PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – PESI v 1.1

MINISTERIO DE TRANSPORTE

2019 - 2022

Grupo de Tecnología de la Información y las Comunicaciones

DICIEMBRE 2019

TABLA DE CONTENIDO

1. OBJETIVO

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.

1.1. Objetivos Específicos

- Realizar diagnóstico inicial de implementación del SGSI de la organización.
- Priorizar las necesidades para la implementación y mejora continua del SGSI.
- Realizar ejercicios de arquitectura empresarial para definición, planificación y disposición de recursos para los proyectos.
- Priorizar los proyectos a implementar para la correcta implementación del SGSI.
- Elaborar Plan estratégico de seguridad de la información.

2. 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.

3. CONTROL DE CAMBIOS:

Versión	Fecha	Modificaciones
v1.1	Diciembre-2019	Ajuste de proyectos para año 2020 conforme a disponibilidad presupuestal.
v1.0	Mayo-2019	Versión inicial del documento

4. TÉRMINOS Y DEFINICIONES

- **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.

5. 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

6. 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.

7. ANÁLISIS DE SITUACIÓN ACTUAL

La situación actual 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

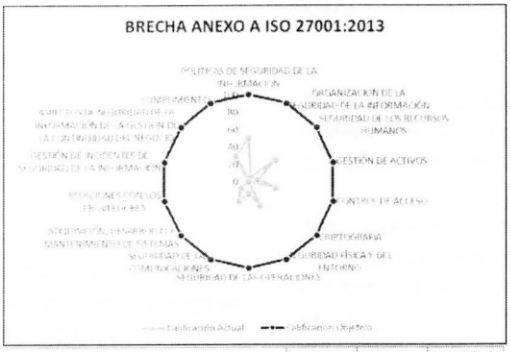
Puntaje Entidad	Valores de Referencia					
	Puntaje máximo grupo par	Quintiles				
		1	2	3	4	5
70.8	89.2	70.8				

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
1. 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.
2. 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.	Política general y políticas del sistema actualizadas, divulgadas y aplicadas por toda la entidad.

		Sin embargo, la política actual debe actualizarse e incluir aspectos adicionales para robustecerla. Se requiere de un manual de políticas de seguridad orientado a los usuarios del Ministerio en todos sus niveles.	
3.	**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).
4.	**Acceso a la Información**	No se cuenta con un índice de información clasificada y reservada. No se encuentra realizar un inventario de activos de información con la clasificación solicitada por MinTIC. La entidad cuenta con la siguiente infraestructura de seguridad informática:	Política y procedimiento de control de acceso lógico implementados. Dueños de proceso concientizados para la definición de segregación de funciones.
5.	**Seguridad Perimetral Lógica**	**Sección con información clasificada reservada.** **(Consultable solo en el documento físico)**	**Sección con información clasificada reservada.** **(Consultable solo en el documento físico)**

		Sección con información clasificada reservada. **(Consultable solo en el documento físico)**	**Sección con información clasificada reservada.** **(Consultable solo en el documento físico)**
6.	**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	Áreas seguras plenamente identificadas y documentadas que cuenten con un Sistema de CCTV con cobertura para las mismas.

		Sección con información clasificada reservada. **(Consultable solo en el documento físico)**	Control de acceso físico a las instalaciones estricto, con verificación de ingreso de equipos propios y de externos documentados y controlados en las bitácoras.
7.	**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.
8.	**Transferencia Segura de Información**	**Sección con información clasificada reservada.** **(Consultable solo en el documento físico)**	Información almacenada o transportada fuera de la organización protegida contra acceso no autorizado.
9.	**Monitoreo de eventos de Seguridad**	**Sección con información clasificada reservada.** **(Consultable solo en el documento físico)**	Sistemas de información con análisis y correlación de logs que permita identificar posibles eventos o brechas de seguridad y prevenir incidentes.
		La Entidad implemento certificados de navegación segura SSL para que las aplicaciones web funcionen sobre HTTPS.	Renovación de los certificados SSL para los aplicativos de la Entidad.
10.	**Seguridad en redes y comunicaciones**	**Sección con información clasificada reservada.** **(Consultable solo en el documento físico)**	**Sección con información clasificada reservada.** **(Consultable solo en el documento físico)**

