Plan Estratégico de Seguridad de la Información **(PESI).**

TRANSMILENIO S.A.

Julio - 2018

ALCALDÍA MAYOR DE BOGOTÁ D.C.

BOGOTÁ MEJOR PARA TODOS

TABLA DE CONTENIDO

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

INTRODUCCIÓN

El Gobierno en Línea en Colombia ha venido siendo implementado de manera sistemática y coordinada en todas las entidades públicas. En los últimos años, se han evidenciado cambios y avances en el uso y apropiación de la tecnología como herramienta que permite mejorar la gestión pública, la provisión de servicios y la transparencia, encaminados a cumplir las funciones del Estado.

TRANSMILENIO S.A., como entidad pública de orden territorial, adscrita a la Secretaria Distrital de Movilidad hace parte de las entidades públicas que han apropiado las iniciativas del Gobierno Nacional y las ha desplegado a todos sus niveles organizacionales, incluyéndolas en los objetivos estratégicos de la entidad y haciéndolas parte fundamental del Plan Estratégico Institucional.

En el desarrollo de sus funciones, TRANSMILENIO S.A., gestiona el desarrollo e integración de los sistemas de transporte público masivo intermodal de pasajeros de la ciudad de Bogotá D.C. y de la región, con estándares de calidad, dignidad y comodidad, permitiendo lograr la adecuada gestión de la información de la entidad. En atención a lo anterior, la entidad asumió el reto de implementar el Sistema de Gestión en Seguridad de la Información, en adelante SGSI, siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno Digital, a su vez reglamentado a través de lo contenido en el título 9 del Decreto 1078 de 2015 para el sector de tecnologías de la información y comunicaciones y el Decreto 1008 de 2018 por el cual se establecen los lineamientos generales de la Estrategia de Gobierno Digital.

En la actualidad, TRANSMILENIO S.A. identifica la información como uno de los activos indispensables en la conducción y consecución de los objetivos definidos en el Plan Estratégico de la Entidad, razón por la cual es necesario establecer un marco en el cual se asegure que la información es protegida de manera adecuada independientemente del medio en la que ésta sea manejada, procesada, transportada o almacenada. Adicional a lo expuesto, en la medida en que los sistemas de información se constituyen en un apoyo de los procesos de la entidad, se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de la información.

TRANSMILENIO S.A. adopta una metodología para la identificación y valoración de los activos de información, y una metodología para la evaluación y tratamiento de los riesgos; siendo éste el medio más eficaz de tratar, gestionar y minimizar los riesgos, considerando el impacto para la entidad y las partes interesadas. Así mismo, el SGSI de TRANSMILENIO S.A. define políticas y procedimientos eficaces y coherentes con la estrategia de la entidad, como desarrollo de los controles adoptados para el tratamiento de los riesgos, los cuales están en continuo seguimiento y medición, a través del establecimiento de indicadores que aseguran la eficacia de los controles; apoyado en los programas de auditoria y la revisión por la dirección, que concluyen en la identificación de oportunidades de mejora las cuales son gestionadas para mantener la mejora continua del SGSI.

Para tal fin, la entidad ha adoptado los lineamientos normativos de: la NTC/ISO 27001:2013, la cual establece los requisitos para la implementación del SGSI, la NTC/ISO 31000:2011 que proporciona el esquema para la gestión de riesgos y las mejores prácticas, tales como GTC/ISO 27002:2015, ISO 27005:2009, entre otras; buscando mejorar el desempeño y la capacidad para prestar un servicio que responda a las necesidades y expectativas las partes interesadas.

Por otra parte, el Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETI), es un documento que expresa las intenciones de la organización, en la implementación de iniciativas y acciones que promuevan el uso de las Tecnologías de la Información y las Comunicaciones – Tics como contribución al logro de los objetivos y lineamientos estratégicos enmarcados en el Plan Estratégico Institucional 2015, El PESI descrito en este documento está alineado completamente con el PETI.

El documento PETI define lineamientos para el mejoramiento del nivel de madurez institucional en la implementación de soluciones tecnológicas que generen valor y promuevan el cumplimiento de la misión con sostenibilidad tecnológica. El fortalecimiento y mejoramiento de la infraestructura tecnológica, el fortalecimiento de una mesa de ayuda, la implementación de los sistemas de seguridad de la información y la continuidad de negocio, la optimización en el procesamiento y análisis de información, el fortalecimiento

y mejora de los procesos institucionales (Estratégicos, Misionales y de Apoyo) y de gestión de la información y gobernabilidad de TI, de acuerdo con la Estrategia Gobierno Digital.

Finalmente, los lineamientos y proyectos para el desarrollo, optimización e implementación efectiva de los Sistemas de Información, así como las iniciativas que permitirán una adecuada gestión de la Infraestructura de Hardware/Software, basados en el MSPI y en las mejores prácticas de gestión de servicios y proyectos de TI, contribuirán no solo con el logro de los objetivos institucionales, sino en la generación de confianza en el uso de los mecanismos tecnológicos para una mejor relación Estado – Ciudadano y la protección de los activos de información (PETI).

1. OBJETIVO

Definir una estrategia de Seguridad de la información, en adelante PESI, liderada por la Dirección de TICs de TRANSMILENIO S.A., a partir de la vigencia 2018 y hasta la vigencia 2021, que responda a las necesidades de preservar la confidencialidad, la integridad y la disponibilidad sobre los activos de información.

1.1 OBJETIVOS ESPECÍFICOS

- Comunicar e implementar la estrategia de seguridad de la información.
- Incrementar el nivel de madurez en la gestión de la seguridad de la información.
- Implementar y apropiar el modelo de seguridad y privacidad de la Información – MPSI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
- Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.
- Asegurar los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.

2. ALCANCE DEL PESI

Teniendo en cuenta el análisis del contexto externo, interno y las partes interesadas, TRANSMILENIO S.A. define el alcance de su Sistema de Gestión en Seguridad de la Información (SGSI) y del PESI, en términos de las características de la entidad, su ubicación, sus activos y su tecnología, así:

TRANSMILENIO S.A adopta, establece, implementa, opera, verifica y mejora el SGSI para el proceso estratégico Gestión de TIC.

Asimismo, el SGSI se ira implementado y adoptando a cada uno de los procesos de manera gradual.

La entidad acorde con su naturaleza jurídica, misión y visión, encontró aplicables todos los requisitos de la NTC/ISO 27001:2013 y todos los controles del Anexo de dicha norma, excluyendo el control A.11.1.6 Áreas de despacho y carga.

En la ilustración 1, se resaltan los procesos que hacen parte del alcance del SGSI.

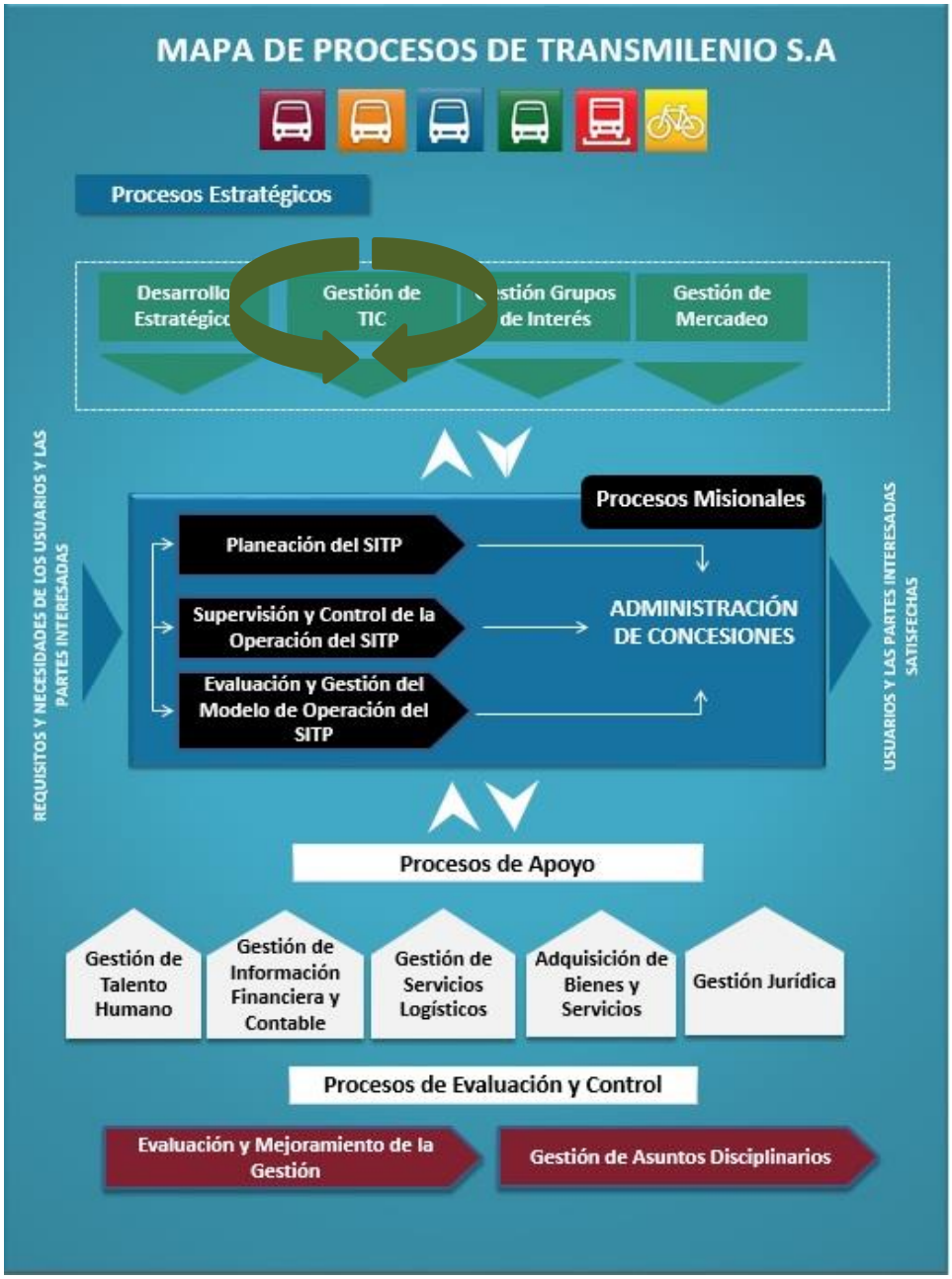

Ilustración 1. Mapa de procesos y alcance del SGSI

3. DEFINICIONES

Activo: en cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Análisis de Riesgo: proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Control: las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Guía: documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Norma: principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

Parte interesada: (Stakeholder) persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Política del SGSI: manifestación expresa de apoyo y compromiso de la alta dirección con respecto a la seguridad de la información.

Política: es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.

Procedimiento: los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

Riesgo: 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. (ISO/IEC 27000).

Seguridad de la información: preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

4. DOCUMENTOS DE REFERENCIA

- NTC/ISO 27001:2013
- NTC/ISO 27005:2009
- GTC/ISO 27002:2015
- Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL y Política de Gobierno Digital.

