TABLA DE CONTENIDO

INTRODUCCIÓN....3
1. OBJETO....4
2. ALCANCE DEL DOCUMENTO....4
3. RESPONSABLES DEL MANUAL....4
4. DOCUMENTOS DE REFERENCIA....4
5. DEFINICIONES....5
6. SISTEMA DE GESTION EN SEGURIDAD DE LA INFORMACIÓN (SGSI)....9
6.1 Contexto de la Entidad....9
6.1.1 Misión y Visión....11
6.2 Contexto Interno y Externo....11
6.2.1 Contexto Interno....12
6.2.2 Contexto Externo....15
6.2.3 Análisis DOFA....19
6.3 Partes Interesadas....19
6.4 Modelo del Sistema de Seguridad de la Información....20
6.4.1 Estructura del Modelo....20
6.4.2 Componentes del SGSI....22
7. POLITICA DE ALTO NIVEL DEL SGSI....25
8. OBJETIVOS DE SEGURIDAD DE LA INFORMACION....26
9. ALCANCE DEL SGSI....27
10. GESTIÓN DE RIESGOS....27
11. DECLARACION DE APLICABILIDAD....28
12. ORGANIZACIÓN DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION)....29
12.1 Estructura organizacional de seguridad de la información....29
12.2 Roles de seguridad de la información....35
12.3 Responsabilidades frente al SGSI....37
12.3.1 Dirección de TIC....37
12.3.2 Dependencias de la entidad....39

13. CULTURA Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN 39
14. MANTENIMIENTO Y MEJORA DEL SGSI 40
14.1 Medición de la eficacia del SGSI.....40
14.2 Auditoria Interna 41
14.3 Revisión por la Dirección.....41
14.4 Mejora del SGSI 41

INTRODUCCIÓN

La definición e implementación del Sistema de Gestión de Seguridad de la Información (SGSI), políticas, y procedimientos de seguridad de la información en TRANSMILENIO S.A, obedece a una decisión estratégica que cumple con la Política de Gobierno Digital en Colombia y el Modelo de Seguridad y Privacidad de la Información (MSPI) que está siendo implementado de manera sistemática y coordinada en todas las entidades del sector público.

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.

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.

Por lo tanto, la entidad asumió el reto de implementar el SGSI, siguiendo los lineamientos del MSPI de la Política 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.

Como complemento a lo anterior, la entidad ha adoptado los lineamientos normativos de: la ISO/IEC 27001:2013, la cual establece los requisitos para la implementación del SGSI, la ISO/IEC 31000:2011 que proporciona el esquema para la gestión de riesgos y las mejores prácticas, tales como 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 de las partes interesadas.

1. OBJETO

Determinar los lineamientos para definir, implementar, operar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) de TRANSMILENIO S.A.

2. ALCANCE DEL DOCUMENTO

Este Manual es para aplicación y conocimiento de los Trabajadores Oficiales, Empleados Públicos y Contratistas que desarrollen funciones o actividades en las diversas dependencias y procesos de la Entidad utilizando la Información de TRANSMILENIO S.A.

3. RESPONSABLES DEL MANUAL

El Profesional Especializado Grado 6 - Seguridad Informática es responsable por la elaboración, actualización y aplicación de este documento El Director de TIC será el responsable por su estricto cumplimiento y mantenimiento.

La revisión y/o actualización de este Manual deberá realizarse cuando se considere pertinente por parte de los responsables de su aplicación y cumplimiento.

4. DOCUMENTOS DE REFERENCIA

- **ISO/IEC 27005:2009**. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en la Seguridad de la Información
- **ISO/IEC 27001:2013**. Tecnología de la información. técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos
- **ISO/IEC 27002:2022**. Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información
- Modelo de Seguridad y Privacidad de la Información (MPSI) – Habilitador Transversal de la Política de Gobierno Digital.

5. DEFINICIONES

Activo de información: todo aquel recurso del Sistema de Seguridad de la Información ISO/IEC 27001:2013 necesario para que la empresa funcione alineada con las políticas de seguridad de la información. Es referido a todo aquel software o hardware o recurso humano en el que procesa, almacena o transmite información y que tiene un valor para la organización. Ejemplo: bases de datos, programas de computación, plataforma tecnológica (procesamiento de datos o comunicaciones), documentos impresos.

Almacenamiento: se refiere a la forma en la que se almacena el activo, como en medios magnéticos, salas, cajas, PC's, Servidores, CD's, DVD's, USBs, Cintas magnéticas, etc.

Auditoría: examen sistemático e independiente para determinar sí las actividades y los resultados relacionados con la seguridad de la información cumplen disposiciones preestablecidas, y sí estas disposiciones se aplican en forma efectiva y son aptas para alcanzar los objetivos.

Base de Datos: conjunto organizado de datos personales que sea objeto de Tratamiento.

Borrado Seguro: aplica solo para medio magnéticos, es un borrado a bajo nivel.

Clasificación de la Información: es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulado por la entidad. Tiene como objetivo asegurar que la información tenga el nivel de protección adecuado. La información debe clasificarse en términos de sensibilidad e importancia para la entidad.

Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Contraseña: serie secreta de caracteres que permite a un usuario tener acceso, a un archivo, computador o programa.

Contratista: persona natural o jurídica que se vincula a la entidad con el objeto de prestar a TRANSMILENIO S.A. un bien o un servicio determinado.

Cultura de seguridad de la información: es aquella red de significados, acciones, creencias y comportamientos que se asocian con la seguridad y control de la información, la cual define en sí misma la forma como una persona cuida y protege ese activo que representa esa figura valiosa para él y por ende para la organización.

Destrucción: se refiere a la actividad para la destrucción de la información que se maneja sobre el activo en el momento en el que este finaliza su ciclo de vida.

Dependencia: oficina o área de la entidad.

Dominio: áreas en las que se desarrolla la ISO/IEC 27001:2013

Disponibilidad: es la característica o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Excepciones: todo aquello que se excluye de la generalidad o regla común.

Firewall: es un computador, software o dispositivo físico que se conecta en una red con salida a internet con el fin de impedir el acceso no autorizado, incorporando elementos que garantizan la privacidad, autentificación y filtraje de contenidos, conforme a las políticas de seguridad de la información, de la entidad donde se instala.

Gestión de riesgos: es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir en el desarrollo de una determinada actividad, abordándose una clasificación de los mismos y construyendo unos planes de acción para su tratamiento.

Hardware (HW): son las partes físicas y tangibles de una computadora, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos, sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Incidente de seguridad de la Información: un evento o serie de eventos de seguridad de la Información no deseados o inesperados, que tiene una la probabilidad significativa de comprometer las operaciones del negocio o amenazar la seguridad de la información de los activos críticos que almacenen, procesen y/o gestionen información.

Información: conjunto de datos acerca de un suceso, hecho, fenómeno o situación, que organizados en un contexto determinado tienen su significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo. Información impresa, escrita, hablada y almacenada.

Integridad: capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización.

Intranet: red de computadores que utiliza la tecnología del protocolo de internet (IP) para compartir información, sistemas operativos o servicios de computación dentro de una organización, es de carácter interno, por lo que solo los miembros de esa organización tienen acceso a ella.

MinTIC (Ministerio de Tecnologías de la Información y las Comunicaciones): es la entidad que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las tecnologías de la información y las comunicaciones. Dentro de sus funciones está incrementar y facilitar el acceso de los usuarios de la organización a las tecnologías de la información, las comunicaciones y a sus beneficios.

MIPG: Modelo Integrado de Planeación y Gestión

MSPI: Modelo de Seguridad y Privacidad de la Información

Partes interesadas: son aquellos individuos o entes que influyen en el proceso de gestión de la seguridad de la información o son influenciados por él. Dentro del contexto del sistema de gestión de seguridad de la información se consideran como partes interesadas (stakeholders), usuarios internos, clientes, directivos, entre otros.

Personal: funcionarios, empleados contratados, consultores y contratistas.

Políticas: conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una Entidad teniendo el propósito de proteger la información, los recursos y la reputación de la misma.

Política de seguridad de la información: establece a alto nivel los objetivos y metas relacionados con la seguridad de la información.

Propietario de la información: individuo, entidad o unidad de negocio que tiene la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información que le han sido asignados o de los que hace uso.

Proveedor: persona natural o jurídica que abastece a otras empresas o personas, con existencias de bienes o servicios, necesarios para el normal desarrollo de las actividades propias de esas personas o empresas.

Registro: documento que suministra evidencia objetiva de las actividades efectuadas o de los resultados alcanzados.

Servidor público o Trabajador Oficial: es una persona que desempeña un empleo público. Se trata de un trabajador que cumple con funciones en el organismo del estado.

Sistema de Gestión de Seguridad de la Información (SGSI): conjunto de políticas, procedimientos, procesos y recursos, basado en un enfoque de riesgo del negocio para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye organigrama, políticas, planificación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos relacionados con la seguridad de la información.

Seguridad de la información: conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

Software: conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación. (Extraído del estándar 729 del IEEE5).

Tercero o subcontratista: es el proveedor de un producto o servicio que afecta la calidad del servicio prestado por la empresa o que desarrolla labores de asesoría, consultoría, implementación, soporte o mantenimiento y demás personas que, sin ser de planta de la Entidad, tienen un nivel de vinculación o brindan algún tipo de servicio dentro de las instalaciones de TRANSMILENIO S.A.