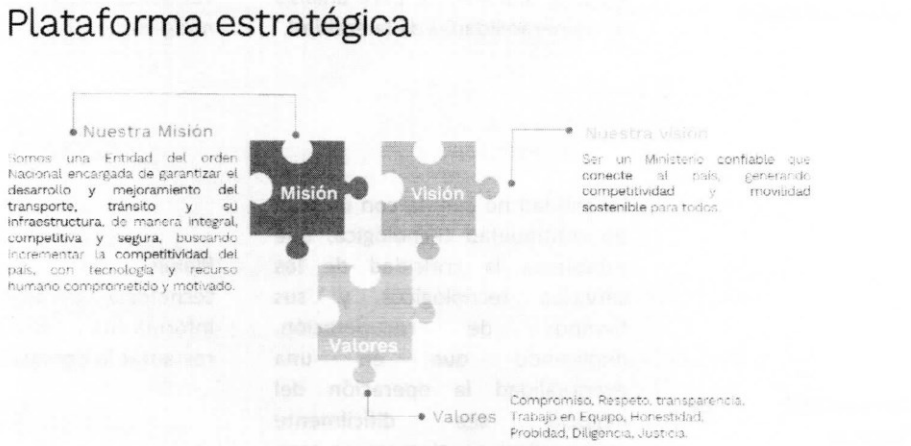
11. Seguridad en proyectos TI	La entidad en la actualidad incluye en sus proyectos de contratación, aspectos básicos como acuerdos de confidencialidad. Sin embargo, no cuenta con políticas documentadas establecidas para la relación de con los proveedores acordes al SGSI.	Políticas de relación con proveedores y gestión de proyectos acorde al SGSI.
12. Gestión de Vulnerabilidades	Se realizan pruebas de Ethical Hacking anualmente para análisis de vulnerabilidades de la entidad.	Sistemas de información con vulnerabilidades conocidas mitigadas.
13. Continuidad de Negocio	**Sección con información clasificada reservada.** **(Consultable solo en el documento físico)**	**Sección con información clasificada reservada.** **(Consultable solo en el documento físico)**
14. Capacitación y sensibilización en Seguridad de la Información.	**Sección con información clasificada reservada.** **(Consultable solo en el documento físico)**	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.

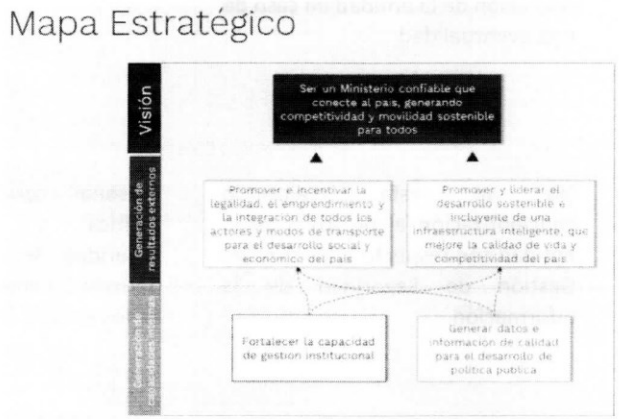
8. ALINEACIÓN ESTRATÉGICA

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.

9. 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

Sección con información clasificada reservada.

(Consultable solo en el documento físico)

GOBIERNO DIGITAL								
TIC para el Estado	TIC para la socieda d	Seguridad y Privacidad (MSPI)	Servicios Ciudadanos Digitales	Arquitectura TI Colombia	Lineamientos impactados (Arquitectura TI)	Gobierno Digital - Consolidado		
x	X	x	x	x	5	2	1	2
x	x	x	x	x	4	2	0	3

Sección con información clasificada reservada. **(Consultable solo en el documento físico)**	x	x	x	x	x	3	3	2	0
	-	-	x	-	-		0	1	0
	-	-	x	-	x	2	2	0	0
	-	-	x	-	x	1	2	0	0

Sección con información clasificada reservada.

(Consultable solo en el documento físico)

-	-	x	-	x	1	2	0	0
-	-	x	-	x	2	2	0	0

Sección con información clasificada reservada. **(Consultable solo en el documento físico)**	-	-	x	-	x	2	2	0	0