5. ESTRUCTURA ORGANIZACIONAL

La organización interna de la Empresa de Transporte del Tercer Milenio - TRANSMILENIO S.A., se presenta en la ilustración 2.

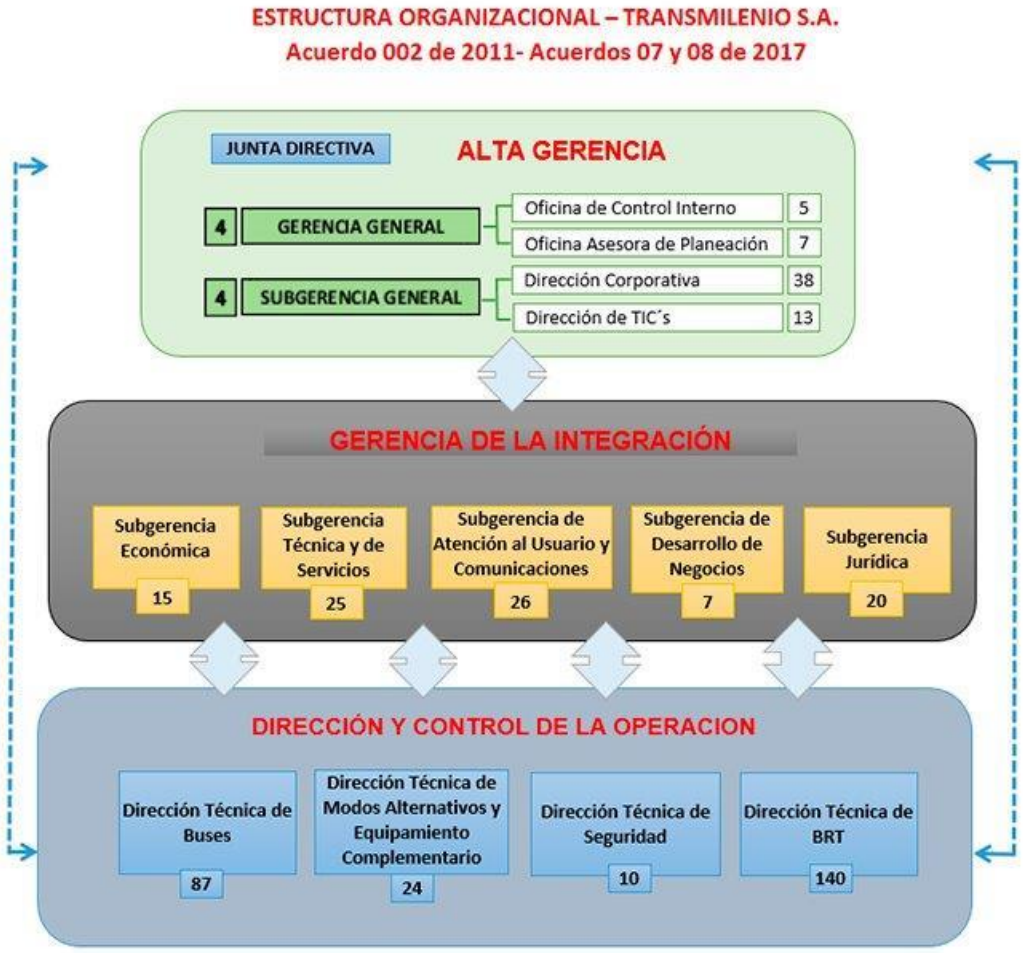

Ilustración 2. Organigrama de TRANSMILENIO S.A.

6. PLANEACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

En la actualidad y de acuerdo con lo establecido en el título 9 del Decreto Único Reglamentario 1078 de 2015 del Sector de Tecnologías de la Información y las Comunicaciones; TRANSMILENIO S.A. trabaja permanentemente en pos de implementar el SGSI siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno Digital con el fin de preservar la integridad, confidencialidad, disponibilidad y privacidad de la información mediante la adecuada gestión del riesgo, la aplicación de la normatividad vigente y la implementación de mejores prácticas relacionadas con seguridad de la información.

En efecto, el modelo del SGSI de TRANSMILENIO S.A. se basa en el ciclo de mejoramiento continuo PHVA (Planear, hacer, actuar y verificar), el cual asegura que el SGSI esté expuesto a revisiones continuas cuando existe un cambio importante en la infraestructura o se requiera mejorar su efectividad dependiendo de las mediciones de parámetros claves de su operación. Se cuenta, entonces, con un ciclo que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar este sistema.

A continuación, se describen los componentes de cada una de estas fases del ciclo:

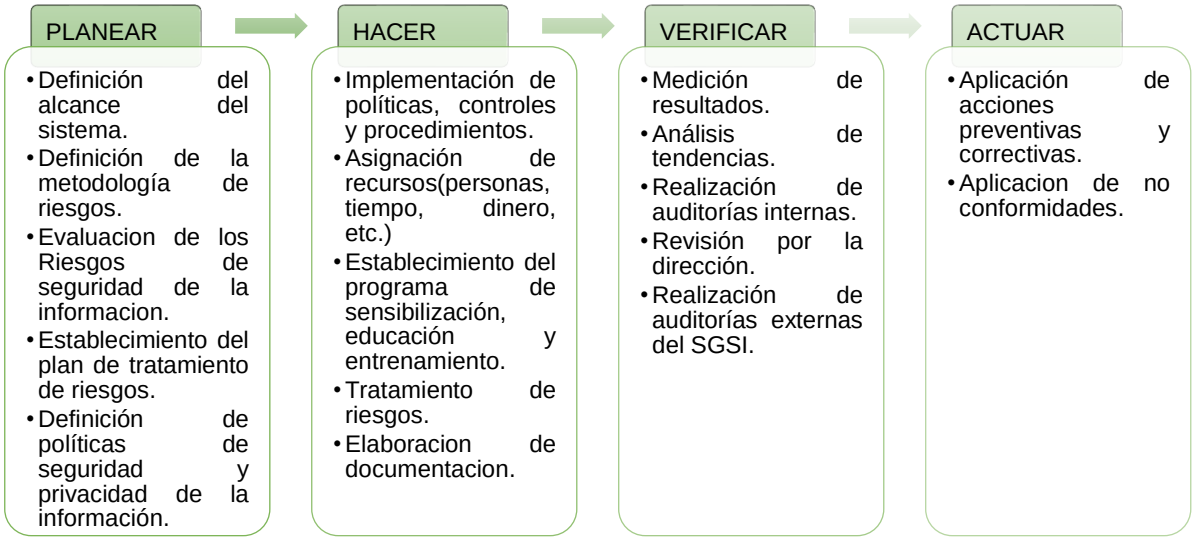

Ilustración 3. Fases del ciclo PHVA

6.1 CONTEXTO DE LA ENTIDAD

La Empresa de Transporte del Tercer Milenio - TRANSMILENIO S.A. es una sociedad pública por acciones del orden distrital con personería jurídica, autonomía administrativa, financiera, presupuestal y patrimonio propio, sometida al régimen de las Empresas Industriales y Comerciales del Estado y vinculada al Sector Movilidad dentro de la estructura administrativa del Distrito Capital.

La Empresa de Transporte del Tercer Milenio - "TRANSMILENIO S.A.", creada por el Acuerdo 04 de 1999 del Concejo de Bogotá D.C., es una entidad descentralizada del orden distrital, dotada de personería jurídica, autonomía administrativa y patrimonio independiente, bajo la forma de sociedad de capital público por acciones, constituida entre

y con aportes de entidades públicas del orden distrital, sometida al régimen jurídico de las empresas industriales y comerciales del Estado. La Dirección y Administración de TRANSMILENIO S.A. estará a cargo de una Junta Directiva y un Gerente. Los demás cargos de dirección y administración, su período y funciones serán las que se señalen en los estatutos. La Junta Directiva esta integrada por el Alcalde Mayor o su delegado quien la preside y cuatro (4) miembros designados de conformidad con los estatutos.

TRANSMILENIO S.A. garantiza la adecuada administración de los recursos provenientes de la prestación del servicio público masivo de transporte y demás ingresos que reciba, utilizando mecanismos financieros idóneos, con el fin de permitir la adecuada operación y la adquisición y reposición de los equipos por parte de los operadores con quienes celebre los respectivos contratos.

La organización interna de la Empresa de Transporte del Tercer Milenio TRANSMILENIO S.A., sociedad por acciones entre entidades públicas del Orden Distrital, está estructurada en tres ámbitos de gestión, así: (i) Alta Gerencia, (ii) Gerencia de la Integración y (iii) Dirección y Control de la Operación (ver ilustración 2).

El ámbito de la Alta Gerencia de la Empresa es responsable de la dirección general y estratégica de la misma, del desarrollo empresarial, de la implementación de buenas prácticas de gobierno corporativo y del emprendimiento de las acciones tendientes a la sostenibilidad del sistema, que garanticen el cumplimiento de su responsabilidad social. Este nivel dirige y articula la ejecución de los procesos de la Empresa orientados todos al cumplimiento de su misión.

El ámbito de la Gerencia de la Integración, responsable del monitoreo integral y sistemático de la vigilancia y control de la prestación del servicio de manera transversal en todos los sistemas de transporte público a cargo de la Empresa, contemplando los factores económicos, técnico, jurídico, de negocios y comunicacional, que garanticen el mejoramiento continuo del servicio en forma integral.

El ámbito de la Dirección y Control de la Operación ejecuta las acciones de vigilancia y control de los niveles de servicio en cada uno de los sistemas de transporte público a cargo de la Empresa, en coordinación directa con la Gerencia de la Integración, para

garantizar la calidad, cobertura, continuidad, eficiencia y acceso del Servicio Público de Transporte.

TRANSMILENIO S.A., quien actúa como ente gestor del Sistema Integrado de Transporte Público, tiene a su cargo la planeación estructural del Sistema y la definición del régimen técnico que regula la operación, gestión y control de la operación, así como la supervisión de todas las zonas del sistema.

Este modelo de gestión y programación de la operación del Sistema se orienta al uso eficiente de la flota, a la prestación del servicio público de transporte en condiciones de eficiencia, calidad y seguridad. [1],

En el marco del Plan Maestro de Movilidad, la carta de navegación de la ciudad en el tema, se establece la estructuración del nuevo Sistema Integrado de Transporte Público de Bogotá (SITP), como instrumento que garantiza mejorar la calidad de vida de los ciudadanos, optimizando los niveles de servicio para viajes que se realizan en la ciudad. El SITP es un sistema organizado e integrado de diferentes servicios de transporte (urbano, especial, complementario, troncal, alimentador y demás modos de transporte que se irán implementado) que buscan el cubrimiento efectivo del transporte en Bogotá.

Dentro del contexto también está garantizar que los equipos usados para la prestación del servicio incorporen tecnología de punta, teniendo en cuenta especialmente el uso de combustibles que generen el mínimo impacto ambiental.

En efecto, TRANSMILENIO S.A., reconoce que la información es uno de los activos más importantes para cumplir las funciones y objetivos que le han sido delegados por el Gobierno Distrital, de ahí la importancia de realizar un análisis del contexto interno y externo de la entidad, con relación a seguridad de la información, para identificar cuáles son los riesgos que pueden o afectan su capacidad para lograr los resultados esperados frente al SGSI; así como identificar cuáles son las necesidades y expectativas de las parte interesadas.

