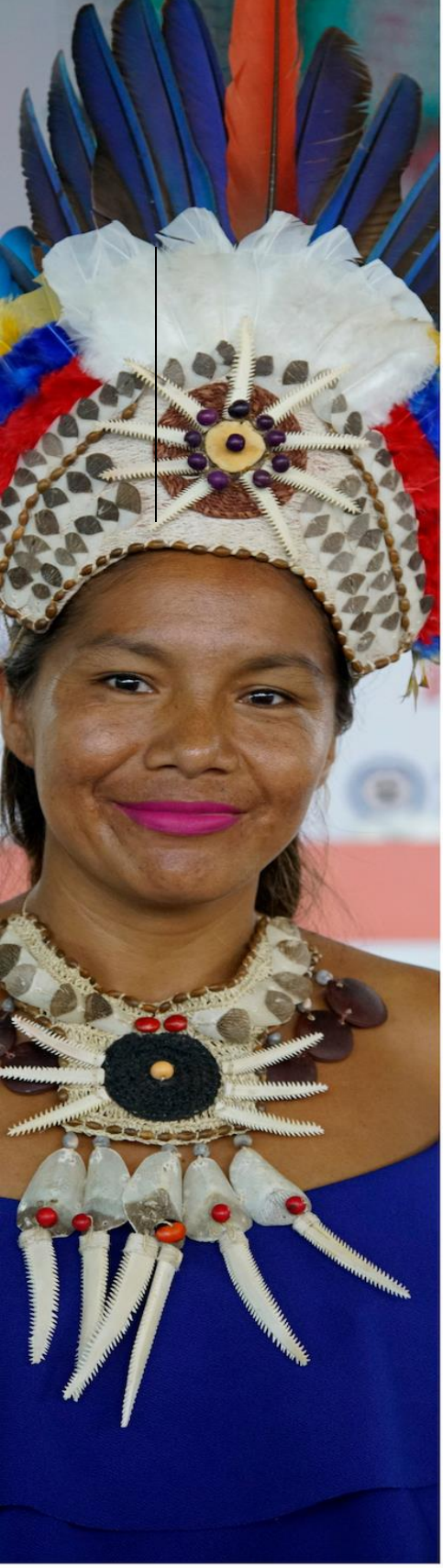
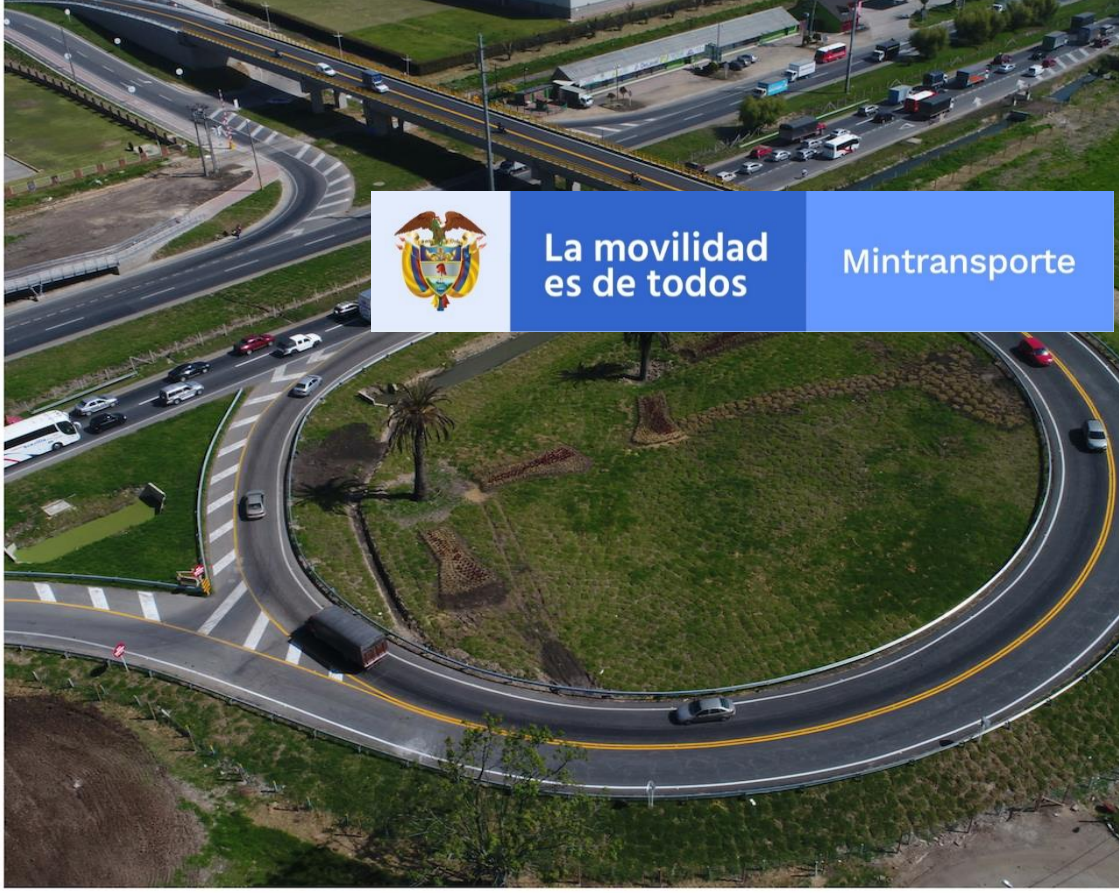