TIC: conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes (Art. 6 Ley 1341 de 2009).

UPS: sistema de alimentación ininterrumpida - Uninterruptible Power Supply (UPS), es un dispositivo que, gracias a un conjunto de baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica a todos los dispositivos que tenga conectados por un tiempo limitado y durante un corte del fluido eléctrico.

Vulnerabilidad: debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

SITP: Sistema Integrado de Transporte Público

6. SISTEMA DE GESTION EN SEGURIDAD DE LA INFORMACIÓN (SGSI)

Como base para la estructuración del Sistema de Gestión de Seguridad de la Información, se establece el contexto de la Entidad desde diferentes aspectos como factor humano, social, ambiental o tecnológico, entre otros, el cual permite definir la estrategia que TRANSMILENIO S.A adopta para la seguridad de la información:

6.1 Contexto de la Entidad

La Empresa de Transporte del Tercer Milenio - TRANSMILENIO S.A. es una sociedad pública por acciones de 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.

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. estarán 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 estará integrada por el Alcalde Mayor o su delegado quien la presidirá y cuatro (4) Miembros designados de conformidad con los estatutos.

TRANSMILENIO S.A. garantizará 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, estará estructurada en tres ámbitos de gestión, así: (i) Alta Gerencia, (ii) Gerencia de la Integración y (iii) Dirección y Control de la Operación;

El ámbito de la Alta Gerencia de la Empresa será 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. Dirigirá y articulará la ejecución de los procesos de la Empresa orientados todos al cumplimiento de su misión.

El ámbito de la Gerencia de la Integración será 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 será responsable de ejecutar 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.

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.

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.

6.1.1 Misión y Visión

El SGSI toma como insumo la Misión y la Visión de TRANSMILENIO S.A, tal como se encuentran definidas por la Entidad en su Plataforma Estratégica.

6.2 Contexto Interno y Externo

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

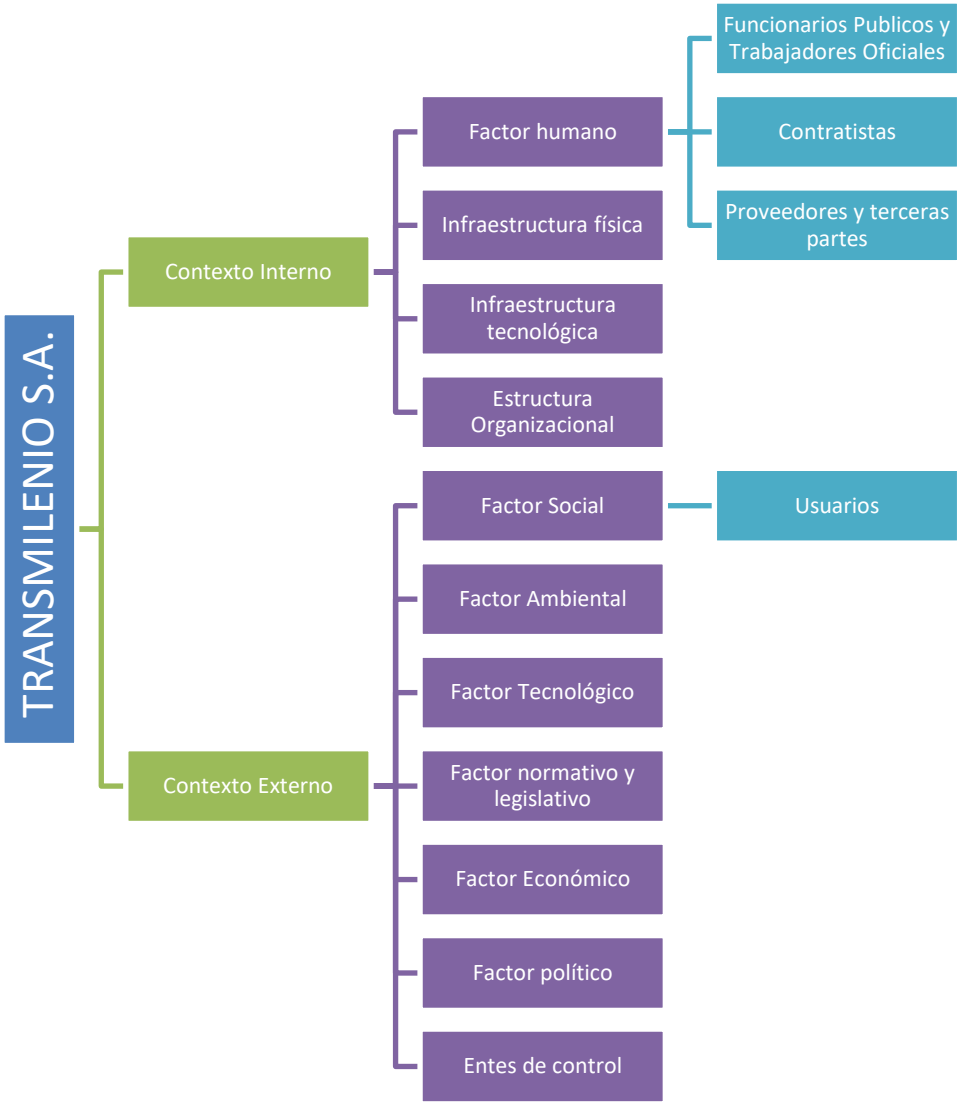


Ilustración 1. Contexto interno y externo de TRANSMILENIO S.A.

6.2.1 Contexto Interno

- **Factor Humano**

Las personas también hacen parte de los activos de información más importantes dentro de la entidad. En TRANSMILENIO S.A., se encuentran representados en funcionarios públicos, trabajadores oficiales, proveedores y terceras partes, que continuamente se encuentran en interacción 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 que ha establecido la entidad para minimizar el riesgo que de alguna manera las personas representan para el SGSI; 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.

En el momento de vinculación a la Entidad y en el marco del proceso de inducción que lidera la Dirección Corporativa, se realiza sensibilización a los servidores públicos donde se les ilustra sobre las políticas de seguridad de la información. De igual forma, al terminar el vinculo laboral, la Entidad toma medidas de seguridad frente al retiro de privilegios y permisos sobre los activos de información que utilizaba el funcionario o contratista retirado.

- **Estructura Organizacional**

Si bien la estructura organizacional es requerida para la asignación de responsabilidades de seguridad de la información dentro del SGSI, es importante conocer el contexto de este aspecto dentro de la Entidad. A continuación, se presenta la organización interna de la Empresa de Transporte del Tercer Milenio - TRANSMILENIO S.A., la cual se soporta en los siguientes acuerdos:

- Acuerdo 002 2011 de Modificación de la estructura organizacional y funciones de las dependencias de la empresa Tercer Milenio TRANSMILENIO S.A.
- Acuerdo 007 2017 Modificación de la estructura organizacional y funciones de las dependencias de la empresa Tercer Milenio TRANSMILENIO S.A. de 2017
- Acuerdo 008 2017 de Modificación de la estructura organizacional y funciones de las dependencias de la Empresa de Transporte del Tercer Milenio TRANSMILENIO S.A.

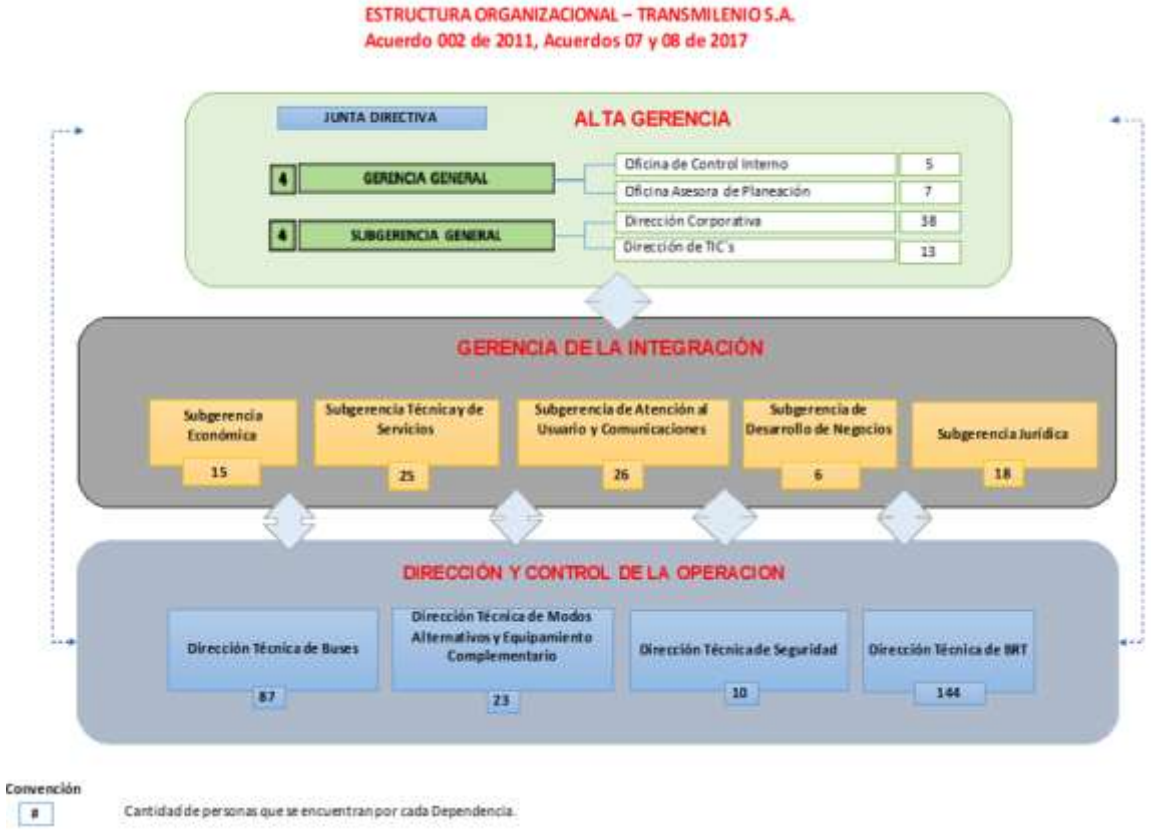


Ilustración 2. Organigrama de TRANSMILENIO S.A.