1 Fuente: Manual del Sistema de Gestión M-OP-001

En la ilustración 4 se detallan los diferentes actores que hacen parte del contexto interno y externo de la entidad.

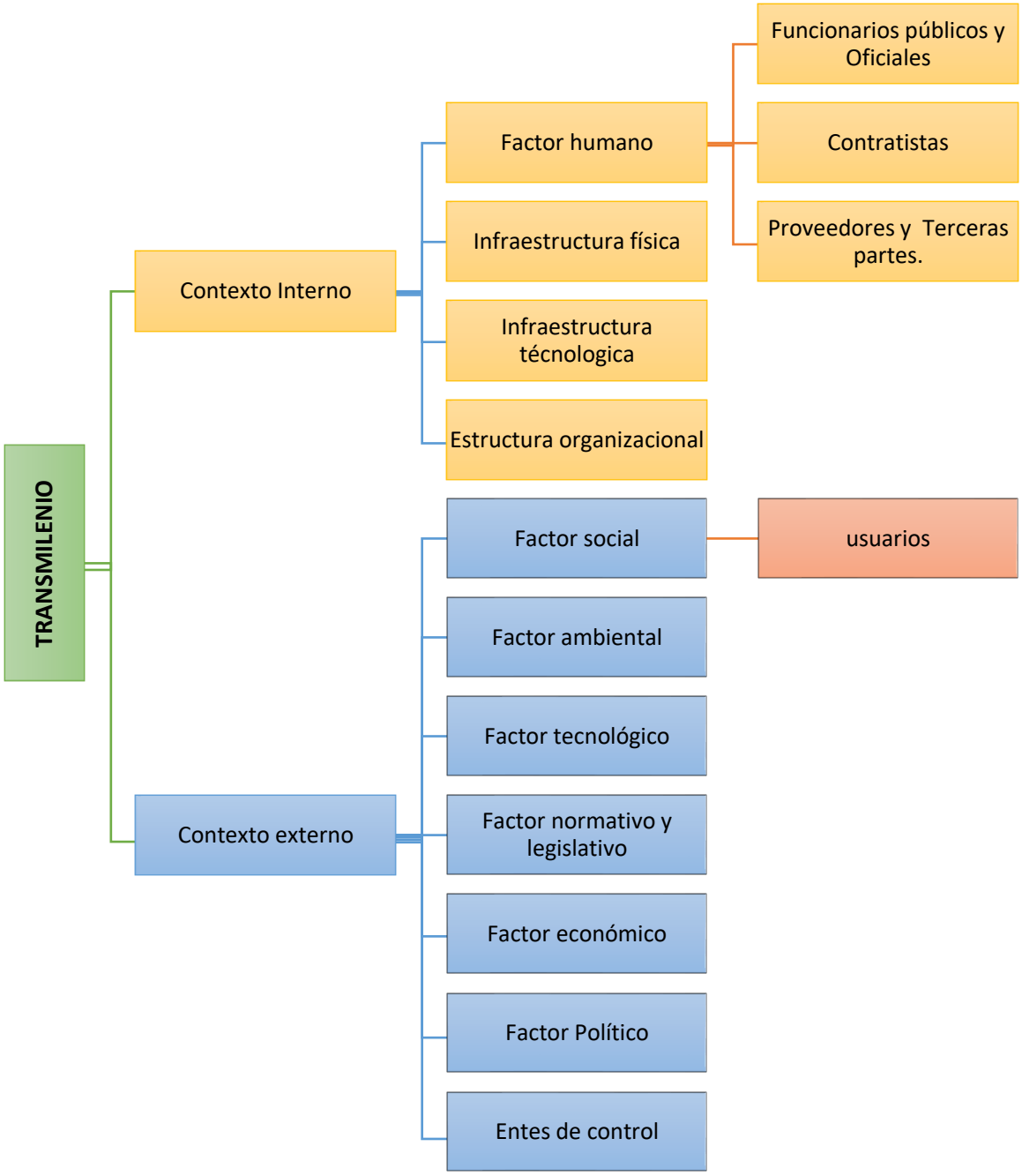

Ilustración 4. Contexto interno y externo de TRANSMILENIO S.A.

6.1.1 Contexto Interno

- **Factor Humano**

Las personas también hacen parte de los activos de información más importantes dentro de la entidad. En TRANSMILENIO S.A., estos activos se encuentran representados en servidores públicos, trabajadores oficiales, proveedores y terceras partes, que continuamente interactuan con los procesos de la entidad, y, por ende, gestionan, procesan, almacenan, distribuyen, intercambian y/o consultan información que puede ser reservada, sensible o interna. Por lo anterior, el factor humano representa una gran influencia para el cumplimiento de los lineamientos y las políticas de seguridad y privacidad de la información; situación que continuamente la entidad prevé a través de comunicados, programas de sensibilización y transferencia de conocimiento con relación a la seguridad de la información.

- **Infraestructura Física**

La sede principal de TRANSMILENIO S.A, se encuentra ubicada en Bogotá en la Av. Eldorado No. 69 - 76 / Edificio Elemento Torre 1 cuenta con unas instalaciones en arriendo, distribuida en 5 pisos del edificio Elemento. Se logró instalar en esta área 659 puestos de trabajo, un comedor, 5 cafeterías, una sala de bienestar, 11 salas de reuniones, 3 auditorios, una enfermería, una sala de espera, 2 recepciones, 19 oficinas de directivos, 6 cuartos de almacenamiento, una emisora, un cuarto de lactancia, 11 cuartos técnicos y eléctricos, 7 baterías de baños, una oficina de la Contraloría y 2 oficinas para otros entes, dichas oficinas cumplen con controles de seguridad para acceder a la misma, se exige porte del carnet institucional para los servidores públicos, contratistas y registro de ingreso para visitantes en la recepción del piso 1, y para el acceso de ingreso a la entidad, debe dirigirse al piso 7 en donde le entregan una identificación impresa y el acompañamiento por parte del funcionario correspondiente. Cuando se ingresen dispositivos tecnológicos se debe:

Los servidores públicos, contratistas, proveedores y terceras partes deben ser registrados en las bitácoras de la recepción del piso donde desarrollan sus actividades.

En cada uno de los pisos donde opera TRANSMILENIO S.A., se cuenta con:

a. Áreas seguras.
b. Sistemas de detección y extinción de incendios.
c. Áreas de evacuación.
d. Señalización de áreas.
e. El edificio cuenta con ocho (4) ascensores.
f. Para ingresar a los centros de cableado de cada piso, lo realiza únicamente personal autorizado con el uso de llaves.
g. Para le ingreso del Datacenter, lo realiza personal autorizado con el uso de sistemas biométricos.

- **Infraestructura Tecnológica**

TRANSMILENIO cuenta con un (1) DATACENTER, ubicado en las instalaciones de la oficina principal en Bogotá el cual soporta toda la gestión tecnológica con mayor capacidad de tener servicios tecnológicos, mediante una primera etapa de adquisición de equipos de Cómputo propios de última generación.

La Entidad actualizó la infraestructura de networking y seguridad con equipos de nueva generación, que permiten mayor administración, rapidez y seguridad de la información. Realizó la adopción de una estrategia de servicio de comunicaciones de largo plazo (hasta el 2019) para garantizar la disponibilidad de las mismas del personal en vía, para apoyo de la operación de la flota troncal, el reporte de incidentes de seguridad y daños en la infraestructura del Sistema, la cual generó ahorros importantes frente al sistema de Red con que se venía operando.

TRANSMILENIO implemento el aprovisionamiento de servicios de plataforma tecnológica en la nube PaaS e IaaS a mediano y largo plazo, por demanda, la cual permite el despliegue de sistemas de información y/o soluciones de software, con la movilidad que proporciona la nube (acceso desde cualquier dispositivo y lugar), generando economías de escala.

Desde el Datacenter, se prestan los servicios de la operación de la entidad soportadas en TI, solamente ingresa personal autorizado a través de un sistema biométrico, el cual cuenta con:

a. Sistemas de detección y extinción de incendios.
b. Racks de servidores, cableado y UPS independientes.
c. Cada rack de servidores cuenta con la seguridad por medio de llaves y el acceso se realiza si es estrictamente necesario.
d. La gestión de los servidores se hace remota a través de los esquemas de protección definida en las políticas de seguridad y privacidad de la información.

6.1.2 Contexto Externo

- **Factor Social**

TRANSMILENIO S.A. como Empresa del Distrito Capital, está encaminada a mejorar la calidad de vida de los usuarios del Sistema y en especial, al público con enfoque diferencial, es decir, a las poblaciones vulnerables. Los programas desarrollados buscan generar un nuevo pacto de confianza entre los usuarios y la entidad, que logren responder a la crisis a través de nuestras capacidades específicas. Es por esto, que TRANSMILENIO S.A., entiende la necesidad de ser parte clave en armonizar el éxito empresarial con el éxito de la sociedad, de conformidad con una de las máximas éticas del desarrollo sostenible: no pueden existir empresas exitosas en sociedades fracasadas. Esta máxima es coherente con la creación de valor compartido que coloca los problemas sociales no en la periferia sino en el centro de la acción empresarial. En este sentido, TRANSMILENIO S.A. ha desarrollado un programa de responsabilidad social alineado con la estrategia.

Por otra parte la Gestión Social es una estrategia que permite la interacción de la Entidad con la comunidad a través de instancias de participación con autoridades locales y distritales, donde se requiere la materialización de acciones y toma de decisiones para el abordaje de un problema, su estudio y comprensión, hasta el diseño y operación de propuestas que respondan a las necesidades de los usuarios y faciliten la divulgación de información relacionada con el Sistema TransMilenio en sus componentes zonal y troncal

mediante espacios de capacitación y sensibilización que fortalezcan los mecanismos de participación ciudadana y el sentido de pertenencia.

- **Factor Ambiental**

TRANSMILENIO S.A. en cumplimiento del factor ambiental interno y externo, ha implementado el Plan Institucional de Gestión Ambiental (PIGA), el cual ha permitido establecer las estrategias para la implementación de la gestión ambiental institucional y del Sistema de Transporte Masivo, en el marco de las competencias que tiene TRANSMILENIO S.A. como Ente Gestor del sistema. Desde la adopción del PIGA por parte de la Administración Distrital como herramienta de gestión, en la Entidad se ha implementado de manera progresiva diferentes estrategias y programas que apuntan al cumplimiento de los objetivos establecidos en el Plan de Gestión Ambiental de Distrito, va atender requisitos de carácter ambiental aplicables al modelo de Transporte Sostenible, en el cual el sistema Transmilenio es referente para dar cumplimiento a los requisitos normativos y otros compromisos que ha suscrito la Entidad[2]

En el marco de la implementación del PIGA se ha estructurado el Subsistema de Gestión Ambiental – SGA., en la cual se han estructurado los programas y actividades para realizar control y seguimiento a los parámetros ambientales propios del sistema, se han adoptado los mecanismos de coordinación interinstitucional para fortalecer estos procesos.
En cuanto a la gestión ambiental institucional, se han adoptado los programas para el uso y ahorro de recursos (agua, energía, papel, etc.), la gestión de residuos, y otros programas de gestión que han presentado avances a lo largo de la implementación del PIGA. La gestión ambiental en el marco del PIGA se ha hecho extensiva a las áreas que son administradas por la Entidad y en las cuales se desarrolla su nacionalidad.