Ministerio de transporte

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - PESI - 2021

CONTENIDO

INTRODUCCION 3

1. GENERALIDADES 4

2. MARCO NORMATIVO 4

3. ALINEACIÓN INSTITUCIONAL 5

4. OBJETIVO GENERAL 7

5. OBJETIVOS ESPECIFICOS 7

6. ALCANCE 8

7. ANÁLISIS DE SITUACIÓN ACTUAL 8

8. PORTAFOLIO DE PROYECTOS 16

9. DETALLE DEL PLAN Y CRONOGRAMA 36

10. COSTO APROXIMADO DE EJECUCIÓN DE PROYECTOS POR AÑO 38

11. ALINEACIÓN ESTRATÉGICA DEL PESI CON EL PETI DE LA ORGANIZACIÓN 42

12. COMUNICACIÓN 42

13. GLOSARIO 42

14. DOCUMENTOS DE REFERENCIA 43

15. CONTROL DE CAMBIOS: 44

16. RESPONSABLE DEL PLAN 44

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, la necesidad de implementar y mantener un 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 lograr una correcta implementación y mantenimiento de 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 establecimiento de un sistema 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

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 organización, a través del documento se desarrollará la situación actúa del Ministerio y los planes para el logro de la situación deseada.

2. 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*

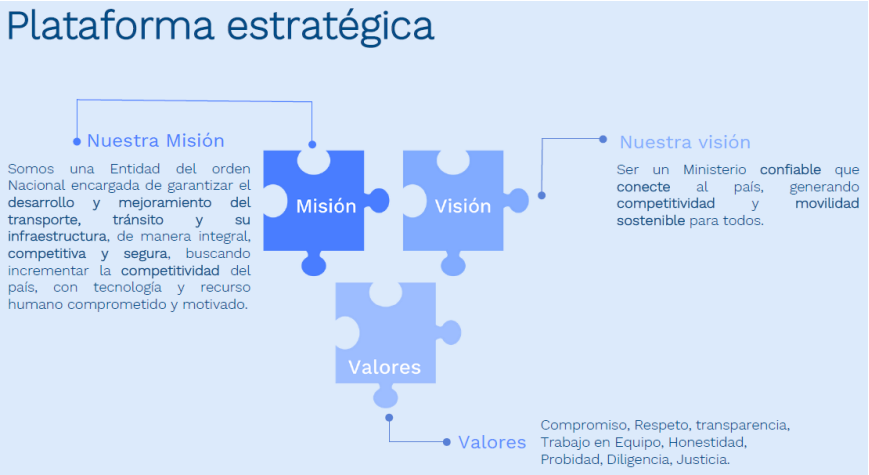
las tecnologías de la información y las comunicaciones, entre otras disposiciones ".

- *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.*

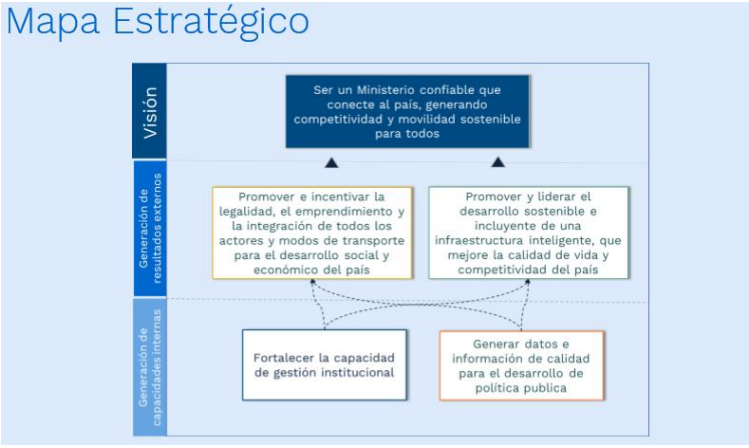
3. ALINEACIÓN INSTITUCIONAL

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 de la siguiente manera:

La plataforma estratégica 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. OBJETIVO GENERAL

Establecer el plan de acción 2019 – 2022, para la implementación, gestión y mejora del Sistema de Gestión de Seguridad de la Información (SGSI) de la MINISTERIO DE TRANSPORTE alineados con la Política de Gobierno Digital y Plan Estratégico de la Organización mediante la implementación de proyectos y actividades para la gestión de riesgos, optimización de recursos y entrega de valor en un entorno de confianza digital seguro.

5. OBJETIVOS ESPECIFICOS

- *Realizar diagnóstico inicial de implementación del SGSI de la organización.*
- *Priorizar las necesidades para la implementación y mejora continua del SGSI.*
- Planificar y realizar la evaluación y auditoría de los controles y lineamientos implementados en el SGSI.

- Priorizar los proyectos a implementar para la correcta implementación del SGSI.
- Actualizar el Plan Estratégico de Seguridad de la Información (PESI) para las vigencias 2021 y 2022.

6. 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 NTC ISO/IEC 27001:2013 – Sistema de Gestión de Seguridad de la Información, así como el fortalecimiento de la infraestructura de ciberseguridad del Ministerio de Transporte.

7. ANÁLISIS DE SITUACIÓN ACTUAL

La situación del 2019 de las Tecnologías de la Información en el MINISTERIO DE TRANSPORTE se determina a partir del informe de Gestión y Desempeño Institucional emitido por la función pública.
A continuación, se muestran los resultados con respecto a Gobierno Digital y Política de Seguridad de la información los cuales involucran el Sistema de Gestión de Seguridad de la Información.

Política de Gobierno Digital

Puntaje Entidad	Valores de Referencia					
	Puntaje máximo grupo par	Quintiles				
		1	2	3	4	5
74,1	86,9	74,1				

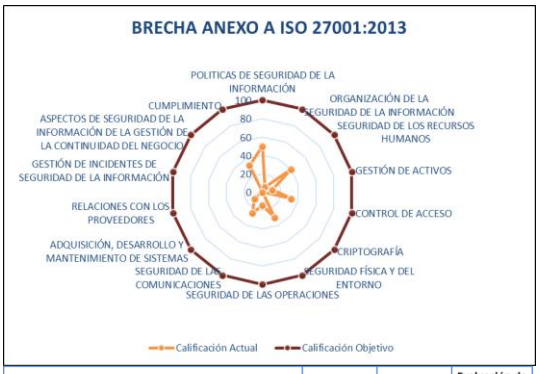
Política de Seguridad Digital

Puntaje Entidad	Valores de Referencia					
	Puntaje máximo grupo par	Quintiles				
		1	2	3	4	5
70,8	89,2	70,8				

El quintil es una medida de ubicación que le permitirá a la entidad conocer que tan lejos está del puntaje máximo obtenido dentro del grupo par. Una entidad con buen desempeño estará ubicada en los quintiles más altos (4 y 5), mientras que una entidad con bajo desempeño se ubicará en los quintiles más bajos (1, 2 y 3).
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 se encuentra con un desempeño bajo.

Con el objetivo de establecer las debilidades en estos componentes de la organización, se diligencia el autodiagnóstico del Modelo de Seguridad de la Información del MINTIC con el fin de profundizar y evidenciar los puntos críticos a trabajar.

A continuación de se presentan los resultados del autodiagnóstico.



	Calificación Actual	Calificación Objetivo	Evaluación de Efectividad de Control
PROMEDIO EVALUACIÓN DE CONTROLES	18	100	INICIAL
PHVA	19	100	PLANIFICACIÓN

DOMINIO	Calificación Actual
POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	50
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	6
SEGURIDAD DE LOS RECURSOS HUMANOS	40
GESTIÓN DE ACTIVOS	11
CONTROL DE ACCESO	32
CRIPTOGRAFÍA	0
SEGURIDAD FÍSICA Y DEL ENTORNO	31
SEGURIDAD DE LAS OPERACIONES	14
SEGURIDAD DE LAS COMUNICACIONES	25
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	11
RELACIONES CON LOS PROVEEDORES	0
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0
CUMPLIMIENTO	32,5

