sistema y verificar el correcto cumplimiento de los controles y lineamientos implementados en el SGSI.	Solicitud a la Oficina de Control Interno.	Solicitud y ejecución de preauditoria por parte de Control Interno, para preparación del sistema para Auditoría externa contratada.	Coordinador del Grupo TIC	01/07/2023	31/12/2023
Ejecutar las acciones de mejora y proyectos encaminadas a la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).	Informe de acciones de mejora implementadas en el SGSI.	Mantenimiento y mejora continua del SGSI.	Coordinador del Grupo TIC Jefe Oficina de Planeación	01/02/2023	31/12/2023

Ejecutar las acciones de mejora y proyectos encaminadas a la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).	Actas de capacitación, correos informativos y divulgación de cambios o nuevos lineamientos de seguridad en nube.	Apropiación de nuevos documentos con lineamiento de seguridad en nube.	Coordinador del Grupo TIC Jefe Oficina de Planeación	01/07/2023	31/12/2023
Ejecutar las acciones de mejora y proyectos encaminadas a la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).	Documento borrador DRP	Establecimiento de DRP (Inicial sin cumplimiento de tiempos RTO o RPO), con infraestructura de copias de respaldo adquirida	Coordinador del Grupo TIC Jefe Oficina de Planeación	01/07/2023	31/12/2023
Establecer y priorizar los proyectos y acciones de mejora para la gestión de las debilidades identificadas.	Documentos de estudio y explicación de propuesta de proyecto.	Establecimiento y generación de propuesta proyecto para adquisición de infraestructura de redundancia, para generación de DRP (cumpliendo las necesidades de los procesos RTO y RPO)	Coordinador del Grupo TIC Jefe Oficina de Planeación	01/07/2023	31/12/2023

Establecer y priorizar los proyectos y acciones de mejora para la gestión de las debilidades identificadas.	Presentación con los proyectos propuestos para la vigencia 2024	Presentación de la necesidad al coordinador del grupo TIC y a la alta dirección para aprobación de presupuesto.	Coordinador del Grupo TIC Jefe Oficina de Planeación	01/07/2023	31/12/2023
Ejecutar las acciones de mejora y proyectos encaminadas a la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).	Inventario de activos de seguridad de la información actualizados.	Acompañamiento y seguimiento en la gestión de activos de seguridad de la Información y de riesgos de seguridad digital	Coordinador del Grupo TIC Jefe Oficina de Planeación	01/02/2023	31/12/2023
Ejecutar las acciones de mejora y proyectos encaminadas a la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).	Matrices de riesgos, e informes de avance de tratamientos de los riesgos de seguridad digital.	Apoyo con la mejora continua de la gestión y metodología de riesgos	Coordinador del Grupo TIC Jefe Oficina de Planeación	01/02/2023	31/12/2023
Actualizar autodiagnóstico del Sistema de Gestión de Seguridad de la información (SGSI) de la organización,	Formato de diagnóstico del MSPI actualizado mensualmente.	Aplicación de instrumento MINTIC para medición del estado de implementación del sistema Aplicación de	Coordinador del Grupo TIC Jefe Oficina de Planeación	01/02/2023	31/12/2023

identificando las debilidades actuales que deben ser fortalecidas.		modelo para medición de madurez del SGSI			
Ejecutar las acciones de mejora y proyectos encaminadas a la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).	Plan de concientización y comunicación, borradores de reuniones, tips, boletines, informes de ejercicios de ingeniería social, evaluaciones y medición de indicadores de seguridad digital.	Ejecutar plan de concientización y comunicación anual del SGSI	Coordinador del Grupo TIC Jefe Oficina de Planeación	01/02/2023	31/12/2023
Ejecutar las acciones de mejora y proyectos encaminadas a la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).	Anexos técnicos, contratos SECOP e informes de apoyo en el seguimiento de ejecución.	Ejecución de actividades periódicas, creación de anexos técnicos para adquisición de renovaciones o contratos de mantenimiento, soporte y garantía de infraestructura tecnológica.	Coordinador del Grupo TIC Jefe Oficina de Planeación	01/02/2023	31/12/2023