Durante los últimos cuatro (4) años con la implementación del programa, se ha logrado mantener el índice de consumo de agua percápita en un valor por debajo del valor establecido como meta en 2012, como resultado de las acciones implementadas, principalmente el mantenimiento a la red hidráulica y a los dispositivos ahorradores, para

[2] **Fuente**: PIGA TRANSMILENIO S.A. V.2016

control de fugas y desperdicios, sumado a las actividades de socialización de buenas prácticas en el uso del agua que posiblemente redundaron en este resultado.

Este programa del componente de gestión ambiental institucional pretende alcanzar una reducción en la generación de residuos ordinarios en la sede administrativa, así como el manejo y gestión integral que redunde en la minimización de la cantidad entregada al servicio de recolección para su disposición final en el relleno sanitario del Distrito. Así mismo, se pretende implementar prácticas adecuadas de manejo que involucren todas las instancias del proceso, desde la misma fuente de generación de los residuos hasta el almacenamiento y entrega, para promover el aprovechamiento de los residuos.

En el Plan Institucional de Gestión Ambiental - PIGA de la Entidad se establecen dos líneas gestión: un componente de gestión ambiental interno que se enfoca a la gestión ambiental institucional de TRANSMILENIO S.A como Entidad y un componente externo enfocado a la gestión ambiental del Sistema Transmilenio en el marco de los contratos de concesión.

- **Factor Tecnológico**

TRANSMILENIO S.A. como Empresa del Distrito Capital, debe implementar, de manera sistemática y coordinada, la Estrategia de Gobierno Digital la cual es una estrategia del Gobierno Nacional liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones, que contribuye con la construcción de un Estado más eficiente, más transparente y participativo y que presta mejores servicios con la colaboración de toda la sociedad, mediante el aprovechamiento de las TIC.

En el campo tecnológico, los avances son vertiginosos, no sólo en cuanto a aplicaciones o servicios sino también en lo relacionado con la gestión de la tecnología al interior de las entidades, hecho que ha transformado los procesos y negocios al interior del mismo Estado.

Por lo anterior, TRANSMILENIO S.A. enfrenta grandes retos encaminados a mantener la seguridad de la información en el desarrollo de las siguientes actividades:

- Planear y conceptualizar soluciones tecnológicas encaminadas a la prestación de servicios de Gobierno Digital.
- Culminar la implementación de las cadenas de trámites y sistemas transversales diseñados.
- Realizar desarrollo/mantenimiento a las soluciones tecnológicas operadas por el Programa.
- Diseñar, desarrollar e implementar soluciones tecnológicas encaminadas a la prestación de servicios de Gobierno Digital.
- Implementar el sistema de gestión de seguridad de la información SGSI para el proceso de la dirección de TIC.

- **Factor Normativo y Legislativo**

TRANSMILENIO S.A., dispone de un marco normativo y regulatorio basado en las recomendaciones de las normas internacionales y normativas legales vigentes. Las normas, leyes, decretos y resoluciones, etc. que se han tenido en cuenta para la implementación del SGSI se encuentran identificadas y documentadas en el *Normograma 2018* [3].

- **Factor Económico**

TRANSMILENIO S.A. de acuerdo con el Plan Estratégico Institucional del 2015, definió un objetivo estratégico encaminado a implementar mecanismos que contribuyan al equilibrio financiero del sistema integrado de transporte público, gestionando los recursos para la expansión y mantenimiento del sistema. Así mismo identificando, desarrollando e implementando nuevas oportunidades de negocio o ingresos asociados a la explotación comercial de los diferentes componentes del sistema, tales como la explotación de la infraestructura y la explotación inmobiliaria.

[3] Ver Nomograma 2018.

TRANSMILENIO S.A promueve instrumentos financieros que conduzcan a promover el acceso al sistema integrado de transporte público a través de tarifas preferenciales a grupos poblacionales en condición de vulnerabilidad.

- **Factor Político[4]**

TRANSMILENIO S.A., contribuye al logro de los objetivos que la Administración Distrital establece para la ciudad de Bogotá D.C., bajo las condiciones que señalan las normas vigentes, las autoridades competentes, los Estatutos, el Plan de Desarrollo aplicable, las necesidades de los usuarios y partes interesadas, las funciones asignadas a la Entidad y los planes, programas y proyectos en los que este incursa.
TRANSMILENIO S.A. considera que uno de sus mayores diferenciadores, es la implementación de la estrategia de Gobierno Digital y del Sistema Gestión de Seguridad de la Información "SGSI" que promueve la confidencialidad, Integridad y Disponibilidad de la Información para los Clientes Internos (Servidores Públicos y/o Contratistas) y Externos (Entidades, usuarios, etc.).

- **Organismos de Vigilancia, Inspección y Control.**

En TRANSMILENIO S.A., sus procesos y activos de información están continuamente expuestos a revisiones por parte de los organismos de vigilancia, inspección y control; la entidad encuentra en el SGSI un mecanismo de control que le permite mantener la confidencialidad, integridad y sobre todo la disponibilidad de dichos activos para responder oportuna y eficazmente las solicitudes de los entes de control.

Entre las entidades de control y seguimiento se encuentran:

- Contraloría General de la Nación
- Oficina de Control Interno de la entidad.
- Oficina de control disciplinario de la entidad.
- Veeduría Distrital.
- Contraloría Distrital.
- Procuraduría General de la Nación.

[4] **Fuente**: Plan Estratégico Institucional 2015

- Contaduría General de la Nación.
- Personería Distrital.
- Departamento Administrativo de la Función Pública.

6.1.3 Análisis DOFA

Luego de identificar los actores internos y externos, a continuación, se presenta el análisis DOFA (debilidades, oportunidades, fortalezas y amenazas) identificado por la entidad con relación a la seguridad de la información.

Tabla 1. Análisis DOFA

	Componentes Internos		Componentes Externos	
	Fortalezas		Oportunidades	
Factor Positivo	F1.	Personal altamente calificado, rigurosidad técnica y con habilidades de liderazgo.	O1.	Aprender de los incidentes conocidos ocurridos en otras Entidades y Organizaciones.
	F2	Se tiene Compromiso de la Alta Dirección de TRANSMILENIO S.A en la seguridad de la información.	O2.	Mantener comunicación activa con Organismos o Entidades Externas frente a temas de Seguridad que permite ampliar el panorama y la visión para la Entidad.
	F3.	Se cuenta con el Sistema integrado de Gestión, que permite comunicar todos procesos y hacerlos parte integral del mismo.	O3.	Lograr que los objetivos de la Entidad se cumplan con un alto nivel de Seguridad en el manejo de la Información.
	F4.	TRANSMILENIO S.A, como Entidad Pública dispone de un marco normativo y regulatorio basado en las recomendaciones de las normas internacionales y normativas legales vigentes.	O4	Participar con Entidades Públicas distritales en pro de fortalecer la apropiación de la Cultura del SGSI.
	F5	Se cuenta con una sede principal arrendada en donde operan las oficinas Transmilenio y el Datacenter. Con condiciones físicas, ambientales y de seguridad.	O5	Transmilenio como entidad pública del orden territorial, debe implementar, de manera sistemática y coordinada, la Estrategia de Gobierno Digital de Mintic

	Componentes Internos		Componentes Externos	
	Debilidades		Amenazas	
Factor Negativo	D1.	La entidad debe fortalecer los programas de divulgación y sensibilización a los funcionarios y/o Contratistas, proveedores y terceros frente al SGSI.	A1.	Apropiarse de los cambios normativos y legislativos vigentes que afecten el SGSI.
	D2.	La entidad carece de seguimiento y monitoreo de los controles implementados para verificar la efectividad y eficacia de estos.	A2.	Mantenerse actualizado con las evoluciones tecnológicas.
	D3.	La entidad debe fortalecer el sistema de gestión de riesgos de seguridad de la información y el tratamiento de los mismos que afecten el SGSI.	A3.	Dar cumplimiento a los requisitos de Organismos de Vigilancia, Inspección y Control.
	D4.	Constante rotación del personal operativo en todos los procesos de la entidad.	A4.	Dar cumplimiento al Manual del SGSI y a las políticas de seguridad y privacidad de la información.
	D5	La entidad carece de uso y apropiación del SGSI.	A5	Ataques cibernéticos a las entidades públicas.

6.2 PARTES INTERESADAS

TRANSMILENIO S.A. reconoce como sus grupos de interés [5] a las partes interesadas que se presentan en la siguiente tabla:

Tabla 2. Partes Interesadas.

PARTE INTERESADA	DESCRIPCIÓN	NECESIDADES Y EXPECTATIVAS FRENTE A SEGURIDAD DE LA INFORMACION
Usuarios directos	Servidores públicos, oficiales, proveedores y los terceros autorizados.	Las partes interesadas esperan del TRANSMILENIO, un manejo responsable de la *información*, que, en el desarrollo de su objeto, ha sido suministrada, gestionada,

[5] Fuente: Manual del Sistema integrado de Gestión M-OP-001

PARTE INTERESADA	DESCRIPCIÓN	NECESIDADES Y EXPECTATIVAS FRENTE A SEGURIDAD DE LA INFORMACION
Usuarios Indirectos	Usuarios del sistema y la ciudadanía en general.	procesada, almacenada o transferida por la entidad. Adicionalmente las partes interesadas creen en que a través del establecimiento, implementación y mejora continua del SGSI, la entidad asegurará la integridad, disponibilidad y confidencialidad de la información, y el cumplimiento estricto de los requisitos legales, contractuales, regulatorios y normativos.
Entidades publicas	Alcaldía Mayor, Secretaria Distrital de Planeación, Secretaria Distrital de Movilidad, Instituto de desarrollo urbano, Ministerio de transporte.	
Terceros relacionados	Agentes del Sistema: Operadores troncales, operadores de alimentación, operadores zonales, operadores de recaudo, El Sistema Integrado de Recaudo, Control e Información y Atención al Usuario – SIRCI.	
Entidades externas	Entidades homologas de otros países y los organismos internacionales de referencia.	

7. MARCO CONCEPTUAL DEL PESI

Para TRANSMILENIO S.A., son muy importantes los resultados obtenidos en el PESI con el fin de apoyar la implementación del SGSI. El PESI se apoya en el Plan Estratégico Institucional el cual a su vez se fundamenta en la metodología del *Balanced Scorecard* o Cuadro de Mando Integral, debido a su gran utilidad en el direccionamiento de las organizaciones .

