PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI)

TRANSMILENIO



TABLA DE CONTENIDO

INTRODUCCIÓN 4
1. OBJETIVO 6
1.1. Objetivos específicos 6
2. ALCANCE DEL PESI 6
3. DEFINICIONES 7
4. DOCUMENTOS DE REFERENCIA 8
5. MARCO CONCEPTUAL DEL PESI 8
6. DESARROLLO DEL PESI 9
6.1. Metodología 9
6.2. Identificación del contexto 9
6.3. Situación Actual 10
6.4. Definición de iniciativas de seguridad de la información 15
6.5. Portafolio de proyectos 19
6.6. Alineación del PESI y PETI 22
6.7. Priorización de proyectos y mapa de ruta 23
6.7.1. Mapa de ruta de proyectos del PESI 24
7. CONCLUSIONES 25
8. ANEXOS 26

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Metodología Utilizada 9
Ilustración 2. Metodología utilizada para realizar el Autodiagnóstico 11
Ilustración 3. Diagrama de brechas tipo radar por Dominio (corte junio 2024) 12
Ilustración 4. Resultado grafico del cumplimiento ISO/IEC 27001:2013 Ciclo PHVA 14

ÍNDICE DE TABLAS

Tabla 1. Dominios del autodiagnóstico alineados con la Norma ISO/IEC 27001:2013 10
Tabla 2. Resultados por Dominio 13
Tabla 3.Iniciativas de Seguridad de la información frente a los objetivos estratégicos de Seguridad de la Información 16
Tabla 4. Portafolio de proyectos de Seguridad de la información. 20
Tabla 5. Objetivos PETI 22
Tabla 6. Alineación de objetivos del PESI con los objetivos PETI 23
Tabla 7. Criterio inicial para la priorización de los proyectos 24
Tabla 8. Mapa de Ruta de Proyectos del PESI (2022 – 2025) 24

MODIFICACIONES:

VERSIÓN	FECHA	CAMBIO	SOLICITÓ
0	26-jul-2018	Primera versión oficial del documento T-DT-006	No Aplica
1	05-jul-2022	Actualización del documento para el periodo 2022-2025. Se realiza el ajuste de la introducción y los objetivos estratégicos. En el capítulo 2. Alcance. Se amplia aclarando que el SGSI se implementa en los diferentes procesos o dependencias de la Entidad de manera progresiva según lo definido en el mapa de ruta de seguridad de la información Capítulo 3 Definiciones se eliminan los siguientes términos: Análisis de Riesgo, Guía y Parte Interesada. Capítulo 4. Documentos de Referencia: Se elimina la NTC/ISO 27005:2009 y la GTC-ISO 27002:2015 y se incorpora la Norma ISO/IEC 27002:2015 Capítulo 5. denominado Estructura Organizacional se cambia por Marco Conceptual del PESI. Capítulo 6 denominado Planeación del sistema de gestión de seguridad de la información se cambia por el titulo Desarrollo del PESI, y se modifica en su totalidad. Se eliminan las siguientes ilustraciones: No. 1. Mapa de procesos y alcance del SGSI, No. 2. Organigrama de TRANSMILENIO S. A., No. 3. Fases del ciclo PHVA, No. 4. Contesto interno y externo de TRANSMILENIO S. A. y No. 5. Plan Estratégico de Seguridad – PESI, Así mismo se eliminan las siguientes tablas: No.1 Análisis DOFA y No. 2 Partes Interesadas	Director de TIC

VERSIÓN	FECHA	CAMBIO	SOLICITÓ
2	Diciembre 2024	Se realizan los siguientes cambios: Capítulo 4. DOCUMENTOS DE REFERENCIA se incorpora los siguientes documentos referentes a normativas de gestión de riesgos y ciberseguridad: ISO/IEC 27001, ISO/IEC 27001:2022, ISO/IEC 27032:20234, ISOIEC 31000:2018, NIST SP800-53 y NIST Cybersecurity Framework (CSF) 2.0 Capítulo 6.3. Situación Actual, se agrega lo correspondiente al resultado del autodiagnóstico del año 2024. Se actualiza el numeral 6.3. Definición de iniciativas de seguridad de la información, en la que se adicionan las herramientas de señuelos y de monitoreo de red que son indispensables según los incidentes detectados durante los últimos 2 años. Se realizan ajustes de forma y redacción generales en varias secciones del documento.	Director de TIC

INTRODUCCIÓN

TRANSMILENIO S. A., como entidad pública de orden territorial, adscrita a la Secretaría 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 su misión, 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 (Resolución 500 de 2021), este último soportado por 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 controlar y administrar de forma segura la información.

TRANSMILENIO S. A. adopta una metodología para la identificación y valoración de los activos de información, así como una metodología para la evaluación y tratamiento de los riesgos de seguridad digital, 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 las 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. Todo lo anterior, apoyado en los programas de auditoría y la revisión por la dirección que concluyen en la identificación de oportunidades de mejora, que son gestionadas para mantener la mejora continua del SGSI.

Para tal fin, la Entidad ha adoptado los lineamientos normativos de la norma ISO/IEC 27001:2013 en proceso de transición a la ISO/IEC 27001:2022, la cual establece los requisitos para la implementación del SGSI, así como la norma ISO/IEC 31000:2018 que proporciona el esquema y

las mejores prácticas para la gestión de riesgos, en busca de mejorar el desempeño y la capacidad para prestar un servicio que responda a las necesidades y expectativas las partes interesadas.