- **Infraestructura Física**

La Sede Administrativa de TRANSMILENIO S.A., ubicada en Bogotá en la Av. Eldorado No. 69 - 76 / Edificio Elemento Torre 1 cuenta con instalaciones en arriendo, distribuidas en 5 pisos. Las instalaciones cuentan, entre otros, con puestos de trabajo, comedor, cafeterías, sala de bienestar, salas de reuniones, enfermería, sala de espera, recepciones, oficinas de directivos, cuartos de almacenamiento, emisora, cuarto de lactancia, cuartos técnicos y eléctricos, Centro de Datos y Centro de Control. Dichas oficinas cumplen con controles de seguridad para acceder a las mismas, se exige el porte del carnet institucional para los servidores públicos, contratistas así como el registro de ingreso para visitantes en la recepción del piso 1 y para el acceso de ingreso a la entidad en el piso 7 en donde se entrega una identificación impresa y el acompañamiento por parte del funcionario correspondiente.

Cuando se ingresen dispositivos tecnológicos a la entidad, los servidores públicos, contratistas, proveedores y demás partes interesadas deberán registrar dichos dispositivos en las bitácoras de la recepción del piso donde ingresan y/o desarrollan sus actividades.

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

- Áreas seguras.
- Sistemas de detección y extinción de incendios.
- Áreas de evacuación.
- Señalización de áreas.
- El edificio cuenta con ocho (8) ascensores.
- Cuartos de cableado en cada piso debidamente protegidos con llave.

- **Infraestructura Tecnológica**

TRANSMILENIO S.A. cuenta con un (1) DATACENTER que se encuentra 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 realiza frecuentemente la actualización de la infraestructura de red y seguridad con equipos de nueva generación, que permiten mayor administración, rapidez y mayor seguridad de la información. Realiza la adopción de una estrategia de servicio de Comunicaciones de largo plazo para garantizar la disponibilidad de las comunicaciones 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 genera ahorros importantes frente al sistema de Red con que se viene operando.

TRANSMILENIO S.A. 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 con tarjeta de proximidad o sistema biométrico, adicionalmente cuenta con:

- Sistemas de detección y extinción de incendios.
- Se encuentran independientes los racks de servidores, cableado y UPS.
- 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.

El personal autorizado con el uso de sistemas de control de acceso por tarjeta de proximidad podrá tener ingreso del Datacenter.

6.2.2 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. desarrolla y actualiza constantemente programas de Responsabilidad Social alineado con la estrategia.

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 de forma segura en sus componentes zonal y troncal mediante espacios de capacitación y sensibilización que fortalezcan los mecanismos de participación ciudadana y el sentido de pertenencia. Lo anterior, dentro del marco del SGSI, el cual vincula las actividades de protección de la información y sensibilización a sus colaboradores también para este tipo de actividades.

- **Factor Ambiental**

TRANSMILENIO S.A., cuenta con un Plan Institucional de Gestión Ambiental - PIGA, el cual establece las estrategias para la implementación de la gestión ambiental institucional y del Sistema de Transporte Masivo, en el marco de las competencias 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 programas que apuntan al cumplimiento de los objetivos establecidos en el Plan de Gestión Ambiental de Distrito y de los principios de sostenibilidad ambiental.[1]

Por otro lado, en el marco de la implementación del Sistema de Gestión de Seguridad de la información (SGSI) se consideran los posibles riesgos ambientales que se pueden presentar y que pueden derivar en contaminación del ambiente y afectación de los usuarios del servicio, tanto internos como externos, causada por la materialización de riesgos de seguridad de la información, incidentes de seguridad y ciberataques que pueden conducir a incendios o daños físicos sobre la infraestructura tecnológica y las instalaciones de procesamiento de datos.

Lo anterior contempla por lo menos los siguientes escenarios de riesgo:

- Contaminación y afectación a los usuarios por incendios causados de forma intencional o accidental por mala manipulación de los equipos, ingreso de líquidos a los centros de procesamiento de datos, ausencia de alarmas contra incendios, falta de extintores, falta de supervisión, incumplimiento de políticas, uso de productos inadecuados de protección y limpieza, estática y/o deterioro de equipos.
- Afectación del consumo de energía y recursos por manipulación intencional o accidental de equipos en horarios no hábiles, sobre procesamiento y recalentamiento de equipos o ausencia de conciencia en políticas de seguridad de la información relacionadas con el uso óptimo de los recursos.
- Situaciones de riesgo que afecten equipos de procesamiento de datos, recintos o instalaciones, causadas por vandalismo, terrorismo, desastres naturales, ciberataques terroristas, protestas o empleados disgustados.
- Incidentes o accidentes en la operación de la flota de buses que materialicen riesgos ambientales que ocasionen afectación al ambiente, causados por mal funcionamiento de los sistemas de apoyo al control de la operación de Sistema.
- Por lo anterior, como parte de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), así como del Plan Institucional de Gestión Ambiental (PIGA), se adoptan controles de seguridad para mitigar dichos riesgos, garantizando que se considere la protección del medio ambiente así como la salud de los colaboradores en lo relacionado con el componente tecnológico que es gobernado por la seguridad de la información.

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

- **Factor Tecnológico**

TRANSMILENIO S.A. como Empresa del Distrito Capital, implementa, de manera sistemática y coordinada, la Política de Gobierno Digital la cual es una estrategia del Gobierno Nacional liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones y apoyada por la Alta Consejería Distrital de TIC, 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. TRANSMILENIO S.A implementa estas directrices a través de la construcción de sus Sistema de Gestión de Seguridad de la Información (SGSI), y su Plan Estratégico de Tecnologías de la información (PETI), los cuales se encuentran alineados con las recomendaciones y directrices del Gobierno Nacional.

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.

- 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 en la Entidad, en el marco del proceso de Gestión TIC, de la dirección de TIC.

- **Factor Normativo y Legislativo**

TRANSMILENIO S.A., como Empresa del Distrito Capital, 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* [2].

- **Factor Económico**

De acuerdo con el Plan Estratégico Institucional del 2015, TRANSMILENIO S.A. 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.

TRANSMILENIO S.A. define estrategias financieras que conduzcan a promover el acceso al sistema integrado de transporte público a través de tarifas establecidas para uso del sistema, así como preferenciales a grupos poblacionales en condición de vulnerabilidad.

- **Factor Político**

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 política 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

[2] Ver Nomograma de TRANSMILENIO S.A. publicado en el link de Transparencia y Acceso a la información

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.
- Contaduría General de la Nación.
- Personería Distrital.

6.2.3 Análisis DOFA

Luego de identificar los actores internos y externos, se utiliza dicha información para realizar el análisis DOFA (debilidades, oportunidades, fortalezas y amenazas) con relación a la seguridad de la información dentro del marco del SGSI. El análisis DOFA hace parte integral del presente manual y se encuentra en custodia por parte del Grupo de Seguridad de la Información, por ser de acceso restringido.

6.3 Partes Interesadas

TRANSMILENIO S.A. reconoce como partes interesadas del SGSI las que se relacionan a continuación

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

PARTE INTERESADA	DESCRIPCIÓN	NECESIDADES Y EXPECTATIVAS FRENTE A SEGURIDAD DE LA INFORMACION
Usuarios Indirectos	Usuarios del sistema y la ciudadanía en general.	objeto, ha sido suministrada, gestionada, 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 de Bogotá, 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.	