El *Balance Scorecard* es una herramienta útil en la Planeación Estratégica. Esta metodología tiene en cuenta las siguientes fases: revisión de misión, objetivos y estrategias, análisis de la propuesta de valor, recursos financieros, clientes, procesos, crecimiento y aprendizaje; reporte, revisión y comunicación de resultados, cambio y mejoramiento de las Estrategias laborales de cada miembro de la Institución, actualización y adaptación permanente frente a cambios internos y externos del entorno. Asimismo, los

objetivos y metas son evaluables y medibles, generando sus propios indicadores, que deberán ser utilizados como herramienta para el seguimiento, control, evaluación y gestión de la entidad [6].

8. METODOLOGIA UTILIZADA

La metodología utilizada para el desarrollo del PESI se muestra y se explica a continuación:

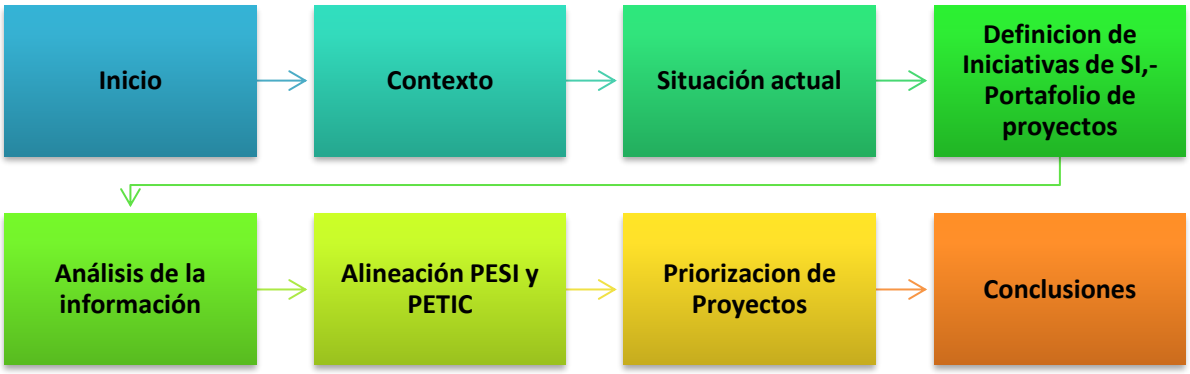

Ilustración 5. Metodología Utilizada

8.1 CONTEXTO

En esta fase inicial del desarrollo del PESI, se busca entender las características principales de la entidad con el fin de que los objetivos de este Plan estén alineados con los objetivos estratégicos de la entidad. Entre los aspectos que se deben considerar para lograr este entendimiento están:

1. La misión
2. La visión
3. Historia y antecedentes
4. Estructura organizacional
5. Procesos

[6] Plan Estratégico Institucional 2015.

6. Cultura y valores
7. Legislación pertinente

8.2 SITUACIÓN ACTUAL

Por situación actual se entiende el nivel de madurez que posee en este momento TRANSMILENIO S.A. con relación a la seguridad de la información. El proceso por el cual se lleva a cabo esta estimación del nivel de madurez se denomina Instrumento de diagnóstico del MSPI de Mintic (Análisis GAP). Para poder realizar el PESI es indispensable que se tenga en cuenta los niveles de madurez alcanzados por cada uno de los dominios (ver figura a continuación) con el fin de plantear prioridades sobre su implementación.

Tabla 3. Dominios

Dominio ISO 27001	Objetivo de control
Política de seguridad de la información.	Objetivo de control A.5
Organización de la seguridad de la información.	Objetivo de control A.6
Seguridad de los RRHH.	Objetivo de control A.7
Gestión de activos.	Objetivo de control A.8
Control de accesos.	Objetivo de control A.9
Criptografía.	Objetivo de control A.10
Seguridad física y del entorno	Objetivo de control A.11
Seguridad en las operaciones.	Objetivo de control A.12
Seguridad en las comunicaciones.	Objetivo de control A.13
Adquisición de sistemas, desarrollo y mantenimiento.	Objetivo de control A.14
Relación con proveedores.	Objetivo de control A.15
Gestión de los incidentes de seguridad de la información	Objetivo de control A.16
Aspectos de seguridad de la información en la Continuidad del negocio.	Objetivo de control A.17
Cumplimiento con requerimientos legales y contractuales.	Objetivo de control A.18

La metodología utilizada para realizar el GAP se presenta a continuación:

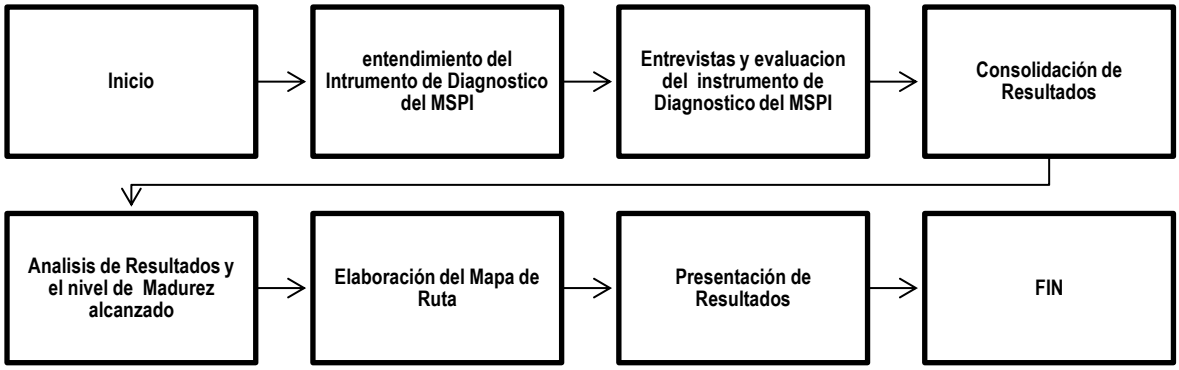

Ilustración 6. Metodologia utilizada en el GAP

El nivel de madurez permite establecer las bases para la mejora continua del proceso de Seguridad de la Información de TRANSMILENIO S.A., e identificar las iniciativas en la materia, las cuales deben estar alineadas a las necesidades que se identificaron en Plan Estratégico de Tecnologías de Información y Comunicaciones y la estrategia de información (PETI).

En seguida, se presenta el nivel de madurez del modelo de seguridad y privacidad de la información y el porcentaje de cumplimiento de la Entidad frente a los 14 dominios de la norma ISO/IEC 27001:2013 y ISO/IEC 27002:2013.

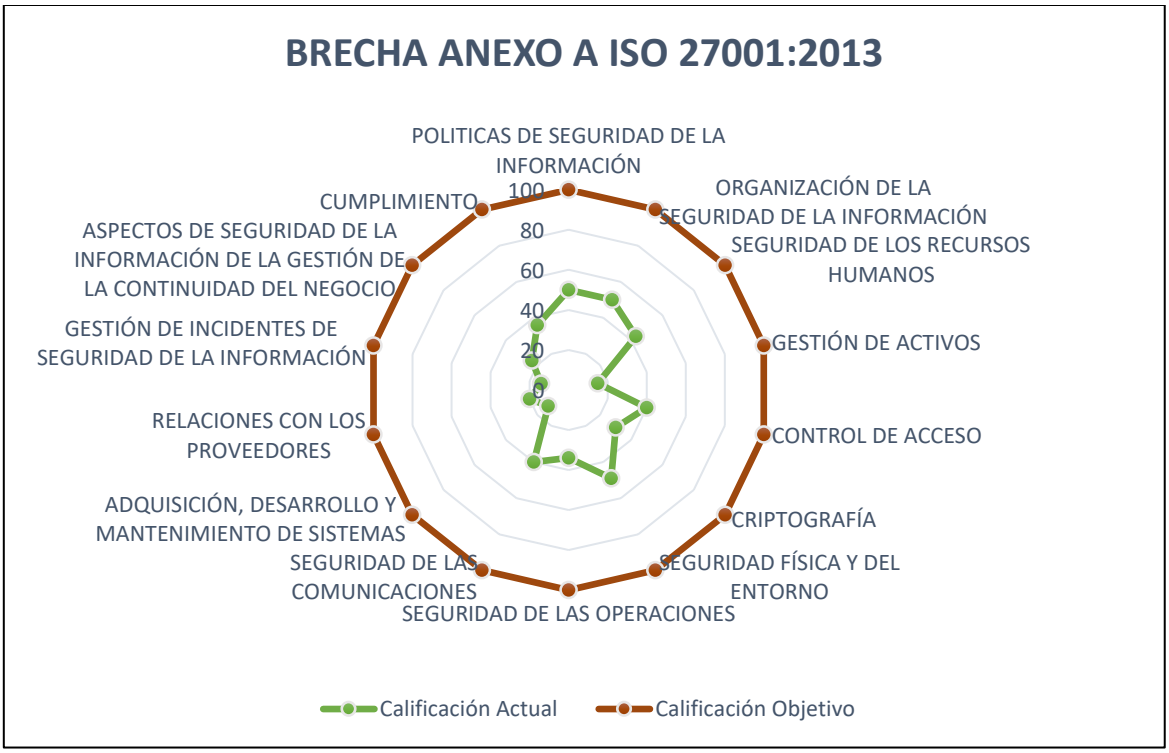

Ilustración 7. Diagrama tipo radar por Dominio

Analizando el gráfico, se puede observar que el dominio con mayor nivel de madurez es el *A.5 Política de seguridad de la información* (Efectivo), A.6 Organización de la Seguridad de la información, seguridad de los recursos humanos (Efectivo), A.11 Seguridad física (Efectivo), y los demás dominios se encuentran por debajo del 40 % que corresponde a un estado repetible e inicial.

En conclusión, el nivel de madurez alcanzado por TRANSMILENIO S.A. está en **33%**, lo que significa que la compañía está en nivel Repetible, los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.

A continuación se presenta la evaluación de efectividad de controles.

Tabla 4. Resultados por Dominio

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	50	100	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	50	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	43	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	15	100	INICIAL
A.9	CONTROL DE ACCESO	40	100	REPETIBLE
A.10	CRIPTOGRAFÍA	30	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	49	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	34	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	40	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	13	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	20	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	14	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	24	100	REPETIBLE
A.18	CUMPLIMIENTO	36	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		33	100	REPETIBLE

Nivel de cumplimiento general – ISO 27001:2013

Con base en los resultados obtenidos a continuación, se presentan los resultados generales de cumplimiento de la norma ISO 27001:2013.