Con base en los resultados de los análisis anteriores y verificación del estado de la infraestructura tecnológica, se pudo evidenciar los puntos que deben ser fortalecidos para una adecuada implementación del Sistema de Gestión de Seguridad de la Información, a continuación, se plantea una descripción de la situación actual y situación deseada de la entidad respecto al sistema de gestión seguridad de la información en las diferentes temáticas:

TEMÁTICA	***SITUACIÓN ACTUAL***	***SITUACIÓN DESEADA***
Establecimiento del Sistema de Gestión de Seguridad de la Información – SGSI	*El SGSI no se encuentra documentado de acuerdo con los lineamientos de la norma ISO 27001:2013 y el Modelo de Seguridad y Privacidad de la Información de MinTIC.*	*Documentos que componen el SGSI liberados y divulgados y aplicados.* *Indicadores para el proceso de Gestión de tecnología y seguridad de la información para*

		medición del desempeño del proceso y del sistema.
		Sistema de gestión de seguridad acreditado y certificado para el proceso de TIC, pero aplicado a toda la entidad.
Políticas de Seguridad de la Información	*Se encuentra la Política General de Seguridad y Privacidad de la Información aprobada por la ministra, pero aún no se encuentra formalmente liberada en el sistema.* *Sin embargo, la política actual debe actualizarse e incluir aspectos adicionales para robustecerla.* *Se requiere de un manual de políticas*	*Política general y políticas del sistema actualizadas, divulgadas y aplicadas por toda la entidad.*

	de seguridad orientado a los usuarios del Ministerio en todos sus niveles.	
Riesgos de Seguridad de la Información	*Se tiene implementada una metodología de riesgos de gestión. Sin embargo, no se ha involucrado el tratamiento de riesgos de seguridad digital para todos los procesos de la organización conforme a las directrices solicitadas por Función Pública y MinTIC.*	*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	*No se cuenta con un índice de información clasificada y reservada.* *No se encuentra realizar un inventario de activos de*	*Política y procedimiento de control de acceso lógico implementados.* *Dueños de proceso concientizados para la definición de segregación de funciones.*

	información con la clasificación solicitada por MinTIC.	*Sistemas de información protegidos contra la divulgación no autorizada prevención de fuga de información.*
Seguridad Perimetral Lógica	*La entidad cuenta con la siguiente infraestructura de seguridad informática:* *Sandbox – Fortinet, sin licenciamiento.* *Fortiweb – Web Application Firewall – Sin licenciamiento.* *FortiAnalyzer – Correlacionador de eventos Fortinet. – Sin licenciamiento.* *La infraestructura de seguridad tiene su licenciamiento caducado hace varios meses y esto implica no contar con soporte de fabricante ni*	*Sistemas de protección perimetral debidamente licenciados periódicamente, evitando brechas de seguridad por ausencia de actualizaciones o soporte con los fabricantes.* *Sistemas de detección y visibilidad de análisis de vulnerabilidades interno contra amenazas persistentes (APTs), que permite actuar oportunamente antes ataques de Ransomware o denegaciones de*

	actualizaciones para enfrentar nuevas amenazas, poniendo en alto riesgo la infraestructura y los servicios de la entidad. *Amenazas y vulnerabilidades avanzadas como APTs.* *Falencias en el control de acceso a la red de nuevos dispositivos como Smartphones, Portátiles de visitantes o funcionarios, impidiendo una implementación adecuadas de políticas de "Bring Your Own Device" o "Trae tu propio dispositivo", facilitando la intrusión de software malicioso en la red o fuga de información.*	*servicio internas o externas.* *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.* *Sistema de Gestión de Eventos y Seguridad de la Información (SIEM) debidamente implementado y monitoreado constantemente y que permita analizar eventos extraños en la entidad y actuar oportunamente ante posibles incidentes.*