Ejecutar las acciones de mejora y proyectos encaminadas a la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).	Anexos técnicos, contratos SECOP e informes de apoyo en el seguimiento de ejecución.	Generación de anexos técnicos y apoyo en la contratación de nuevos proyectos de adquisición de infraestructura de seguridad.	Coordinador del Grupo TIC Jefe Oficina de Planeación	01/02/2023	31/12/2023

9.1. DETALLE Y ORDEN DE ACTIVIDADES A EJECUTAR

<table>
<tr><th colspan="5">2023</th></tr>
<tr><th colspan="2">I - Semestre</th><th colspan="3">II – Semestre</th></tr>
<tr><td colspan="5">PROYECTOS DE GESTIÓN DE LA SEGURIDAD – (SGSI / MSPI)</td></tr>
<tr><td colspan="2">Seguimiento de aplicación de políticas, lineamientos y procedimientos del Sistema de gestión de Seguridad de la Información, con los diferentes responsables de los procedimientos.</td><td colspan="3">Solicitud y ejecución de preauditoria por parte de Control Interno, para preparación del sistema para Auditoría externa contratada.</td></tr>
<tr><td colspan="2">Establecimiento de acciones correctivas de y de mejora para documentos del Sistema que por recursos de personal o infraestructura no están pudiendo ser ejecutados.</td><td colspan="3" rowspan="2">Mantenimiento y mejora continua del SGSI</td></tr>
<tr><td colspan="2">Fortalecimiento y apoyo en la apropiación de documentos del Sistema de Gestión de Seguridad de la Información que no se estén aplicando.</td></tr>
<tr><td>Establecimiento de documentos a actualizar para inclusión y adaptación de lineamientos a seguridad en nube.</td><td>Actualización de políticas procedimientos y manuales identificados para inclusión de lineamientos y buenas practicas de seguridad en nube.</td><td colspan="3">Apropiación de nuevos documentos apropiados con lineamiento de seguridad en nube.</td></tr>
<tr><td colspan="2" rowspan="2">Adquisición e implementación de infraestructura para gestión de copias de respaldo de información.</td><td colspan="3">Redefinición y actualización de procedimiento de gestión de copias de respaldo.</td></tr>
<tr><td>Establecimiento de DRP (Inicial sin cumplimiento de tiempos RTO o RPO), con infraestructura de copias de respaldo adquirida</td><td>Establecimiento y generación de propuesta proyecto para adquisición de infraestructura de redundancia, para generación de DRP (cumpliendo las necesidades de los procesos RTO y RPO)</td><td>Presentación de la necesidad al coordinador del grupo TIC y a la alta dirección para aprobación de presupuesto.</td></tr>
<tr><td colspan="5">Acompañamiento y seguimiento en la gestión de activos de seguridad de la Información y de riesgos de seguridad digital</td></tr>
<tr><td colspan="5">Apoyo con la mejora continua de la gestión y metodología de riesgos</td></tr>
<tr><td colspan="5">Aplicación de instrumento MINTIC para medición del estado de implementación del sistema
Aplicación de modelo para medición de madurez del SGSI</td></tr>
<tr><td colspan="5">Ejecutar plan de concientización y comunicación anual del SGSI</td></tr>
<tr><td colspan="5">RENOVACIONES Y ACTIVIDADES PERIÓDICAS</td></tr>
<tr><td colspan="5">Ejecución anual de pruebas de Ethical Hacking (Contratadas e internas)</td></tr>
<tr><td colspan="5">Remediación anual de vulnerabilidades (Contratadas e internas)</td></tr>
<tr><td colspan="5">Renovación anual de certificados SSL (3 años)
Ethical Hacking e implementación de sistemas de firma digital para tramite documental</td></tr>
</table>