Tabla 1. Partes Interesadas

6.4 Modelo del Sistema de Seguridad de la Información

6.4.1 Estructura del Modelo

El modelo del SGSI de TRANSMILENIO S.A. se encuentra basado en el ciclo de mejoramiento continuo PHVA (Planear, hacer, actuar y verificar), el cual asegura que el Sistema 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 el SGSI. A continuación, se ilustra el Modelo del SGSI definido y adoptado por la entidad:

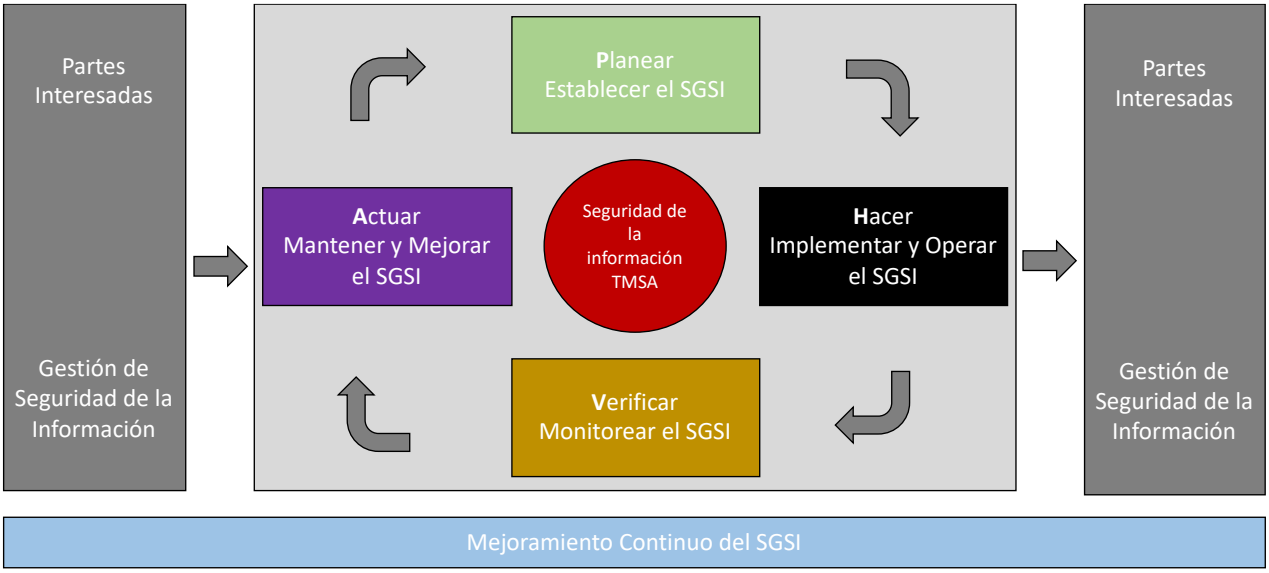


Ilustración 3. Modelo del SGSI basado en el Ciclo PHVA

De igual forma, cada uno de las fases del ciclo PHVA incluye diferentes actividades propias de la seguridad de la información que se alinean con lo especificado en la norma ISO/IEC 27001:2013 y el Modelo de Seguridad y Privacidad de la Información (MSPI), tal como se presenta a continuación:

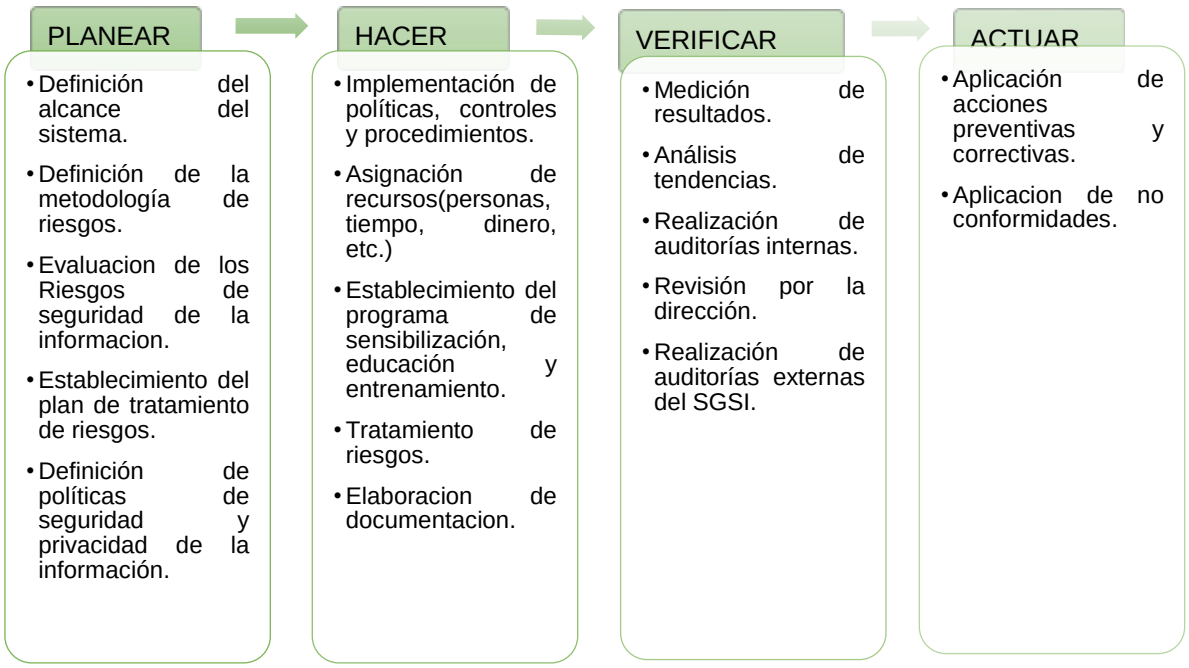


Ilustración 4. Fases del ciclo PHVA

6.4.2 Componentes del SGSI

Por lo anterior, en el ámbito de Seguridad de la Información, los componentes del sistema contemplan los principios, políticas, procedimientos, estándares, protocolos, instructivos e infraestructura tecnológica en diferentes niveles de acuerdo a su importancia, tal como se ilustran y se describen a continuación:

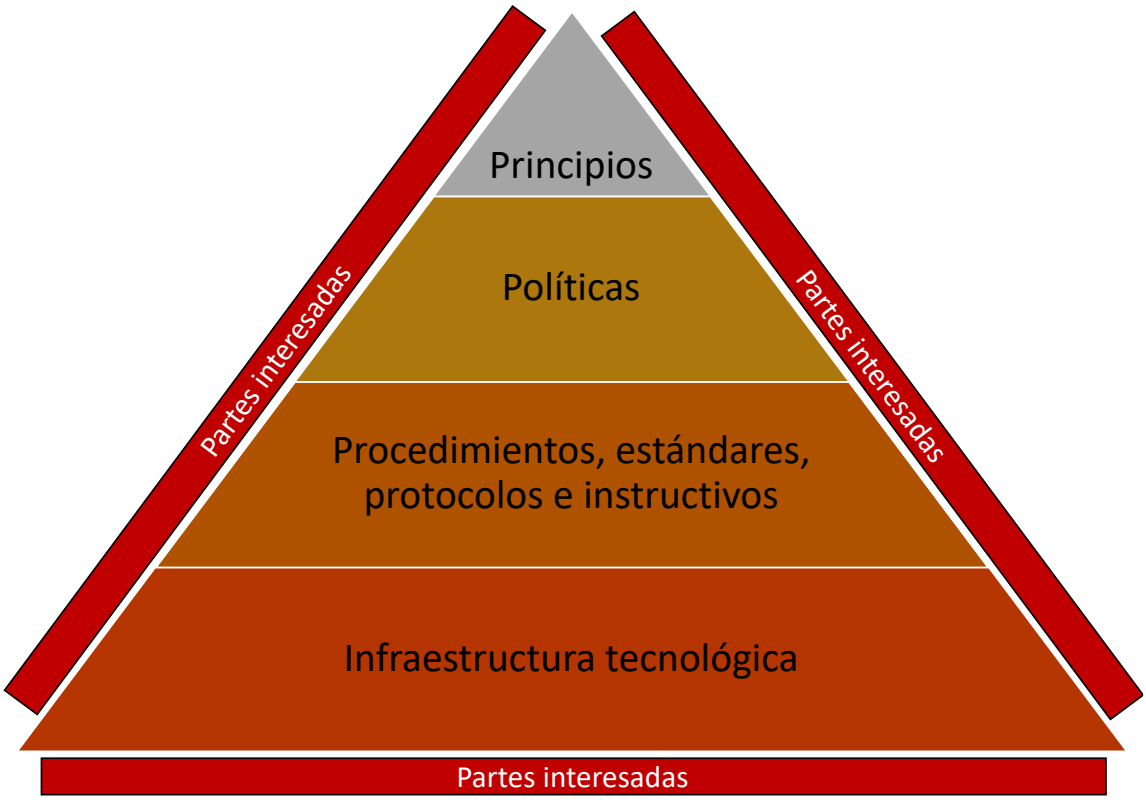


Ilustración 5. SGSI desde la perspectiva de sus componentes

- **Principios**

Los principios son el soporte de la visión, la misión, la estrategia y los objetivos estratégicos de la entidad. En el marco de la seguridad de la información se exponen a continuación:

- ✓ La información es uno de los activos más importantes de TRANSMILENIO S.A. y, por lo tanto, se espera que sea utilizada acorde con los requerimientos de la entidad.
- ✓ La **confidencialidad** de la información de la entidad y de terceras partes debe ser mantenida, independientemente del medio o formato donde se encuentre.