	No existen controles orientados a evitar la Fuga de Información, ni a nivel de correo electrónico (OFFICE 365) ni a nivel de dispositivos finales (Smartphones, computadores o portátiles). *No es posible ejecutar un análisis oportuno de los eventos registrados en los dispositivos de seguridad de la entidad, lo que dificulta la detección de posibles ataques o incidentes que puedan presentarse en la infraestructura de la entidad.* *No hay trazabilidad en las acciones ejecutadas sobre*	*Sistema de protección y monitoreo contra ataques cibernéticos y amenazas internas para los datos críticos alojados en las bases de datos debidamente parametrizado, implementado y gestionado.*

	las bases de datos, lo que facilita la modificación no autorizada por parte de propios o terceros en la entidad.	
Seguridad Perimetral Física	*La organización cuenta con acceso a través de tarjeta HID y accesos por huella, además de un sistema CCTV que cubre varias áreas de la organización, sin embargo, no existen los planos de áreas seguras y muchos controles físicos no están debidamente justificados en su ubicación.* *La logística actual de ingreso y salida de las instalaciones del Ministerio es laxa y puede facilitarse el hurto de*	*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.*

	información o de los equipos que los almacenan, así como también es posible la afectación de la integridad de los funcionarios del Ministerio.	
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 en la actualidad no cuenta con ningún herramienta o esquema para el cifrado de para los equipos portátiles, unidades de almacenamiento externo o la información que es transportada o*	*Información almacenada o transportada fuera de la organización protegida contra acceso no autorizado.*

	compartida con terceros.	
Monitoreo de eventos de Seguridad	*La Entidad no cuenta con una solución de monitoreo de eventos de seguridad en la plataforma tecnológica.*	*Sistemas de información con análisis y 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*	*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*

	perdida de información.	*equipos a la red de la entidad aplicando plantillas de seguridad.*
Seguridad en proyectos TI	*La entidad en la actualidad incluye en sus proyectos de contratación, aspectos básicos como acuerdos de confidencialidad. Sin embargo, no cuenta con políticas documentadas establecidas para la relación de con los proveedores acordes al SGSI.*	*Políticas de relación con proveedores y gestión de proyectos acorde al SGSI.*
Gestión de Vulnerabilidades	*Se realizan pruebas de Ethical Hacking anualmente para análisis de vulnerabilidades de la entidad.*	*Sistemas de información con vulnerabilidades conocidas mitigadas.*

Continuidad de Negocio	*La entidad no cuenta con un plan de continuidad tecnológica, que establezca la criticidad de los servicios tecnológicos y sus tiempos de recuperación. 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 computo 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 computo 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.	*No se está realizando concientización al personal de la entidad con respecto al 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.*

Para lo anterior se requiere seguir liberando e implementando 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 servidores, fortalecimiento de controles de acceso físico y lógica de la Entidad.

8. PORTAFOLIO DE PROYECTOS

Conforme a la alineación estrategita para el cumplimiento de las iniciativas y macroproyectos, se plantea el siguiente catálogo de proyectos 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*	*x*	*X*	*x*	*x*	*x*	*5*	*2*	*1*	*2*

	determinado para su recuperación y restablecimiento. *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.*									

IMPLEMENTACIÓN DEL MSPI	*La entidad se encuentra en un avance del 19% en la implementación del MSPI, para el año pasado la entidad debió alcanzar el 100% de avance, lo que constituye un incumplimiento a los decretos establecidos por MinTIC. Actualmente se tienen hallazgos por parte de la Contraloría General de la República relacionados al incumplimiento de estos lineamientos. Por lo tanto, debe implementarse el MSPI urgentemente para cumplir con la*	*x*	*x*	*x*	*x*	*x*	*3*	*3*	*2*	*0*

	política de Gobierno Digital y subsanar los hallazgos reportados.									
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
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*	-	-	x	-	x	2	2	0	0

	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.									
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 tratar esta problemática y disminuir su probabilidad de ocurrencia.*	-	-	*x*	-	*x*	*1*	*2*	*0*	*0*

SISTEMA DE DETECCIÓN Y VISIBILIDAD ANÁLISIS DE VULNERABILIDADES INTERNAS CONTRA AMENAZAS PERSISTENTES. (DDI)	*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 que puedan estar causando degradación en el servicio, o vulnerabilidades o brechas de seguridad que puedan ser*	-	-	*x*	-	*x*	*1*	*2*	*0*	*0*

	aprovechadas para afectar la integridad, confidencialidad o disponibilidad de la información y con lo anterior la operación del negocio.									
SISTEMA PARA GESTIÓN Y CORRELACIÓN DE EVENTOS (SIEM)	*La organización realiza análisis de eventos de forma independiente, lo cual no garantiza una correcta interpretación para la detección de posibles brechas, o incidentes, lo que hace necesario implementar un sistema centralizado para el análisis eficaz de toda esta información.*	-	-	*x*	-	*x*	*2*	*2*	*0*	*0*