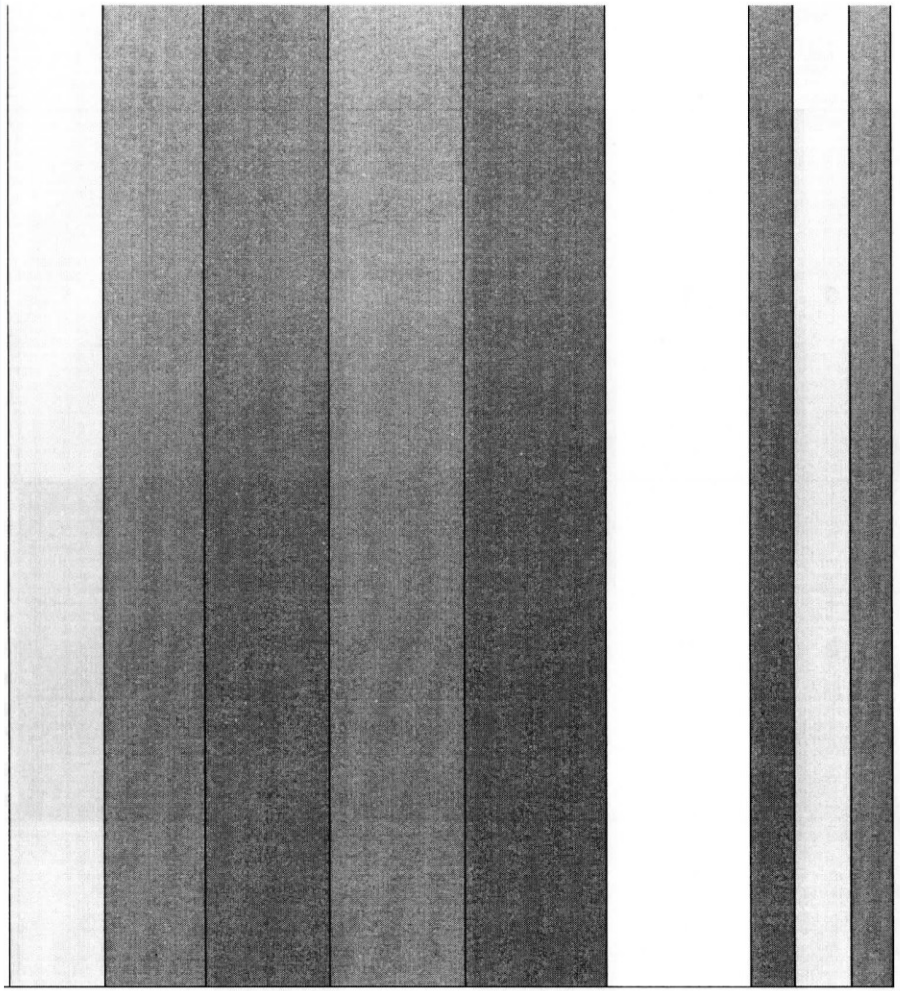
Sección con información clasificada reservada.

(Consultable solo en el documento físico)

-	-	x	-	x	1	2	0	0
-	-	x	-	x	1	2	0	0
x	X	x	x	x	4	2	1	2

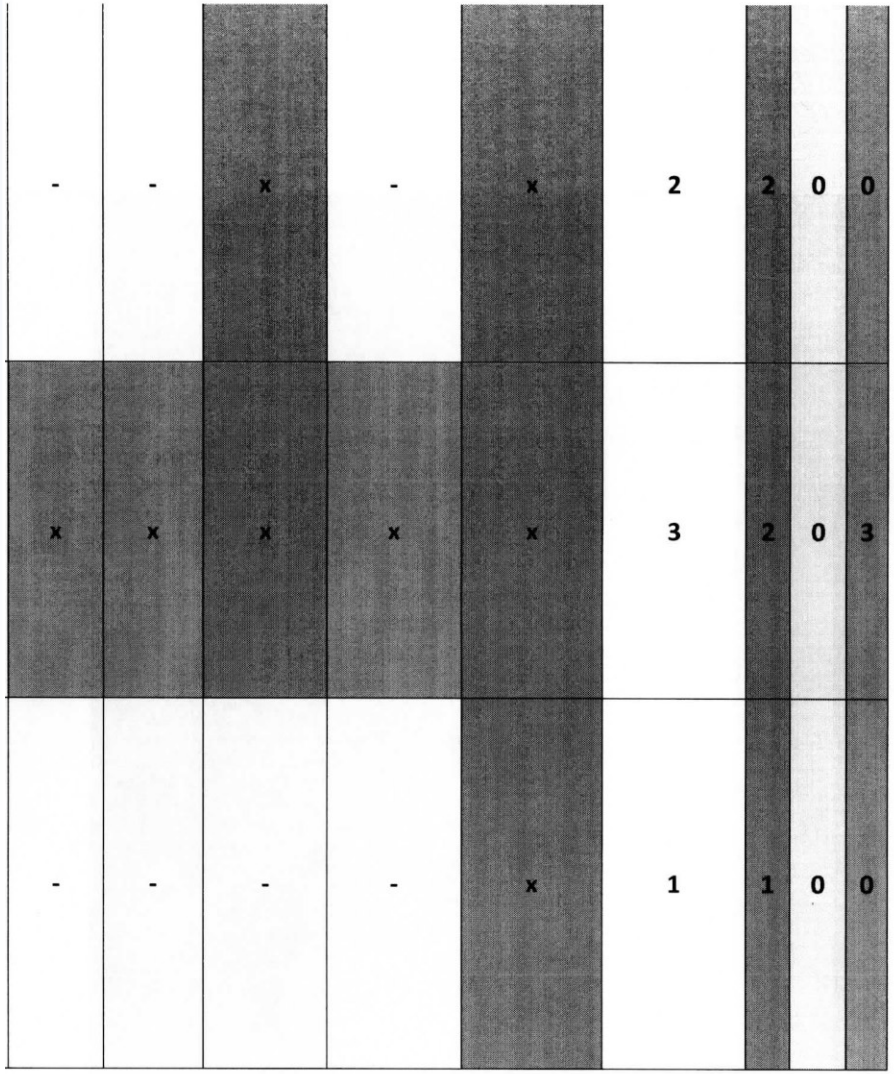
Sección con información clasificada reservada.