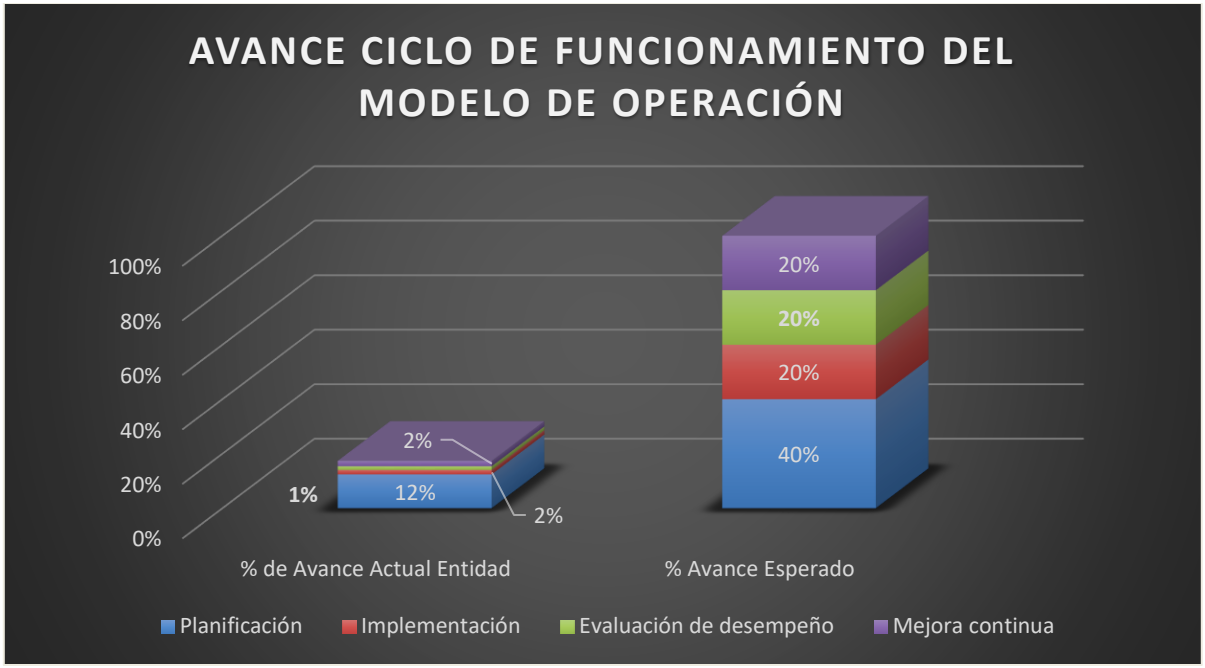

Ilustración 8. Resultado grafico del cumplimiento ISO 27001:2013 PHVA

Se puede concluir que se observan importante oportunidad de mejora, con respecto a la norma internacional ISO/IEC 27001:2013 se obtuvo un puntaje de cumplimiento del **17%**, y para la efectividad de los controles de seguridad 27002:2013 se obtuvo un **33%.** Por lo anterior, es perentorio que el portafolio de proyectos de seguridad de la información debe incluir un proyecto que permita el fortalecimiento y mejoramiento del sistema de gestión de seguridad de la información para TRANSMILENIO S.A.

8.3 ANALISIS Y PRIORIZACION DE INICIATIVAS DE SEGURIDAD DE LA INFORMACION

Teniendo en cuenta el resultado anterior, se identifican las iniciativas de seguridad de la información, los cuales deben estar alineadas al plan estratégico de TRANSMILENIO S.A., y los resultados de la calificación actual del instrumento de diagnóstico del Modelo de seguridad y privacidad de la información. De otra parte, es importante que las iniciativas estén enmarcadas dentro de los controles sugeridos para garantizar una adecuada arquitectura de seguridad de la información y un esquema de defensa a profundidad utilizando soluciones y tendencias de seguridad de la información y de tecnología. Estas

iniciativas fueron seleccionadas de acuerdo con el nivel de madurez de cada Dominio teniendo como referencia la calificación actual obtenida menor al 60 % de efectividad:

Tabla 5. Iniciativas de Seguridad de la información versus objetivos estratégicos de Seguridad de la Información

INICIATIVAS	DESCRIPCION DE LAS INICIATIVAS	ESTRATEGIA SEGURIDAD DE LA INFORMACIÓN OBJETIVOS DE SEGURIDAD			
		Gobierno o Modelo de seguridad de información	Gestión de riesgos de Seguridad	Desarrollo y gestión del programa de seguridad de la información.	Gestión de incidentes de seguridad de la información.
I.00	Actualizar el manual de políticas de seguridad y privacidad de la información, e incluir en el plan de cultura 2018 la divulgación de estas.	X			
I.01	Elaborar el plan estratégico de seguridad de la información	X			
I.02	Definir e integrar la seguridad de la información en el ciclo de vida de los proyectos para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto.	X			
I.03	Diseñar y documentar un plan anual de cultura y sensibilización en seguridad de la información para empleados, proveedores y terceros de TRANSMILENIO.	X			
I.04	Implementar un plan anual de cultura y sensibilización en seguridad de la información para empleados, proveedores y terceros de TRANSMILENIO.	X			

INICIATIVAS	DESCRIPCION DE LAS INICIATIVAS	ESTRATEGIA SEGURIDAD DE LA INFORMACIÓN OBJETIVOS DE SEGURIDAD			
		Gobierno o Modelo de seguridad de información	Gestión de riesgos de Seguridad	Desarrollo y gestión del programa de seguridad de la información.	Gestión de incidentes de seguridad de la información.
I.05	Definir y adoptar una política y unas medidas de seguridad de la información, para gestionar los riesgos introducidos por el uso de dispositivos móviles y el teletrabajo.			X	
I.06	Realizar inventario de los activos de información de cada uno de los procesos de la entidad y realizar su valoración y clasificación según la criticidad para la compañía.			X	
I.07	Identificar los riesgos de seguridad de la información para cada uno de los procesos.		X		
I.08	Gestionar el Tratamiento de riesgos de seguridad de la información de los riesgos identificados en cada uno de los procesos.		X		
I.09	Diseñar y documentar el programa de ejercicios al plan de recuperación ante desastres, ante escenarios de fallas de las tecnologías, garantizando que se mantengan los controles de seguridad.	X			
I.10	Ejecutar el programa de ejercicios al plan de recuperación ante desastres, ante escenarios de fallas de las tecnologías, garantizando que se mantengan los controles de seguridad			X	
I.11	Documentar los esquemas de arquitecturas redundantes en dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core, servidores y almacenamiento.			X	

INICIATIVAS	DESCRIPCION DE LAS INICIATIVAS	ESTRATEGIA SEGURIDAD DE LA INFORMACIÓN OBJETIVOS DE SEGURIDAD			
		Gobierno o Modelo de seguridad de información	Gestión de riesgos de Seguridad	Desarrollo y gestión del programa de seguridad de la información.	Gestión de incidentes de seguridad de la información.
I.12	Definir y establecer un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, en el cual se establezcan controles para proteger la confidencialidad de la información.			X	
I.13	Definir y establecer la metodología de desarrollo seguro			X	
I.14	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.			X	
I.15	Monitorear el cumplimiento del ciclo de vida de gestión de usuarios (creación, modificación, activación, desactivación, eliminación, entre otros) verificando que se cumple para todas las aplicaciones.			X	
I.16	Definir e implementar una política sobre el uso de controles criptográficos para la protección de la información en la organización.			X	
I.17	Monitorear a los terceros periódicamente para verificar que los controles de seguridad, los acuerdos de servicio definidos y demás requerimientos de seguridad que se contrataron están siendo implementados, operados y mantenidos.				X

INICIATIVAS	DESCRIPCION DE LAS INICIATIVAS	ESTRATEGIA SEGURIDAD DE LA INFORMACIÓN OBJETIVOS DE SEGURIDAD			
		Gobierno o Modelo de seguridad de información	Gestión de riesgos de Seguridad	Desarrollo y gestión del programa de seguridad de la información.	Gestión de incidentes de seguridad de la información.
I.18	Implementar la gestión centralizada de usuarios para todos los aplicativos del negocio.			X	
I.19	Implementar una solución de gestión de identidades para usuarios privilegiados			X	
I.20	Implementar una solución como servicio de borrado seguro de información			X	
I.21	Implementar como servicio una solución de anti malware avanzado para la protección contra amenazas avanzadas persistentes (APT).			X	
I.22	Establecer e implementar pruebas, análisis y gestión de vulnerabilidades a los elementos de mayor criticidad tanto a nivel de infraestructura como a nivel de aplicaciones web.			X	
I.23	Establecer e implementar pruebas de Hacking Ético sobre los aplicativos críticos.			X	
I.24	Implementar una solución que permite la transferencia segura de archivos, mediante protocolos de cifrado.			X	
I.25	Implementar una solución de DLP (Data Loss Prevention), con el fin de controlar y monitorear el intercambio de información confidencial y/o sensible.			X	
I.26	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web			X	

INICIATIVAS	DESCRIPCION DE LAS INICIATIVAS	ESTRATEGIA SEGURIDAD DE LA INFORMACIÓN OBJETIVOS DE SEGURIDAD			
		Gobierno o Modelo de seguridad de información	Gestión de riesgos de Seguridad	Desarrollo y gestión del programa de seguridad de la información.	Gestión de incidentes de seguridad de la información.
I.27	Implementar un correlacionador de eventos (SIEM) como servicios para monitorear el comportamiento de activos de información críticos.			X	
I.28	Operar y mantener el sistema de gestión de seguridad de la información SGSI, incluyendo todos los procesos de la compañía.			X	
I.29	Asegurar el uso y adaptación e entornos de computación en la nube			X	
I.30	Implementar y monitorear los indicadores del sistema de gestión de seguridad de la información				X
I.31	Entrenamiento a los equipos de recuperación de los procesos críticos del negocio	X			

8.4 DEFINICIÓN DEL PORTAFOLIO DE PROYECTOS DE SEGURIDAD DE LA INFORMACIÓN

En esta etapa, después del análisis y priorización de iniciativas, se define el portafolio de proyectos del plan estratégico PESI, agrupados en proyectos relacionados con:

- ✓ Gobierno o modelo de seguridad de información.
- ✓ Gestión de riesgos de Seguridad.
- ✓ Desarrollo y gestión del plan de seguridad de la información.
- ✓ Gestión de incidentes de seguridad de la información.