SISTEMA DE DEFENSA PARA PROTECCIÓN Y MONITOREO DE BASES DE DATOS - (DAM)	*Teniendo en cuenta los resultados de las investigaciones realizadas por entidades especializadas en seguridad como lo es Kaspersky Lab, las empresas grandes en un solo incidente de ciberseguridad les cuesta a las empresas grandes un promedio de $861,000 dólares. Por su parte, las empresas pequeñas y medianas (PyMES) terminan pagando $86,500 dólares* *Lo más alarmante es que el costo de la recuperación aumenta significativamente*	-	-	x	-	x	2	2	0	0

	según el momento en que se descubre el ataque. Las PyMES tienden a pagar 44% más por recuperarse de un ataque descubierto una semana o más después de que se originara, en comparación con los ataques detectados el mismo día. *Conforme a lo anterior el Ministerio debe desarrollar la capacidad de detectar posibles eventos o situaciones no deseadas antes de que estas se conviertan en incidentes y puedan causar impactos*									

	monetarios o que puedan afectar la reputación de la entidad. Por lo cual, se debe adquirir una solución para monitoreo de bases de datos que permitan detectar manipulación no autorizada de información, robo o perdida de la misma.									
IMPLEMENTACIÓN DE SISTEMA DE ANÁLISIS DE VULNERABILIDADES Y FIREWALL EN ESTACIONES DE TRABAJO	*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 que los equipos cuenten con un software Antivirus, se*	-	-	*x*	-	*x*	*1*	*2*	*0*	*0*

	requiere que tengan una solución integral de protección, en la cual se cuenta con sistemas de análisis de vulnerabilidades y prevención de eventos									
IMPLEMENTACIÓN DE HERRAMIENTA DE CIFRADO DE EQUIPOS Y ARCHIVOS	*Si la entidad llega a sufrir hurto de sus equipos, la información en su interior no se encuentra cifrada, es necesario implementar cifrado de los equipos para evitar divulgación no autorizada de información sensible en caso de robo o perdida.*	-	-	*x*	-	*x*	*1*	*2*	*0*	*0*

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 que ningún sistema de información es invulnerable, de la misma forma sucede con los riesgos de desastre naturales, los cuales no pueden ser prevenidos.*	*x*	*X*	*x*	*x*	*x*	*4*	*2*	*1*	*2*

	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 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 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 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 no ejecuta periódicamente análisis de vulnerabilidades a su infraestructura, lo que no permite evidencias mejoras.*	-	-	*x*	-	*x*	*2*	*2*	*0*	*0*

RENOVACIÓN ANUAL DE LICENCIAMIENTO Y SOPORTE DE INFRAESTRUCTURA TECNOLÓGICA DE SEGURIDAD DEL MINISTERIO DE TRANSPORTE.	*Desde la primera semana de febrero, la infraestructura de seguridad se encuentra sin licenciamiento, es decir, sin soporte y sin actualizaciones, lo que deja vulnerables las redes y la infraestructura del Ministerio. Se requiere mantener un presupuesto definido para la renovación de los licenciamientos de la infraestructura para evitar mayores brechas de seguridad.*	*x*	*x*	*x*	*x*	*x*	*3*	*2*	*0*	*3*

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 información del Ministerio.*	-	-	-	-	*x*	*1*	*1*	*0*	*0*

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, 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*	*x*	*x*	*x*	*X*	*X*	*2*	*4*	*1*	*0*

	de Carga (RNDC), RUNT, entre otros.									
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*	-	-	*x*	-	-	-	*1*	*0*	*0*

	MINTIC, numeral A.6.2. Donde es necesario proteger la información que es consultada, procesada y evitar su 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. DETALLE DEL PLAN Y CRONOGRAMA

Con base en los proyectos propuestos y ruta crítica para la ejecución de estos, se planifica la ejecución de los mismos con una proyección a cuatro años como se muestra a continuación:

<table>
<tr><th colspan="2">2019</th><th colspan="2">2020</th><th colspan="2">2021</th><th colspan="2">2022</th></tr>
<tr><th>I – Semestre</th><th>II – Semestre</th><th>I – Semestre</th><th>II – Semestre</th><th>I – Semestre</th><th>II – Semestre</th><th>I – Semestre</th><th>II – Semestre</th></tr>
<tr><td colspan="8">PROYECTOS DE GESTIÓN DE LA SEGURIDAD – (SGSI / MSPI)</td></tr>
<tr><td colspan="2" rowspan="3">Planificación y elaboración de los lineamientos, procesos y procedimientos que componen el SGSI.</td><td colspan="2" rowspan="2">Implementación de los lineamientos, procesos y procedimientos que componen el SGSI.</td><td>Seguimiento y apropiación de los documentos del SGSI</td><td>Preauditoria NTC ISO 27001:2013 Sistema de Gestión de Seguridad de la Información (Proceso Gestión de Tecnologías y seguridad de la información)</td><td>Certificación NTC ISO 27001:2013 Sistema de Gestión de Seguridad de la Información (SGSI) (Proceso Gestión de Tecnologías y seguridad de la información)</td><td>Extensión del alcance del SGSI a los procesos misionales de la entidad Preauditoria NTC ISO 27001:2013 Sistema de Gestión de Seguridad de la Información (Procesos misionales y Proceso Gestión de Tecnologías y seguridad de la información)</td></tr>
<tr><td colspan="4">Mantenimiento y mejora continua del SGSI</td></tr>
<tr><td colspan="2">• Generación de Análisis de Riesgos de Disponibilidad (Selección procesos BIA)</td><td>• Generación Análisis BIA (Toda la entidad)
• Establecimiento recursos</td><td>• Definición DRP (Plan de Recuperación de Desastres)
• Ejecución de pruebas DRP</td><td colspan="2">Diseño de BCP (Plan de continuidad de negocio)</td></tr>
</table>

<table>
<tr><th colspan="2">2019</th><th colspan="2">2020</th><th colspan="2">2021</th><th colspan="2">2022</th></tr>
<tr><th>I – Semestre</th><th>II – Semestre</th><th>I – Semestre</th><th>II – Semestre</th><th>I – Semestre</th><th>II – Semestre</th><th>I – Semestre</th><th>II – Semestre</th></tr>
<tr><td colspan="2"></td><td colspan="2">• Definición preliminar de estrategia de respaldo y retención</td><td>necesario para redefinición estrategia de respaldo y retención.</td><td>• – Plan de recuperación de desastres – Actualización BIA</td><td colspan="2"></td></tr>
<tr><td colspan="2" rowspan="2">Implementación de guía para la administración del riesgo definida por el DAFP para la gestión de riesgos de seguridad digital</td><td colspan="6">Acompañamiento y seguimiento de riesgos de seguridad digital</td></tr>
<tr><td colspan="6">Mejora continua de la gestión y metodología de riesgos</td></tr>
<tr><td colspan="8">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="8">Ejecutar plan de concientización y comunicación anual del SGSI</td></tr>
<tr><td colspan="8">RENOVACIONES Y ACTIVIDADES PERIÓDICAS</td></tr>
<tr><td colspan="8">Ejecución anual de pruebas de Ethical Hacking (Contratadas e internas)</td></tr>
<tr><td colspan="8">Remediación anual de vulnerabilidades (Contratadas e internas)</td></tr>
<tr><td colspan="8">Renovación anual de certificados SSL (3 años)
Ethical Hacking e implementación de sistemas de firma digital para tramite documental</td></tr>
<tr><td colspan="2">Renovación de licenciamiento infraestructura de seguridad año 2019.</td><td colspan="2">Renovación de licenciamiento infraestructura de seguridad año 2020.</td><td colspan="2">Renovación de licenciamiento infraestructura de seguridad año 2021</td><td colspan="2">Renovación de licenciamiento infraestructura de seguridad año 2022.</td></tr>
</table>

<table>
<tr><th colspan="8">NUEVOS PROYECTOS DE INFRAESTRUCTURA DE SEGURIDAD INFORMÁTICA Y CONTINUIDAD DE TI</th></tr>
<tr><th colspan="2">2019</th><th colspan="2">2020</th><th colspan="2">2021</th><th colspan="2">2022</th></tr>
<tr><th>I Semestre</th><th>II Semestre</th><th>I Semestre</th><th>II Semestre</th><th>I Semestre</th><th>II Semestre</th><th>I Semestre</th><th>II Semestre</th></tr>
<tr><td rowspan="2">N/A</td><td rowspan="2">Implementación de sistema de análisis de vulnerabilidades y firewall en estaciones de trabajo (Endpoints)</td><td colspan="6">CENTRO DE COMPUTO ALTERNO
(Susceptible a cambios según decisión de tenerlo en la Nube o local)</td></tr>
<tr><td colspan="2">Implementación de herramienta de cifrado de equipos y archivos</td><td colspan="2">Implementar correlacionador de eventos (SIEM)</td><td colspan="2" rowspan="2">Implementación de escritorios virtuales</td></tr>
<tr><td>N/A</td><td>Firewall adicional para implementación de redundancia.</td><td colspan="2" rowspan="2">Sistema de defensa para protección y monitoreo de bases de datos – (DAM)</td><td colspan="2">Definición e Implementación Política BYOD</td></tr>
<tr><td>N/A</td><td>Sistema de análisis de vulnerabilidades (WAS)</td><td colspan="2">Programa de protección contra la fuga de información DLP</td><td colspan="2">SOC – Centros de Operaciones de Seguridad /NOC – Centros de Operaciones de Redes</td></tr>
</table>