(Consultable solo en el documento físico)



Sección con información clasificada reservada.

(Consultable solo en el documento físico)



Sección con información clasificada reservada.

(Consultable solo en el documento físico)

x	x	x	X	X	2	4	1	0
-	-	x	-	-	-	1	0	0

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 y adecuación de sus instalaciones físicas.

10. PLAN DE EJECUCIÓN DE ACTIVIDAD Y PROYECTOS – PESI

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="2">Implementación de los lineamientos, procesos y procedimientos que componen el SGSI.</td><td rowspan="2">Implementación de los lineamientos, procesos y procedimientos que componen el SGSI.</td><td>Auditoría Externa Preparatoria para certificación ISO 27001:2013 (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 colspan="2">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="5">Mantenimiento y mejora continua del SGSI</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="2">Aplicación de instrumento MINTIC para medición del estado de implementación del sistema</td><td colspan="2">Aplicación de instrumento MINTIC para medición del estado de implementación del sistema</td><td colspan="2">Aplicación de modelo para medición de madurez del SGSI</td><td colspan="2">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="2">N/A</td><td>• Análisis BIA (Toda la entidad)
• Definición estrategia de respaldo y retención</td><td>Definición DRP (Plan de Recuperación de Desastres)</td><td colspan="2">Ejecución de pruebas DRP
- Plan de recuperación de desastres – Actualización BIA</td><td colspan="2">Diseño de BCP
(Plan de continuidad de negocio)</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="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">NUEVOS PROYECTOS DE INFRAESTRUCTURA DE SEGURIDAD INFORMÁTICA Y CONTINUIDAD DE TI</td></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="3">Implementación de escritorios virtuales</td></tr>
<tr><td>N/A</td><td rowspan="2">Firewall Adicional para implementación de redundancia.</td><td colspan="2">Programa de protección contra la fuga de información DLP</td><td colspan="2">Sistema de control de acceso basado en identidades y política BYOD</td></tr>
<tr><td>N/A</td><td>Sistema de detección y visibilidad análisis de vulnerabilidades internas contra amenazas persistentes.</td><td colspan="2">Sistema de defensa para protección y monitoreo de bases de datos – (DAM)</td><td colspan="2">SOC - Centros de Operaciones de Seguridad /NOC - Centros de Operaciones de Redes</td></tr>
</table>

11. COSTO APROXIMADO DE EJECUCIÓN DE PROYECTOS POR AÑO

2019 (EJECUTADO)		2020		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	$ 20.000.000	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	Auditoría Externa ISO27001:2013	$ 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 monitoreo de bases de datos – (DAM) x 2 años	$ 662.267.284			Renovación DAM x 1 año	$ 112.000.000	Renovación DAM x 1 año	$ 112.000.000
				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	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	SOC - Centros de Operaciones de Seguridad /NOC - Centros de Operaciones de Redes	$ 150.000.000
Total	**$ 905.000.000**	**Total**	**$ 630.000.000**	**Total**	**$ 1.282.000.000**	**Total**	**$ 2.462.000.000**
Total $ 6.523.267.284							
NOTA: Los proyectos a ejecutar por cada vigencia (año) podrán verse sometidos a modificaciones, conforme al presupuesto asignado por la alta dirección.							

12. 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.

13. 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.

ELABORÓ	REVISÓ	APROBÓ
Nombre: José Ricardo Acevedo **Cargo: Coordinador Grupo TIC y CIO** Hugo Alejandro Casallas **Cargo: CISO Ministerio de Transporte** Juan Carlos Valenzuela B **Cargo: Esp. Seguridad de la Información**	Nombre: José Ricardo Acevedo **Cargo: Coordinador Grupo TIC y CIO**	Nombre: Ángela María Orozco Gómez **Cargo: Ministra de Transporte** Fecha: 26-Dic-2019