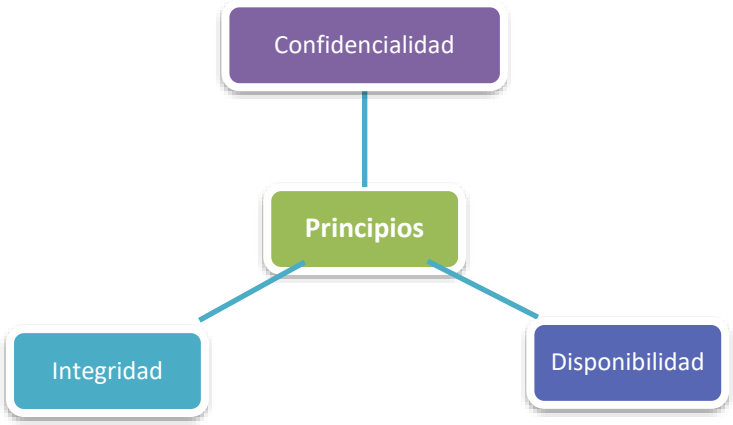


Ilustración 6. Principios de seguridad de la información

- ✓ La información de la entidad debe preservar su **integridad** independientemente de su residencia temporal o permanente, o la forma en que sea transmitida.
- ✓ La información de la entidad debe estar **disponible** cuando sea requerida.

- **Políticas**

Las políticas de seguridad y privacidad de la información de TRANSMILENIO S.A. tienen por objetivo general asegurar que la información sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones (Confidencialidad); que esté protegida contra modificaciones no planeadas, realizadas con o sin intención (Integridad), que esté disponible cuando sea requerida (Disponibilidad) y que sea utilizada para los propósitos que fue obtenida (Privacidad).

Los objetivos específicos que persiguen las Políticas de Seguridad de la Información son:

- ✓ Establecer los fundamentos para el desarrollo y la implantación del SGSI.
- ✓ Definir la conducta a seguir en lo relacionado con el acceso, uso, manejo y administración de los recursos de información.
- ✓ Establecer y comunicar la responsabilidad en el uso de los activos de información, que soportan los procesos y sistemas del negocio.
- ✓ Administrar los riesgos en seguridad de la información.

- ✓ Establecer los canales de comunicación que le permitan a la Alta Dirección mantenerse informada de los riesgos y uso inadecuado de los activos de información, y las acciones tomadas para su mitigación y corrección.
- ✓ Proteger la imagen, los intereses y el buen nombre de TRANSMILENIO S.A.

Las políticas para TRANSMILENIO S.A. están documentadas y establecidas en el *Manual de Políticas de seguridad y privacidad de la información* (*M-DT-001)*, el cual se encuentra adoptado oficialmente en el Sistema de Gestión - SIG de la Entidad. En consecuencia, las políticas del SGSI se constituyen como directrices establecidas por la alta dirección y/o en cabeza del Líder u Oficial de Seguridad de la información.

- **Procedimientos, estándares, protocolos e instructivos**

✓ **Procedimientos**

Los procedimientos de Seguridad de la Información se apoyan en la *Política de seguridad y privacidad de la información*. Dentro de los procedimientos que se contemplan como parte del Sistema de Gestión de Seguridad de la información se encuentran, entre otros, los siguientes:

- Procedimiento para la gestión de incidentes de seguridad de la información (P-DT- 020)
- Procedimiento para el control de cambios de infraestructura tecnológica (P-DT-017)
- Procedimiento de control de acceso físico (P-DT-021)
- Procedimiento para el intercambio seguro de información electrónica (P-DT-012)

✓ **Estándares**

Los estándares de seguridad se utilizan para mantener los diferentes componentes del SGSI con unas directrices normalizadas de seguridad. Esto permite establecer una línea base la cual da los parámetros básicos de seguridad y de ahí en adelante, dependiendo de los requisitos de los servicios, se habilitan estos servicios o protocolos. Ejemplos de estándares incluyen la norma ISO/IEC 27001:2013 en la cual se basa el SGSI de TRANSMILENIO S.A para su respectiva implementación.

✓ **Protocolos e Instructivos**

Documentos que tienen por objetivo conducir, encaminar y dirigir las acciones de seguridad de la información para dar cumplimiento a los principios y políticas definidas por TRANSMILENIO S.A. Dentro de los Protocolos e Instructivos que hacen parte del SGSI se encuentran, entre otros:

- T-DT-003 Protocolo a seguir para gestionar el uso de Medios Removibles
- T-DT-007 Plan de Cultura y Sensibilización del SGSI
- T-DT-002 Protocolo de estándares para el Desarrollo de Software en TRANSMILENIO S.A.
- T-DT-011 Gestión de seguridad de la información en continuidad de Negocio
- I-DT-001 Instructivo para la identificación, valoración y clasificación de activos de información.

✓ **Infraestructura tecnológica**

La infraestructura tecnológica corresponde al hardware y software que soportan las actividades que realiza la Entidad a través de sus procesos de negocio y está conformada, entre otros, por los siguientes componentes:

- Infraestructura de seguridad perimetral
- Infraestructura de conectividad
- Sistemas de información y Bases de datos
- Software de monitoreo de seguridad
- Sistemas de almacenamiento y copias de respaldo
- Licenciamiento de software

7. POLITICA DE ALTO NIVEL DEL SGSI[3]

Armonizados con el Plan Estratégico Institucional, la entidad establece la siguiente Política de alto nivel del SGSI:

"La información es reconocida por TRANSMILENIO S.A como uno de los activos más importantes para lograr su objetivo fundamental de contribuir al desarrollo sostenido del sector movilidad , mediante la prevención, vigilancia y control , es por eso que se compromete a disponer sus recursos tanto físicos, tecnológicos, financieros, informativos, de conocimiento y humanos para liderar y fortalecer la seguridad de la información a través del establecimiento, implementación y mejora continua de un Sistema de

[3] Las políticas de seguridad de la información se encuentran consignadas dentro del Manual M-DT-001 Políticas de seguridad y privacidad de la información de TRANSMILENIO S.A

gestión de seguridad de la información (SGSI); cuyo fin es el aseguramiento de la integridad, disponibilidad y confidencialidad de la información mediante la gestión y tratamiento adecuado de los riesgos, en el marco de los requisitos de la entidad, los legales o reglamentarios, y las obligaciones de seguridad contractuales; con servidores públicos, trabajadores oficiales, proveedores y partes interesadas, comprometidos a participar activamente en el desarrollo de la cultura de seguridad de la información".

8. OBJETIVOS DE SEGURIDAD DE LA INFORMACION

Articulados con la Política de alto nivel del SGSI, la entidad define los siguientes objetivos de seguridad y privacidad de la información:

1. Adoptar un SGSI en TRANSMILENIO S.A, como una decisión estratégica.
2. Definir y divulgar las Políticas de Seguridad y privacidad de la información a todos los funcionarios de la entidad.
3. Asignar los recursos, la infraestructura tecnológica y el personal necesario para la gestión de la seguridad de la información de la Entidad.
4. Implementar y fortalecer los controles para la protección de los activos de información.
5. Minimizar los riesgos extremos y altos de seguridad de la información.
6. Controlar y prevenir los incidentes de Seguridad de Información.
7. Prevenir incumplimientos normativos, legales y/o contractuales a través del seguimiento continuo al cumplimiento de las políticas de seguridad y privacidad de la información.
8. Construir una cultura en seguridad de la información al interior de la entidad.
9. Mantener la mejora continua del SGSI a través de la atención oportuna y eficaz de los planes de acción.

9. ALCANCE DEL SGSI

A partir del análisis del contexto interno y externo, así como las partes interesadas, TRANSMILENIO S.A. define el alcance de SGSI, teniendo en cuenta las características de la Entidad, su ubicación, sus activos y su tecnología, de la siguiente manera:

"TRANSMILENIO S.A., establece, implementa, opera, verifica y mejora el SGSI basado en la norma ISO/IEC 27001:2013 con el objetivo de proteger la confidencialidad, integridad y disponibilidad de los activos de información para las siguientes dependencias:

- *Dirección Técnica de TIC.*
- *Subgerencia Jurídica.*
- *Subgerencia técnica y de servicios.*
- *Dirección Técnica de Seguridad.*
- *Subgerencia de Atención al Usuario y Comunicaciones.*

No obstante, si bien en la actualidad el alcance del SGSI se encuentra limitado a las áreas mencionadas anteriormente, se aclara que en aras de cubrir la totalidad de las dependencias de TRANSMILENIO S.A, dicho alcance se extenderá a las demás dependencias de forma gradual y conforme a lo definido dentro del Plan Estratégico de Seguridad de la Información (PESI).

10. GESTIÓN DE RIESGOS

La metodología adoptada por TRANSMILENIO S.A. para la gestión de riesgos de Seguridad Digital se define dentro del manual "M-OP-002 Manual para la gestión del riesgo en TRANSMILENIO S.A", el cual contempla todas las fases necesarias para la identificación, evaluación, valoración, tratamiento y aceptación del riesgo.

Entre los beneficios de analizar, identificar y tratar adecuadamente los riesgos, se encuentran:

- Aumentar la probabilidad de alcanzar los objetivos.
- Cumplir con los requisitos legales y reglamentarios pertinentes y con las normas Internacionales.
- Mejorar la prestación del servicio interno y externo.

- Establecer una base confiable para la toma de decisiones y la planificación estratégica.
- Mejorar los controles existentes.
- Mejorar la eficacia y la eficiencia operativa.
- Incrementar el desempeño frente al SGSI.
- Mejorar la gestión de incidentes.
- Minimizar los riesgos de seguridad de la información.
- Aportar una buena base de conocimiento frente a la solución de incidentes y riesgos.