10. COSTO APROXIMADO DE EJECUCIÓN DE PROYECTOS POR AÑO

2019 (EJECUTADO)		2020 (EJECUTADO)		2021		2022	
Proyecto	**Valor**	**Proyecto**	**Valor**	**Proyecto**	**Valor**	**Proyecto**	**Valor**
n/a	n/a	Pruebas de Ethical Hacking anual (Contratada)	$ 50.000.000	Pruebas de Ethical Hacking anual (Contratada)	$ 50.000.000	Pruebas de Ethical Hacking anual (Contratada)	$ 50.000.000
n/a	n/a	Remediación anual de vulnerabilidades (Contratada)	$ 30.000.000	Remediación anual de vulnerabilidades (Contratada)	$ 30.000.000	Remediación anual de vulnerabilidades (Contratada)	$ 30.000.000

Renovación de licenciamiento infraestructura de seguridad año 2019 (FW, IPS, WAF, Sandbox)	*$ 400.000.000*	*Renovación de licenciamiento infraestructura de seguridad año 2020 (FW, IPS, WAF, Sandbox)*	*$ 410.000.000*	*Renovación de licenciamiento infraestructura de seguridad año 2021 (FW, IPS, WAF, Sandbox)*	*$ 410.000.000*	*Renovación de licenciamiento infraestructura de seguridad año 2021 (FW, IPS, WAF, Sandbox)*	*$ 410.000.000*
Implementar correlacionador de eventos (SIEM) x 2 años	*$ 572.000.000*	*Implementación de herramienta de cifrado de equipos y archivos*	*$ 140.000.000*	*Preauditoria NTC ISO 27001:2013 Sistema de Gestión de Seguridad de la Información.*	*$40.000.000*	*Implementación de escritorios virtuales (FASE I)*	*$ 1.200.000.000*
Sistemas AntiDDOS x 2 años	*$ 480.000.000*					*Certificación NTC ISO 27001:2013 Sistema de Gestión de Seguridad de la Información (SGSI).*	*$ 40.000.000*
Web Application Scanner (WAS) x 1 año	*$ 35.000.000*			*Renovación SIEM x 1 año*	*$ 140.000.000*	*Renovación SIEM x 1 año*	*$ 140.000.000*
Sistema de defensa para protección y	*$ 662.267.284*			*Renovación DAM x 1 año*	*$ 150.000.000*	*Renovación DAM x 1 año*	*$ 112.000.000*

monitoreo de bases de datos – (DAM) x 2 años							
				Renovación DDOS x 1 año	*$ 130.000.000*	*Renovación DDOS x 1 año*	*$ 130.000.000*
						Programa de protección contra la fuga de información DLP	*$ 200.000.000*
						SOC – Centros de Operaciones de Seguridad /NOC – Centros de Operaciones de Redes	*$ 150.000.000*
Total	***2.149.267.284***	***Total***	***630.000.000***	***Total***	***950.000.000***	***Total***	***2.462.000.000***
Total $ 6.191.267.284							
NOTA: Los proyectos a ejecutar por cada vigencia (año) podrán verse sometidos a modificaciones, conforme al presupuesto asignado por la alta dirección.							

11. 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.

12. 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.

13. 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.*

14. 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*

15. CONTROL DE CAMBIOS:

VERSIÓN	***FECHA***	***MODIFICACIONES***
V1.2	*Diciembre-2020*	*Ajuste de cronograma de actividades y proyectos para los años 2021 y 2022, con base a la asignación de recursos y avance de implementación del MSPI*
v1.1	*Diciembre-2019*	*Ajuste de proyectos para año 2020 conforme a disponibilidad presupuestal.*
v1.0	*Mayo-2019*	*Versión inicial del documento*

16. RESPONSABLE DEL PLAN

Nombre completo: José Ricardo Acevedo
Cargo: Coordinador Grupo TIC y CIO
Dependencia: Grupo TIC
E mail: jacevedo@mintransporte.gov.co