2023	
I - Semestre	***II – Semestre***
Renovación de licenciamiento infraestructura de seguridad año 2023.	
NUEVOS PROYECTOS DE INFRAESTRUCTURA DE SEGURIDAD INFORMÁTICA Y CONTINUIDAD DE TI	
Adquisición de infraestructura de respaldos disco y cinta	*Implementación de herramienta de cifrado de equipos y archivos* *Definición e Implementación Política BYOD*
Adquisición de firewall de aplicaciones web (WAF) para nube	*Plan Piloto de escritorios virtuales*
SOC/NOC (Monitoreo de Infraestructura 7 x 24)	*Implementación de servicios DLP para protección de fuga de información*
Adquisición de software de ciberseguridad *(Software para detección proactiva de vulnerabilidades e indicadores de compromiso)*	

9.2. COSTO APROXIMADO DE EJECUCIÓN DE PROYECTOS 2023

2022	
Proyecto	***Valor***
Proyectos nuevos	
Adquisición de infraestructura de respaldos disco y cinta	*$ 700.000.000*

Adquisición de firewall de aplicaciones web (WAF) para nube	*$230.000.000*
SOC/NOC (Monitoreo de Infraestructura 7 x 24)	*$350.000.000*
Pruebas de Ethical Hacking anual (Contratada)	*$ 140.000.000*
Piloto de escritorios virtuales (FASE I)	*$ 80.000.000*
Software para detección proactiva de vulnerabilidades e indicadores de compromiso	*$ 220.000.000*
Renovación infraestructura de seguridad	
Renovación software EndPoint	*218.722.000*
Renovación de licenciamiento infraestructura de seguridad año 2023 (FW, IPS, WAF, Sandbox, SIEM, Anti DDoS)	*$1.175.727.445*
Renovación DAM x 1 año	*$235.995.106*
Web Application Scanner (WAS) x 1 año	*$53.865.969*
Total Anual Aproximado	***$ 3.404.310.520***

10. COMUNICACIÓN

El presente documento será comunicado a las partes interesadas por medio de la página web de MINISTERIO DE TRANSPORTE como documento de conocimiento general de la organización.

11. GLOSARIO

- ***Riesgo de seguridad de la información:*** *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.*
- ***Confidencialidad:*** *Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.*
- ***Integridad:*** *Propiedad de la información relativa a su exactitud y completitud.*
- ***Disponibilidad:*** *Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.*
- ***Seguridad de la Información:*** *Preservación de la confidencialidad, integridad y disponibilidad de la información.*
- ***MSPI:*** *Modelo de seguridad y privacidad de información*
- ***SGSI:*** *Sistema de gestión de seguridad de la información*
- ***Vulnerabilidad:*** *Debilidad de un activo o control que puede ser explotada por una o más amenazas.*
- ***Amenaza:*** *Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.*

12. DOCUMENTOS DE REFERENCIA

- *Manual de Gobierno Digital – MinTIC.*
- *Norma NTC ISO 27001:2013 Sistema de Gestión de Seguridad de la Información - ICONTEC.*
- *Modelo de Seguridad y Privacidad de la Información – MINTIC*
- *Modelo Integrado de Planeación y Gestión – MIPG - DAFP*
- *Documento CONPES 3854 - Política Nacional de Seguridad Digital*
- *Marco de Referencia – Arquitectura de TI Colombia - G.ES.06 Guía Cómo Estructurar el Plan*
- *Estratégico de Tecnologías de la Información – PETI – MINTIC.*
- *Plan estratégico MINISTERIO DE TRANSPORTE 2019 – 2022*

13. RESPONSABLE DEL PLAN

Nombre completo: Catalino Posso Arboleda
Cargo: Coordinador (e) Grupo TIC
Dependencia: Grupo de Tecnologías de la Información y las Comunicaciones
Elaboró: Hugo Alejandro Casallas Larrotta
Elaboró: Juan Carlos Valenzuela Buitrago