Los riesgos de Seguridad Digital se enfocan en las situaciones que puedan afectar la confidencialidad, integridad y disponibilidad de la información. Por lo tanto, como parte de este proceso se realiza la identificación de los activos críticos, tipificados en tipos de activos como lo son los activos de tipo Información, Hardware, Software, Servicios, Personal y ubicaciones físicas de la Entidad. Una vez se han identificado los activos críticos y las situaciones de riesgo, así como amenazas, vulnerabilidades, probabilidad, impacto, se define el Plan de Tratamiento del Riesgo, el cual permite estructurar las actividades que reduzcan el riesgo residual. Con lo anterior, se actualiza la Declaración de Aplicabilidad, el Plan Estratégico de Seguridad de la Información (PESI) y su respectivo mapa de ruta.

11. DECLARACION DE APLICABILIDAD

La declaración de aplicabilidad es un documento basado en el anexo A de la norma ISO/IEC 27001:2013 que agrupa 114 controles en 14 dominios. A través de la declaración de aplicabilidad, TRANSMILENIO S.A. identifica los controles aplicables que serán implementados como parte del SGSI y sus excepciones.

Elementos que forman parte de la declaración de aplicabilidad:

- ✓ Los objetivos de control.
- ✓ La aplicabilidad del control.
- ✓ La justificación de la inclusión o exclusión.
- ✓ Tipo de control
- ✓ Los requisitos aplicables.

La declaración de aplicabilidad se soporta con base en lo consignado dentro del Plan de Tratamiento de Riesgos, el Plan Estratégico de Seguridad de la Información (PESI) y su mapa de ruta.

12. ORGANIZACIÓN DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION)

12.1 Estructura organizacional de seguridad de la información

Para el diseño, establecimiento, implementación, operación y mejora del SGSI, TRANSMILENIO S.A. adopta el modelo de una organización de tipo centralizada o unidad central, de donde se emite la política de seguridad y privacidad de la información, asegura el despliegue de las directrices de seguridad a las demás dependencias de la entidad para su conocimiento y aplicación.

Para tal fin, la entidad ha delegado el liderazgo del SGSI a la Dirección de TIC, quien articula la participación de las diferentes dependencias de la Entidad en la adopción de las directrices y políticas de seguridad de la Información. No obstante, la última instancia responsable por el SGSI será la Gerencia General y el Comité Integrado de Gestión y Desempeño.

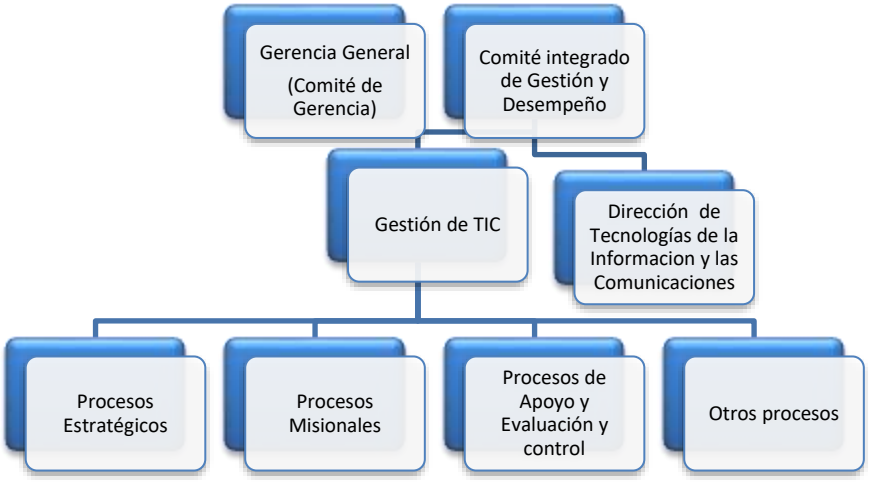


Ilustración 7. Organización del SGSI

- **Comité de Gerencia**

En esta instancia se definen las directrices y lineamientos bajo los cuales debe operar el SGSI; sus responsabilidades son:

- Contemplar en el marco del C*omité Integrado de Gestión y Desempeño* todas las funciones relacionadas del Comité del SGSI.

- Mantener dentro de la planta de personal de TRANSMILENIO S.A, un funcionario que tenga asignado el rol de Líder u Oficial de Seguridad de la información, quien será el encargado de gestionar todo lo relacionado con la seguridad de la información en la entidad.
- Invitar al Profesional Especializado Grado 06 – Seguridad informática a las sesiones de comité de gerencia cuando se requieran tratar, absolver o tomar acciones y decisiones asociadas al Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad.
- Establecer, aprobar y actualizar los lineamientos y políticas del SGSI, asegurando su integración con los demás procesos de la entidad, el Plan Estratégico y el Plan Distrital de Desarrollo actual. Como resultado se cuenta con el M-DT-001 Manual de Políticas de Seguridad y Privacidad de la información.
- Velar por el cumplimiento de la política de seguridad y privacidad de la información, comprometiéndose para que los servidores públicos, oficiales y contratistas, a su cargo, y partes interesadas conozcan y apliquen los controles de seguridad establecidos.
- Vigilar que se ejecute el programa de auditorías o revisiones internas por parte de la Oficina de Control Interno, al menos una vez al año para que se realicen las mejoras correspondientes.
- Definir el nivel de aceptación del riesgo de acuerdo con lo establecido en el M-OP-002 Manual para la gestión del riesgo en TRANSMILENIO S.A.
- Asignar los recursos necesarios para garantizar la eficacia del SGSI.

- **Comité Institucional de Gestión y Desempeño**

Para establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI, el Comité Institucional de Gestión y Desempeño – MIPG, tiene como responsabilidades:

- Evaluar y aprobar las estrategias y la política de seguridad y privacidad de la información que requiera la entidad de acuerdo con la dinámica y condiciones de esta.
- Fijar directrices institucionales para la aplicación de los mecanismos de protección de seguridad de la información.
- Evaluar y aprobar las políticas básicas y específicas de seguridad y privacidad de la información; garantizando su difusión y aplicación en la entidad.
- Evaluar y aprobar Planes de Continuidad de la seguridad de la información que ante una situación crítica pueda verse amenazada de manera parcial o total.

- Aprobar los programas periódicos de ejercicios de continuidad del negocio y recuperación.
- Apoyar la identificación de los procesos críticos de la entidad, así como analizar y proponer soluciones tecnológicas que requiera la misma.
- Generar y apoyar los planes de socialización, sensibilización y transferencia de conocimiento en los temas relacionados con el SGSI.

- **Lider u Oficial de Seguridad de la Información**

La Dirección General asigna el rol "Líder u Oficial de Seguridad de la Información" al Profesional Especializado Grado 6 - Seguridad informática para efectos de garantizar y liderar la implementación, mantenimiento y mejora del SGSI. Por lo tanto, este Profesional actúa bajo las directrices que establezca el *Comité Institucional de Gestión y Desempeño* de TRANSMILENIO, así:

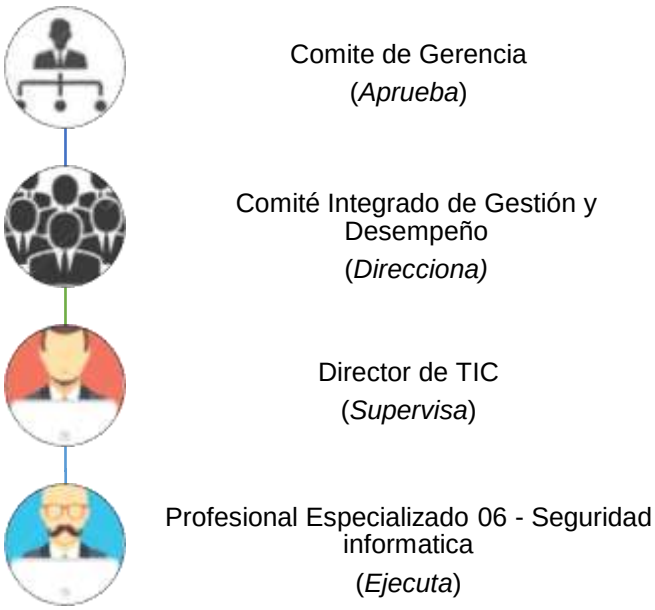


Ilustración 8. Modelo de operación del Líder y Oficial de Seguridad de la Información

En consecuencia, el Profesional Especializado 06 - Seguridad Informática, planea, diseña e implementa el SGSI de la entidad a través de la definición de Políticas, lineamientos, controles, requerimientos legales y buenas prácticas.

Por otro lado, el Profesional Especializado Grado 06 – Coordinador de procesos Corporativos, el Profesional Universitario Grado 03 - Gestor de Bases de Datos y Aplicaciones Corporativas, el Técnico

Administrativo Grado 02 y el Grupo de Seguridad de la información de la Dirección de TIC junto con su equipo de contratistas, apoyan la implementación técnica de los controles del Sistema de Gestión de seguridad de la información (SGSI). No obstante, como parte de la supervisión y control del sistema se involucra la Oficina de Control Interno, la cual está encargada del monitoreo a través de auditorías y revisiones al SGSI.