Tabla 6. Portafolio de proyectos SI

PROYECTOS DE SEGURIDAD DE LA INFORMACION (SI)					
No. PROYECTO	**DESCRIPCION DEL PROYECTO**	**INICIATIVA**	**DESCRIPCION DE INICIATIVAS**	**ESTADO**	**RECURSOS FINANCIEROS**
P01	Definición y elaboración del plan estratégico de seguridad de la información.	I.01	Elaborar el plan estratégico de seguridad de la información	Proceso	SI
P.02	Integrar los componentes del sistema de gestión de seguridad de la información en el ciclo de vida de los proyectos de Transmilenio S.A	I.02	Definir e integrar la seguridad de la información en el ciclo de vida de los proyectos para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto.	No Iniciado	NO
P.03	Desarrollar el Plan de cultura y sensibilización en seguridad de la información para empleados, contratistas proveedores y terceros.	I.03	Diseñar y documentar un plan anual de cultura y sensibilización en seguridad de la información para empleados, proveedores y terceros de TRANSMILENIO.	Proceso	NO
		I.04	Implementar un plan anual de cultura y sensibilización en seguridad de la información para empleados, proveedores y terceros de TRANSMILENIO.	No Iniciado	SI
P.04	Sistema de control de acceso para dispositivos móviles y Implementación VPN'S en Teletrabajo.	I.05	Definir y adoptar una política y unas medidas de seguridad de la información, para gestionar los riesgos introducidos por el uso de dispositivos móviles y el teletrabajo.	No Iniciado	SI
P.05	Gestión de activos de información para todos los procesos de la entidad.	I.06	Realizar inventario de los activos de información de cada uno de los procesos de la entidad y realizar su valoración y clasificación según la criticidad para la compañía.	No Iniciado	SI
P.06	Gestión y tratamiento de los Riesgos de Seguridad	I.07	Identificar los riesgos de seguridad de la información para cada uno de los procesos.	Iniciado	SI

PROYECTOS DE SEGURIDAD DE LA INFORMACION (SI)					
No. PROYECTO	DESCRIPCION DEL PROYECTO	INICIATIVA	DESCRIPCION DE INICIATIVAS	ESTADO	RECURSOS FINANCIEROS
	de la información para todos los procesos de la entidad.	I.08	Gestionar el Tratamiento de riesgos de seguridad de la información de los riesgos identificados en cada uno de los procesos.	No Iniciado	SI
P.07	Desarrollo y Gestión del programa de continuidad del Negocio.	I.09	Diseñar y documentar el programa de ejercicios al plan de recuperación ante desastres, ante escenarios de fallas de las tecnologías, garantizando que se mantengan los controles de seguridad.	No Iniciado	SI
		I.10	Ejecutar el programa de ejercicios al plan de recuperación ante desastres, ante escenarios de fallas de las tecnologías, garantizando que se mantengan los controles de seguridad	No Iniciado	SI
P.08	Actualizar los esquemas de arquitecturas redundantes en dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core, servidores y almacenamiento.	I.11	Documentar los esquemas de arquitecturas redundantes en dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core, servidores y almacenamiento.	No Iniciado	NO
P.09	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.12	Definir y establecer un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, en el cual se establezcan controles para proteger la confidencialidad de la información.	No Iniciado	NO
P.10	Adaptación de metodología para el desarrollo Seguro en las aplicaciones.	I.13	Definir y establecer la metodología de desarrollo seguro	No Iniciado	NO

PROYECTOS DE SEGURIDAD DE LA INFORMACION (SI)					
No. PROYECTO	DESCRIPCION DEL PROYECTO	INICIATIVA	DESCRIPCION DE INICIATIVAS	ESTADO	RECURSOS FINANCIEROS
P.11	Gestión de accesos y privilegios de TI	I.14	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.	Iniciado	NO
		I.15	Monitorear el cumplimiento del ciclo de vida de gestión de usuarios (creación, modificación, activación, desactivación, eliminación, entre otros) verificando que se cumple para todas las aplicaciones.	Iniciado	NO
P.09	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.16	Definir e implementar una política sobre el uso de controles criptográficos para la protección de la información en la organización.	Iniciado	NO
P.12	Evaluación y desempeño del sistema de Gestión de seguridad de la información	I.17	Monitorear a los terceros periódicamente para verificar que los controles de seguridad, los acuerdos de servicio definidos y demás requerimientos de seguridad que se contrataron están siendo implementados, operados y mantenidos.	No Iniciado	NO
P.11	Gestión de accesos y privilegios de TI	I.18	Implementar la gestión centralizada de usuarios para todos los aplicativos del negocio.	No Iniciado	NO
P.13	Gestión de herramienta para cuentas privilegiadas	I.19	Implementar una solución de gestión de identidades para usuarios privilegiados	No Iniciado	SI
P.14	Implementación de Software para	I.20	Implementar una solución como servicio de borrado seguro de información	No Iniciado	SI

PROYECTOS DE SEGURIDAD DE LA INFORMACION (SI)					
No. PROYECTO	DESCRIPCION DEL PROYECTO	INICIATIVA	DESCRIPCION DE INICIATIVAS	ESTADO	RECURSOS FINANCIEROS
	borrado seguro de Información				
P.09	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.21	Implementar como servicio una solución de anti malware avanzado para la protección contra amenazas avanzadas persistentes (APT).	Proceso	SI
P.15	Adquisición de Software o servicio de análisis de vulnerabilidades y hacking Ético	I.22	Establecer e implementar pruebas, análisis y gestión de vulnerabilidades a los elementos de mayor criticidad tanto a nivel de infraestructura como a nivel de aplicaciones web.	No Iniciado	SI
		I.23	Establecer e implementar pruebas de Hacking Ético sobre los aplicativos críticos.		
P.16	Herramientas de cifrado de información automatizados, Repositorio centralizado de información cifrada.	I.24	Implementar una solución que permite la transferencia segura de archivos, mediante protocolos de cifrado.	No Iniciado	SI
P.17	Gestionar una solución de DLP (Data Loss Prevention) para el correo Electrónico y equipos críticos.	I.25	Implementar una solución de DLP (Data Loss Prevention), con el fin de controlar y monitorear el intercambio de información confidencial y/o sensible.	No Iniciado	SI
P.18	Gestionar una herramienta WAF para la protección de las aplicaciones WEB de TRANSMILENIO S.A	I.26	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web	No Iniciado	SI
P.19	Gestionar una solución de correlacionador de eventos (SIEM) como servicio, para monitorear el	I.27	Implementar un correlacionador de eventos (SIEM) como servicios para monitorear el comportamiento de activos de información	No Iniciado	SI

PROYECTOS DE SEGURIDAD DE LA INFORMACION (SI)					
No. PROYECTO	DESCRIPCION DEL PROYECTO	INICIATIVA	DESCRIPCION DE INICIATIVAS	ESTADO	RECURSOS FINANCIEROS
	comportamiento de activos de información críticos.		críticos.		
P.09	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información, incluyendo todos los procesos de la compañía.	I.28	Operar y mantener el sistema de gestión de seguridad de la información SGSI, incluyendo todos los procesos de la compañía.	No Iniciado	SI
P.09	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.29	Asegurar el uso y adaptación e entornos de computación en la nube	No Iniciado	SI
P.12	Evaluación y desempeño del sistema de Gestión de seguridad de la información	I.30	Implementar y monitorear los indicadores del sistema de gestión de seguridad de la información	Iniciado	NO
P.07	Desarrollo y Gestión del programa de continuidad del Negocio.	I.31	Entrenamiento a los equipos de recuperación de los procesos críticos del negocio	No Iniciado	SI

9. ALINEACIÓN PESI Y PETIC

La alineación del PESI y PETIC busca sincronizar los objetivos estratégicos de TI (PETIC), los cuales definen lineamientos para el mejoramiento del nivel de madurez institucional en la implementación de soluciones tecnológicas que generen valor y promuevan el cumplimiento de la misión con sostenibilidad tecnológica. Así mismo el PESI define objetivos que permiten asegurar la confidencialidad, integridad y disponibilidad de los activos de información. para ello se establecen los objetivos de TI que están directamente involucrados en el plan estratégico de seguridad de la información.

Tabla 7. Objetivos PETIC.

Objetivo PETI	Objetivo
1.	Alinear la estrategia de TI con la estrategia de TRANSMILENIO y del sector movilidad, así como del Gobierno Nacional
2.	Maximizar el aporte de las TIC a los procesos internos para la transformación de TRANSMILENIO.
3.	Ejercer el Gobierno de las TIC de TRANSMILENIO.
4.	Posicionarse como aliado estratégico de todos los procesos internos de TRANSMILENIO.
5.	Mejorar la satisfacción de los usuarios, así como la del ciudadano que utiliza los servicios de TRANSMILENIO.
6.	Proveer información oportuna y de calidad para la toma de decisiones en los procesos internos de TRANSMILENIO.
7.	Entregar oportunamente sistemas de información de calidad, funcionales, eficientes y confiables fortaleciendo los procesos internos de TRANSMILENIO.
8.	Fortalecer la Gestión de las TIC y de la seguridad de la información en los procesos internos de la entidad.
9.	Fortalecer las competencias y desarrollo profesional del equipo de TI de TRANSMILENIO.
10.	Desarrollar la capacidad de innovación y prospectiva tecnológica.

.

De los anteriores objetivos del PETI el número 8 y 9 están relacionados con el sistema de gestión de seguridad de la información.

Tabla 8. Alineación de objetivos del PESI con los objetivos PETIC.

Dominio	Objetivo del PESI	# de objetivo del PETIC	Estado Actual	Nivel
A.5. Políticas de la seguridad de la información	La adopción de políticas de seguridad de la información debe obedecer a una decisión estratégica, las cuales servirán de directrices para proteger la información de propiedad del ICA.	8	**50%**	**EFECTIVO**
A.6. Organización de la seguridad de la información	La definición de los roles y responsabilidades para la seguridad de la información es el aspecto fundamental para iniciar y controlar la implementación y la operación de lo relacionado con la protección de la información propiedad del ICA.	8	**50%**	**EFECTIVO**

Dominio	Objetivo del PESI	# de objetivo del PETIC	Estado Actual	Nivel
A.7. Seguridad de los recursos humanos	Las personas son el componente más importante en todo el modelo de seguridad de la información, por lo tanto, antes de su contratación, durante su permanencia y en el proceso de finalización o cambios de cargo, la entidad debe asegurar que los funcionarios y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	8 y 9	**43%**	**EFECTIVO**
A.8. Gestión de activos	Identificar los activos de información y definir las responsabilidades de protección apropiadas, asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización y evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios; son las principales razones de la entidad para garantizar la gestión adecuada de los activos y la asignación de las respectivas responsabilidades sobre los mismos.	8 y 9	**15%**	**INICIAL**
A.9. Control de acceso	Las técnicas de control de acceso permiten proteger la información en términos de la confidencialidad, la integridad y la disponibilidad.	8	**40%**	**REPETIBLE**
A.10. Criptografía	Las técnicas de cifrado ayudan a proteger la información de acuerdo a su nivel de clasificación, la implementación de éstas, el uso apropiado y eficaz de la criptografía permiten proteger la confidencialidad, la autenticidad y/o la integridad de la información propiedad de la entidad.	8	**30%**	**REPETIBLE**
A.11. Seguridad física y del entorno	La debida protección de los centros de datos, archivos documentales, equipos, oficinas, entre otros, es un aspecto que se debe considerar cuando se trate de la seguridad de la información.	8	**49%**	**EFECTIVO**
A.12. Seguridad de las operaciones	Lograr que las operaciones protejan la información debe ser un compromiso de la entidad.	8	**34%**	**REPETIBLE**
A.13. Seguridad de las comunicaciones	La transferencia de información está expuesta a múltiples riesgos, por ello la entidad debe implementar medidas preventivas para evitar su divulgación o modificación.	8	**40%**	**REPETIBLE**
A.14. Adquisición, desarrollo y mantenimiento de sistemas	Mantener la seguridad de la información durante el ciclo de desarrollo requiere contar con una metodología de desarrollo seguro. Las aplicaciones normalmente mantienen información importante de la entidad, por esta razón se deben implementar controles de seguridad dentro de ellas.	8 y 9	**13%**	**INICIAL**
A.15. Relación con los Proveedores	Asegurar la protección de los activos de la entidad que sean accesibles para los proveedores y terceros y mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores	8 y 9	**20%**	**INICIAL**

Dominio	Objetivo del PESI	# de objetivo del PETIC	Estado Actual	Nivel
A.16. Gestión de incidentes de seguridad de la información	La adecuada gestión de los incidentes de seguridad de la información permite proteger los tres pilares de la seguridad: la confidencialidad, la integridad y la disponibilidad de la información. La implementación de estos controles permite asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.	8 y 9	**14%**	**INICIAL**
A.17. Aspectos de seguridad de la información de la gestión de continuidad de negocio	Poder contar con planes para la continuidad del negocio y la recuperación ante desastres es importante para preservar la disponibilidad de la información. La entidad debe adoptar estos controles para asegurar la disponibilidad de las instalaciones de procesamiento de información durante una situación adversa, adicionalmente debe verificar a intervalos regulares dichos controles con el fin de asegurar que son válidos y eficaces.	8 y 9	**24%**	**REPETIBLE**
A.18. Cumplimiento	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad es importante para no incurrir en demandas, multas u otra clase de afectación a la imagen o a las finanzas de la entidad.	8	**36%**	**REPETIBLE**

10. INFORME DE RESULTADOS

10.1 PRIORIZACION DEL PORTAFOLIO DE PROYECTOS

Una vez identificadas las iniciativas y los proyectos con base en el resultado de diagnóstico de la situación actual del instrumento del MSPI de Mintic, es necesario priorizar los proyectos, para lo cual se tuvo en cuenta la estrategia de seguridad de la información (Gobierno o Modelo de seguridad de información, gestión de riesgos de Seguridad, Desarrollo y gestión del programa de seguridad de la información y Gestión de incidentes de seguridad de la información). Para ello se construyeron las siguientes categorías de prioridad que permiten evaluar y determinar una secuencia sistemática para el desarrollo del Plan Estratégico de Seguridad de la Información (PESI):

Tabla 9. Criterios para priorización de proyectos.