Entre las responsabilidades y funciones del Profesional Especializado Grado 06 – Coordinador de Procesos Corporativos, el Profesional Universitario Grado 03 - Gestor de Bases de Datos y Aplicaciones Corporativas, el Técnico Administrativo Grado 02, y el Grupo de Seguridad de la información de la Dirección de TIC, así como de la oficina de control interno para cada fase del ciclo PHVA, se encuentran:

PHVA	Profesional Especializado Grado 6 - Seguridad Informática	Profesional Especializado Grado 06 – Coordinador de procesos corporativos Profesional Universitario Grado 03 - Gestor de Bases de Datos y Aplicaciones Corporativas Técnico Administrativo Grado 02, de la Dirección de TIC Grupo de Seguridad de la información	Oficina de Control Interno (Dentro del marco de sus funciones de auditoría)
P	1. Planificar, diseñar e implementar el SGSI de la entidad, sus Políticas, lineamientos y controles, los requerimientos legales y buenas prácticas.	-	1. Definir el plan de auditorias frente al Sistema de Gestión de Seguridad de la información (SGSI)
P	2. Planificar y diseñar el Modelo de Seguridad y Privacidad de la Información acorde con la Estrategia de Gobierno Digital.	-	-
P	3. Planear las Actividades correspondientes a la estrategia de Ciberseguridad definida por el Ministerio de Defensa Nacional.	-	-

PHVA	Profesional Especializado Grado 6 - Seguridad Informática	Profesional Especializado Grado 06 – Coordinador de procesos corporativos Profesional Universitario Grado 03 - Gestor de Bases de Datos y Aplicaciones Corporativas Técnico Administrativo Grado 02, de la Dirección de TIC Grupo de Seguridad de la información	Oficina de Control Interno (Dentro del marco de sus funciones de auditoría)
H	1. Desarrollar las actividades de coordinación de Seguridad de la Información y seguridad Informática de la entidad.	1. Administrar las herramientas de seguridad perimetral de la entidad.	1. Verificar los controles definidos de Seguridad de la Información y Seguridad Informática de la entidad.
H	2. Establecer directrices y hacer seguimiento a los controles definidos en los procedimientos, estándares, guías, instructivos y buenas prácticas relacionadas con la Seguridad de la Información y la Seguridad Informática.	2. Implementar los controles definidos en los procedimientos, estándares, guías, instructivos y buenas prácticas relacionadas con la Seguridad de la Información y la Seguridad Informática.	2. Verificar el cumplimiento de los controles definidos en los procedimientos, estándares, guías, instructivos y buenas prácticas relacionadas con la Seguridad de la Información y la Seguridad Informática.
H	3. Revisar y actualizar la documentación definida para el Sistema de Gestión de Seguridad de la Información SGSI.	3. Actualizar la documentación correspondiente, e implementar los cambios en el Servicio que lideran.	3. Verificar la aplicabilidad de documentación correspondiente.
H	4. Diseñar Planes de sensibilización para los funcionarios, contratistas, proveedores y terceros frente a la Cultura de Seguridad de la Información de la entidad.	4. Participar en la apropiación de Planes de sensibilización frente a la Cultura de Seguridad de la Información de la entidad.	4. Verificar el cumplimiento del plan de sensibilización y Cultura de Seguridad de la Información de la entidad.
H	5. Hacer seguimiento al Plan de Tratamiento de Riesgos referente a la Seguridad de la Información de la Entidad	5. Implementar los controles definidos en el Plan de Tratamiento de Riesgos referente a la Seguridad de la Información del a Entidad.	5. Evaluar la efectividad de los controles definidos en el Plan de Tratamiento de Riesgos referente a la Seguridad de la Información de la Entidad

PHVA	Profesional Especializado Grado 6 - Seguridad Informática	Profesional Especializado Grado 06 – Coordinador de procesos corporativos Profesional Universitario Grado 03 - Gestor de Bases de Datos y Aplicaciones Corporativas Técnico Administrativo Grado 02, de la Dirección de TIC Grupo de Seguridad de la información	Oficina de Control Interno (Dentro del marco de sus funciones de auditoría)
H	6. Evaluar, los conceptos técnicos de requerimientos de Seguridad Informática.	6. Implementar los requerimientos establecidos de Seguridad Informática.	
H	7. Elaborar la Metodología del Plan de Recuperación de Desastres "DRP".	7. Implementar el Plan de Recuperación de Desastres "DRP".	6. Evaluar cumplimiento del Plan de Recuperación de Desastres "DRP" de la dirección de TIC.
H	8. Coordinar las acciones necesarias para identificar, controlar, reducir y evaluar los Incidentes de Seguridad de la Información de la entidad. Hacer seguimiento a la gestión de incidentes de seguridad de la información de la entidad.	8. Realizar y documentar las acciones necesarias para mitigar los Incidentes de Seguridad de la Información de la entidad.	7. Evaluar la gestión de incidentes de seguridad de la información de la entidad.
H	9. Gestionar el Análisis de vulnerabilidades y remediación a la Infraestructura Tecnológica de la entidad.	9. Realizar las actividades para el análisis de vulnerabilidades y remediación a la Infraestructura Tecnológica de la entidad.	
H	10. Definir los indicadores de Gestión y llevar a cabo su medición y análisis.	10. Entregar el reporte de la Gestión y cumplimiento del Servicio a su cargo.	9. Evaluar el cumplimiento de los indicadores de Gestión
V	1. Verificar la aplicación del Sistema de Gestión de Seguridad de la Información de la entidad.	-	1. Evaluar el grado de avance de la implemente del Sistema de Gestión de seguridad de la Información de la entidad.

PHVA	Profesional Especializado Grado 6 - Seguridad Informática	Profesional Especializado Grado 06 – Coordinador de procesos corporativos Profesional Universitario Grado 03 - Gestor de Bases de Datos y Aplicaciones Corporativas Técnico Administrativo Grado 02, de la Dirección de TIC Grupo de Seguridad de la información	Oficina de Control Interno (Dentro del marco de sus funciones de auditoría)
V		-	2. Verificar el cumplimiento de la gestión de vulnerabilidades y el Plan de Remediación de la Dirección TIC.
A	1. Reportar los Incidentes de alto Impacto a la Gerencia de la entidad.	1. Gestionar los incidentes de seguridad de la información con alto impacto.	1. Revisar los reportes de los Incidentes de alto Impacto a la Gerencia de la entidad.
A	2. Reportar al Director de TIC el incumplimiento de las actividades del Sistema de Gestión de Seguridad de la Información de la entidad.	-	2. Realizar auditorías internas al cumplimiento por parte de las áreas, al Sistema de Gestión de Seguridad de la Información de la entidad SGSI.
A	3. Fomentar la mejora continua del Sistema de Gestión de Seguridad de la Información de la entidad.	-	

Tabla 2. Responsabilidades de la Dirección TIC y la OCI en el ciclo PHVA del SGSI

12.2 Roles de seguridad de la información

De acuerdo con la estructura organizacional, a continuación, se definen los roles de seguridad de la información para el SGSI, que pueden ser asignados a cargos ya establecidos en la entidad dentro del marco de sus funciones:

- **Trabajadores Oficiales y Contratistas de la Dirección de TIC.**

Los Trabajadores Oficiales y Contratistas de la Dirección de TIC son responsables de aplicar y mantener los estándares de seguridad en los recursos informáticos de su responsabilidad (Ejemplo: Sistema

Operativo, Red, Equipos de Escritorio, Firewall, Aplicación, Base de datos, Middleware, etc.) acorde con el modelo del SGSI de la entidad y bajo la autorización del propietario de la información correspondiente.

- **Administrador de infraestructura.**

El Administrador de infraestructura es responsable de aplicar los procedimientos operativos de identificación, autenticación y control de acceso tendientes a proteger los activos de información, así como de actualizar los sistemas de acuerdo con el modelo del SGSI de la entidad.

- **Técnicos de Mesa de Ayuda**

Los técnicos de mesa de ayuda son responsables de aplicar los procedimientos de administración de la Operación en los elementos de seguridad, como monitoreo de alertas, de incidentes de seguridad y de vulnerabilidades, que se presenten en los recursos de información de la entidad. Su función debe estar alineada con los procesos operativos de TI.

- **Propietarios de activos de información**

El propietario de un activo de información tiene entre sus responsabilidades:

- Definir el nivel de clasificación de la información, dar las directrices de uso del activo, autorizar privilegios y definir el ciclo de vida del mismo.
- Reportar a la dirección de TIC, a través de los mecanismos definidos, cualquier incidente de seguridad de la información, para que sea tratado y corregido mediante la aplicación de controles.
- Implementar las medidas de seguridad de la información en su área para evitar fraudes, robos o interrupción en los servicios o en los activos de información.
- En los casos en que aplique, asegurarse de que el personal: servidores públicos, oficiales, contratistas y/o proveedores tengan cláusulas de confidencialidad en los contratos de acuerdo con sus responsabilidades.

- **Usuarios de la información**

Se entiende por usuario de la información cualquier servidor público, trabajador oficial, contratista, proveedor o tercero, que utiliza la información procesada y suministrada por TRANSMILENIO S.A. para ejercer sus funciones. Entre las responsabilidades de los usuarios de la información se encuentran:

- Conocer, comprender y aplicar las políticas de seguridad de la información establecidas por la entidad.
- Llevar a cabo su trabajo asegurándose de que sus acciones no afecten la seguridad de la información.
- Reportar a la dirección de TIC, a través de los mecanismos definidos, cualquier incidente de seguridad de la información, para que sea tratado y corregido mediante la aplicación de controles.
- Hacer uso de las mejores prácticas definidas en la entidad para todos los temas relacionados con seguridad de la información.
- Cumplir con la cláusula de confidencialidad y manejo de la información contenida en el contrato firmado con la entidad.

12.3 Responsabilidades frente al SGSI

En el marco de sus funciones y competencias, las Dependencias de TRANSMILENIO S.A. tendrán las siguientes responsabilidades en relación con el SGSI:

12.3.1 Dirección de TIC

La Dirección de TIC tiene como objeto la gestión, planeación, mantenimiento y soporte de TIC para la Entidad, así como la interlocución técnica con los diferentes agentes del sistema en los temas de materia de tecnología y comunicaciones.

En el marco del SGSI, esta Dependencia tiene las siguientes responsabilidades:

- Realizar el levantamiento, actualización y mantenimiento de los activos de información pertenecientes al proceso de GESTIÓN TIC
- Realizar la gestión del riesgo del proceso teniendo en cuenta la metodología de la entidad.
- Cumplir con las disposiciones normativas vigentes aplicables al Sistema de Gestión de Seguridad de la Información, así como a cualquier requerimiento de seguridad de la entidad.
- Aplicar los controles necesarios que permitan la disponibilidad, confidencialidad e integridad de la información de los activos de información tecnológicos y recursos informáticos de la entidad.

- Evitar la divulgación, modificación, retiro, destrucción no autorizada de la información que se encuentra almacenada en medios magnéticos.
- Autorizar la creación o modificación de las cuentas de acceso o recursos de la entidad.
- Sensibilizar a los usuarios para que sigan buenas prácticas de seguridad en el uso de contraseñas.
- Realizar y mantener copias de seguridad de la información en medio digital.
- Asegurar la instalación de software antivirus que brinde protección contra código malicioso en todos los recursos informáticos.
- Velar por que el software que se utilice en la entidad sea licenciado y no atente contra la normatividad vigente.
- Ser los únicos autorizados para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes.
- Establecer un procedimiento que asegure la desactivación o bloqueo de los privilegios de acceso sobre los recursos tecnológicos, los servicios de red y los sistemas de información, cuando el servidor público, oficial, contratista o usuario haya sido desvinculado o haya terminado el contrato con la entidad.
- Mantener mecanismos de control de acceso a las áreas seguras a cargo de la Dirección de TIC, implementando una bitácora u otro para control de ingreso..
- Aplicar el procedimiento para la gestión de los cambios que se presenten al interior de la entidad, en los procesos, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
- Planificar periódicamente actividades que involucren auditorias de los sistemas en producción y asegurar que los documentos, dispositivos y medios utilizados para las auditorias de los sistemas de información estén custodiados y protegidos de accesos no autorizados.
- Asegurar la privacidad y la protección de la información de datos personales, almacenados en las bases de datos, como se exige en la legislación y la reglamentación pertinentes.
- Documentar los resultados de las auditorias de los sistemas de Información.
- Apoyar en la identificación y gestión para garantizar la protección de la información al momento de ser transferida o comunicada a un tercero.

- Garantizar que los activos de información se encuentren ubicados y protegidos de tal modo que se reduzcan los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
- Ejecutar las copias de seguridad de los activos de información devueltos.
- Ejecutar el procedimiento de borrado seguro de los activos de información devueltos.
- Reportar incidentes de seguridad siguiendo el procedimiento de Gestión de Incidentes definido por la entidad y publicado respectivamente en la Intranet dentro del proceso de GESTIÓN TIC.

12.3.2 Dependencias de la entidad

En el marco del SGSI y de sus funciones, las dependencias de la entidad deben cumplir con las siguientes responsabilidades:

- Realizar el levantamiento, actualización y mantenimiento de los activos de información pertenecientes a su proceso. Esto se hace a través de la definición y actualización de las tablas de retención documental (TRD) y con el acompañamiento de la Dirección de TIC para los activos tecnológicos.
- Participar en las actividades de gestión de Riesgos de Seguridad Digital de su proceso teniendo en cuenta la metodología consignada en el M-OP-002 Manual para la gestión del riesgo en Transmilenio.
- Cumplir con las disposiciones normativas vigentes aplicables al Sistema de Gestión de Seguridad de la Información, así como a cualquier requerimiento de seguridad que se encuentre dentro del marco normativo que aplique a la entidad.
- Asegurar la privacidad y la protección de la información de datos personales que sea manejada por su proceso, como se exige en la legislación y la reglamentación vigente.
- Reportar los incidentes de seguridad siguiendo el procedimiento P-DT-020 Gestión de Incidentes de Seguridad de la Información, definido por la entidad y publicado respectivamente en la Intranet dentro del proceso de Gestión de TIC.

13. CULTURA Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

En el marco del proceso de Gestión del Talento humano, el cual tiene por objetivo “Garantizar la disponibilidad y competencia del recurso humano necesario para la operación de TRANSMILENIO”, la

entidad selecciona, vincula y evalúa a los servidores públicos con base en su educación, experiencia, formación y habilidades determinadas en el Manual especifico de funciones y competencias laborales adoptado por la Resolución No. 234 del 24 de mayo de 2017, Resolución No.661 del 27 de noviembre de 2017.

De la misma forma la entidad realiza evaluaciones de desempeño laboral y diagnóstico de necesidades de capacitación que permiten medir y analizar la gestión de la entidad para el mejoramiento continuo y la seguridad de la información, que a su vez son fuente para la elaboración anual del Cronograma de capacitación, entrenamiento y reentrenamiento. Lo anterior soportado en planes de sensibilización periódicos y el Plan estratégico institucional 2015, crean una entidad más efectiva y segura en la prestación del servicio público y fortalece el cumplimiento no solo de la misión institucional, sino también de la Política del SGSI.

En el marco del proceso de adquisición de bienes y servicios cuyo objeto es *"garantizar la compra u obtención correcta y oportuna de los bienes y servicios requeridos para la operación de TRANSMILENIO S.A.,* selecciona, vincula y evalúa el recurso humano (contratistas, proveedores y terceros) en función de los requisitos de educación, experiencia, formación y habilidades que se evalúan previo a la contratación, para la prestación de servicios profesionales y de apoyo.

Finalmente, como parte de las actividades de cultura y sensibilización TRANSMILENIO S.A. define su Plan de Cultura y Sensibilización, el cual contempla la estrategia que se aplica anualmente para sensibilizar a los usuarios de la Entidad en materia de Seguridad de la información a través de la divulgación de diferentes aspectos, entre otros, tales como Políticas de Seguridad, ingeniería social o Ciberseguridad.

14. MANTENIMIENTO Y MEJORA DEL SGSI

14.1 Medición de la eficacia del SGSI

Para evaluar el desempeño de la seguridad de la información y la eficacia del SGSI, la entidad ha definido diferentes Indicadores, los cuales se encuentran documentados en el indicador NASI – Nivel de Adopción de Seguridad de la Información, el cual forma parte integral de los Indicadores de Gestión de la Dirección de TIC. Así mismo, a través de la gestión de riesgos de seguridad, con cada valoración se identifican los controles a aplicar y se definen los Planes de Tratamiento que se implementarán, los cuales ayudarán a mitigar su materialización

14.2 Auditoría Interna

Con el propósito de verificar el cumplimiento del SGSI y el seguimiento a los compromisos derivados de este, la entidad llevará a cabo, por lo menos una vez al año, auditorías internas al Sistema de gestión de seguridad de la información, con el que se establecen los responsables y actividades para la planeación y la realización de las auditorias, que buscan verificar la adecuación, implementación y eficacia del SGSI y que contribuye en asegurar la eficiencia, eficacia y efectividad del mismo. Esta revisión podrá ser realizada por la Oficina de Control Interno, por un tercero o por quien sea designado al interior de la Entidad.

14.3 Revisión por la Dirección

La revisión por la Dirección tiene como finalidad asegurar la conveniencia, adecuación y eficacia del sistema, en donde se evalúan las oportunidades de mejora y la necesidad de realizar ajustes a la estructura o los lineamientos del SGSI. En TRANSMILENIO, S.A. en el marco del *Comité Institucional de Gestión y Desempeño, se* coordina y asegura que se realice como mínimo, una vez al año.

Dentro de los temas que se revisan por la dirección se encuentran:

- Riesgos de seguridad de la información y plan de tratamiento de riesgos
- Cumplimiento al PESI y su mapa de ruta
- Resultado de la medición de los indicadores de gestión de Seguridad de la Información
- Incidentes de seguridad de la información
- Resultados de las evaluaciones de auditoría
- Oportunidades de mejora y recomendaciones de seguridad.

14.4 Mejora del SGSI

A partir de hallazgos o situaciones de mejora identificadas por diferentes fuentes, tales como revisión por la dirección, resultados de indicadores, autocontrol, entre otros, la entidad aplica el procedimiento P-OP-017 Acciones correctivas, preventivas y de mejora del SIG.