PRIORIDAD	
PRIORIDAD	**DESCRIPCION**
0	Elaboración del presente Plan Estratégico de Seguridad de la Información.
1	Gobierno o Modelo de seguridad de información, el cual Incluye las iniciativas que soportan el desarrollo del modelo de seguridad de la informacion .
2	Gestion de Riesgos Operacionales: Hace referencia a los proyectos y actividades que mitigan los riesgos de seguridad de la información catalogados como relevantes, garantizando salvaguardar la información en su confidencialidad, disponibilidad e integridad.
3	Desarrollo y gestión del programa de seguridad de la información; hace refencia aquellos proyectos que permiten la Operación y mantenimiento del Sistema de Gestión de Seguridad de la información .
4	Desempeño: Soportan aquellos proyectos que permiten la evaluacion del desempeño y mejora continua del SGSI.

A continuación, se presenta por prioridad los proyectos que se deben desarrollar a partir de la vigencia 2018 y hasta la vigencia 2021.

Tabla 10. Prioridad de Proyectos año 2018- año 2021

No. PROYECTO	NOMBRE DEL PROYECTO	PRIORIDADES				
		0	1	2	3	4
		Año 2018 PESI	Año 2018 Gobierno o Modelo de seguridad de Información	Año 2018-2019 Gestión de Riesgos Operacionales	Año 2019-2020 Desarrollo y gestión del PESI	Año 2021 Desempeño y mejora continua del SGSI.
P.00	Desarrollar e implementar las políticas de seguridad y privacidad de la información para Transmilenio		**X**			
P.01	Definición y elaboración del plan estratégico de seguridad de la información.	**X**				
P.02	Integrar los componentes del sistema de gestión de seguridad de		**X**			

No. PROYECTO	NOMBRE DEL PROYECTO	PRIORIDADES				
		0	1	2	3	4
		Año 2018 PESI	Año 2018 Gobierno o Modelo de seguridad de Información	Año 2018-2019 Gestión de Riesgos Operacionales	Año 2019-2020 Desarrollo y gestión del PESI	Año 2021 Desempeño y mejora continua del SGSI.
	la información en el ciclo de vida de los proyectos de Transmilenio S.A.					
P.03	Desarrollar el Plan de cultura y sensibilización en seguridad de la información para empleados, contratistas proveedores y terceros.		**X**			
P.04	Sistema de control de acceso para dispositivos móviles y Implementación VPN'S en Teletrabajo.				**X**	
P.05	Gestión de activos de información para todos los procesos de la entidad.			**X**	**X**	
P.06	Gestión y tratamiento de los Riesgos de Seguridad de la información para todos los procesos de la entidad.			**X**		
P.07	Desarrollo y Gestión del programa de continuidad del Negocio.				**X**	**X**
P.08	Actualizar los esquemas de arquitecturas redundantes en dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core, servidores y almacenamiento.				**X**	
P.09	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información				**X**	**X**
P.10	Adaptación de metodología para el desarrollo Seguro en las aplicaciones.				**X**	
P.11	Gestión de accesos y privilegios de TI				**X**	

No. PROYECTO	NOMBRE DEL PROYECTO	PRIORIDADES				
		0	1	2	3	4
		Año 2018 PESI	Año 2018 Gobierno o Modelo de seguridad de Información	Año 2018-2019 Gestión de Riesgos Operacionales	Año 2019-2020 Desarrollo y gestión del PESI	Año 2021 Desempeño y mejora continua del SGSI.
P.12	Evaluación y desempeño del sistema de Gestión de seguridad de la información			**X**	**X**	
P.13	Gestión de herramienta para cuentas privilegiadas				**X**	
P.14	Implementación de Software para borrado seguro de Información			**X**		
P.15	Adquisición de Software o servicio de análisis de vulnerabilidades y hacking Ético		**X**	**X**		
P.16	Herramientas de cifrado de información automatizados, Repositorio centralizado de información cifrada.				**X**	
P.17	Gestionar una solución de DLP (Data Loss Prevention) para el correo Electrónico y equipos críticos.				**X**	
P.18	Gestionar una herramienta WAF para la protección de las aplicaciones WEB de TRANSMILENIO S.A				**X**	
P.19	Gestionar una solución de correlacionador de eventos (SIEM) como servicio, para monitorear el comportamiento de activos de información críticos.				**X**	**X**

11. PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

El plan estratégico corresponde a la ejecución de los proyectos definidos en el portafolio de proyectos de seguridad de la información que aportan al cumplimiento de los objetivos de seguridad de la información y al plan estratégico TIC (PETI).

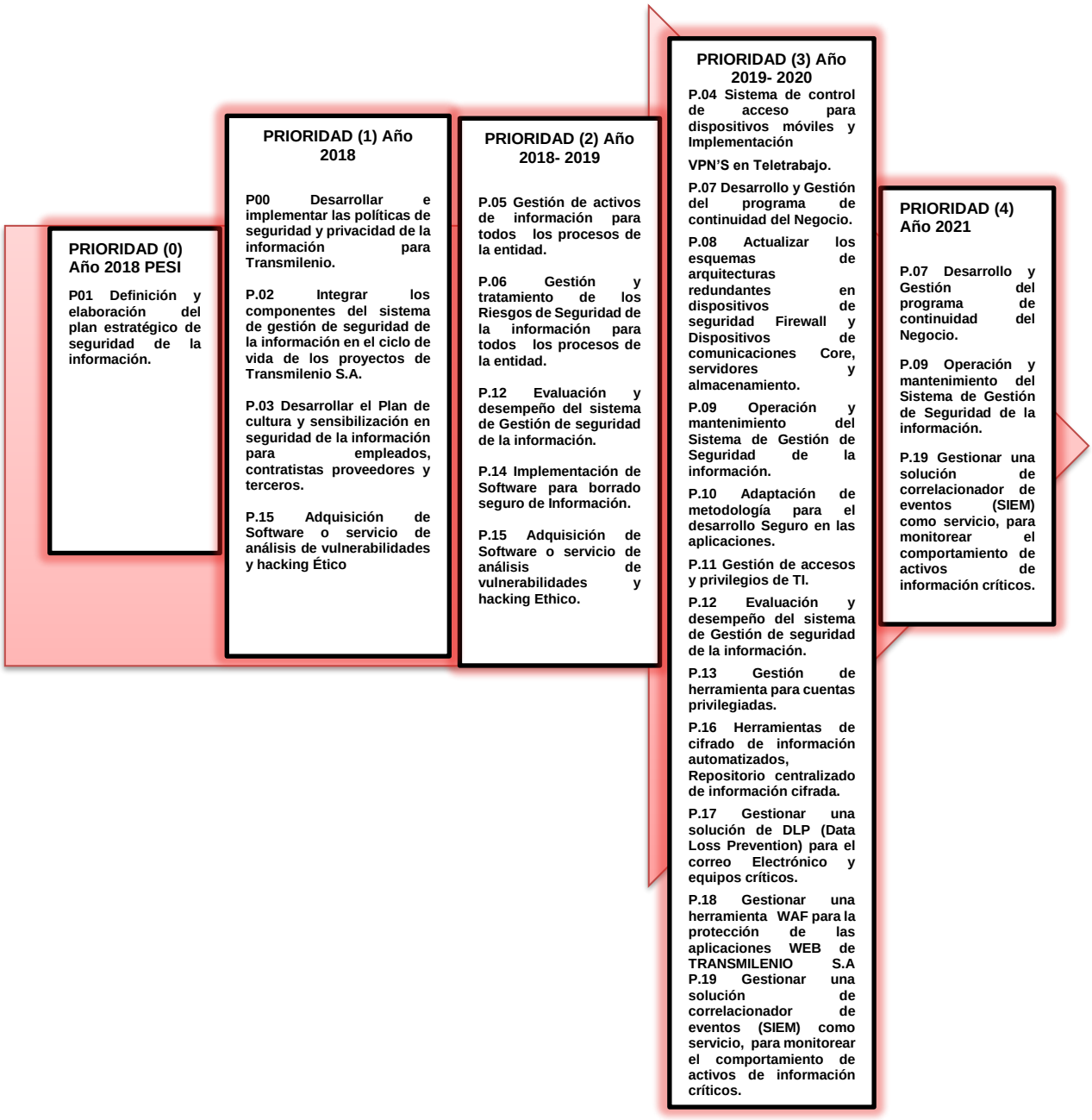

Ilustración 9. Plan Estratégico de Seguridad de la Información - PESI

12. CONCLUSIONES

El diseño de un Plan Estratégico para la Gestión de Seguridad de la Información - PESI - basado en el modelo de mejores prácticas y lineamientos de seguridad, basado en la Norma internacional ISO/IEC 27001:2013 y la ISO/IEC 27002:2013, y el alineamiento del plan estratégico de TRANSMILENIO S.A. es una herramienta de gran ayuda que permite identificar los diferentes proyectos de seguridad de la información que debe adelantar la Entidad de manera que permita cumplir y mantener el Sistema de Gestión de Seguridad de la Información y el modelo de seguridad y privacidad de la información.

Para lograr lo antes expuesto, es importante contar con el apoyo y la aprobación de la Alta Dirección de TRANSMILENIO S.A. y con el compromiso de todas las áreas involucradas en el proceso.

El portafolio de proyectos que tendrá el plan estratégico debe ser desarrollados y ejecutados para lograr un sistema de seguridad de la información conforme a los más altos estándares de seguridad, cumpliendo los requisitos y temas regulatorios en concordancia con los objetivos estratégicos de la Entidad.