Por otra parte, el presente documento hace parte integral del Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETI), el cual es el documento que expresa las intenciones de la organización en la implementación de iniciativas y acciones que promueven el uso de las Tecnologías de la Información y las Comunicaciones como contribución al logro de los objetivos y lineamientos estratégicos y que se encuentran enmarcados en el Plan Estratégico Institucional de la Entidad.

Finalmente, la adopción de la estrategia de seguridad digital en TRANSMILENIO S. A. se reforzó a través de la resolución 355 de 2022, “Por la cual se adopta el modelo de seguridad y privacidad de la información- MSPI como habilitador de la política de Gobierno Digital, la estrategia de seguridad digital para TRANSMILENIO S. A., así como los manuales requeridos para su implementación”. Dentro de esta resolución se contempla:

- Adoptar el Modelo de Seguridad y Privacidad de la información (MSPI)
- Adoptar la estrategia de seguridad digital orientada por el PESI
- Adoptar el Manual del Sistema de Gestión de seguridad de la información.
- Adoptar el Manual de Políticas de Seguridad y privacidad de la información
- Aplicación del Sistema de Gestión de Seguridad de la Información (SGSI)
- Análisis y tratamiento de riesgos de seguridad digital y controles
- Establecimiento del Plan de Cultura y sensibilización en seguridad digital
- Oficialización de la documentación asociada al SGSI
- Cumplimiento del Modelo de Seguridad y Privacidad de la Información– MSPI y la estrategia de seguridad digital

1. OBJETIVO

Definir el Plan Estratégico de Seguridad de la Información, en adelante "PESI" de TRANSMILENIO S. A., para el período comprendido entre los años 2022 - 2025, y que responda a las necesidades de preservación de la confidencialidad, integridad y la disponibilidad de la información.

1.1. Objetivos específicos

- Diseñar, comunicar e implementar la estrategia de adopción de seguridad de la información.
- Definir el mapa de ruta para la implementación del Plan Estratégico de Seguridad de la Información.
- Lograr incrementar el nivel de madurez en seguridad de la información a partir de la adopción del Modelo de Seguridad y Privacidad de la Información (MPSI).
- Asegurar los recursos de TI, de tal forma que se pueda soportar la continuidad de la prestación de los servicios.

2. ALCANCE DEL PESI

Teniendo en cuenta el análisis del contexto[1] interno y externo, así como las partes interesadas, TRANSMILENIO S. A. define el alcance de su Plan Estratégico de Seguridad de la Información como una alineación con el Sistema de Gestión de Seguridad de la Información (SGSI) de la siguiente manera:

- TRANSMILENIO S. A. adopta, establece, implementa, opera, verifica y mejora el SGSI para los procesos incluidos dentro de su alcance, los cuales se encuentran documentados dentro del M-DT-004 Manual del SGSI.
- El SGSI se implementa en los diferentes procesos o dependencias de la Entidad de manera progresiva según lo definido en el mapa de ruta de seguridad de la información, el cual es un anexo del presente documento.
- La Entidad, acorde con su naturaleza jurídica, misión y visión, encontró aplicables todos los requisitos y controles de la norma ISO/IEC 27001:2013, excluyendo el control A.11.1.6 Áreas de despacho y carga.

[1] Se aclara que el análisis de contexto interno y externo, así como toda la estructura de seguridad de la información se define y documenta dentro del manual M-DT-004 Manual 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 esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (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.

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.

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

- Norma ISO/IEC 27001:2013
- Norma ISO/IEC 27001:2022
- Norma ISO/IEC 27002:2015
- Norma ISO/IEC 27002:2022
- Norma ISO/IEC 27032:2023
- Norma ISOIEC 31000:2018
- Modelo de Seguridad y Privacidad de la Información – MSPI. MinTIC
- NIST SP800-53
- NIST Cybersecurity Framework (CSF) 2.0

5. MARCO CONCEPTUAL DEL PESI

El Plan Estratégico de Seguridad de la Información (PESI) es una herramienta que permite a TRANSMILENIO S. A. identificar, definir y planear la ejecución de un marco de actividades, que desde diferentes frentes, apoyan la adopción de la estrategia de seguridad de la información que soporta la misión de la Entidad. El PESI se soporta en el Plan Estratégico de Tecnologías de la información y las comunicaciones (PETI) que a su vez se soporta en el Plan Estratégico Institucional, y que alinea los objetivos estratégicos, que para el caso del presente plan, corresponden a los mencionados dentro del Plan Estratégico Institucional, Artículo Octavo, Quinto objetivo corporativo[2].

De igual forma, tal como ocurre con el Plan Estratégico Institucional y el PETI, lo definido dentro del PESI será monitoreado mediante actividades de seguimiento, con el fin de medir la adopción de las iniciativas y los proyectos que las enmarcan. Esto garantiza que se detecten desviaciones en el cumplimiento de los objetivos de control, políticas, medidas de seguridad tecnológicas entre otros que protegen la información de la Entidad.

En los siguientes numerales se describirá el desarrollo del PESI, donde se incluye su metodología, situación actual, análisis, definición de iniciativas, alineación con el PETI y estructuración de prioridades como un mapa de ruta. Todo lo anterior para la vigencia 2022-2025.

[2] https://www.transmilenio.gov.co/publicaciones/146045/plan_estrategico/

6. DESARROLLO DEL PESI

6.1. Metodología

La metodología utilizada para el desarrollo del PESI se muestra a continuación con cada una de sus fases:

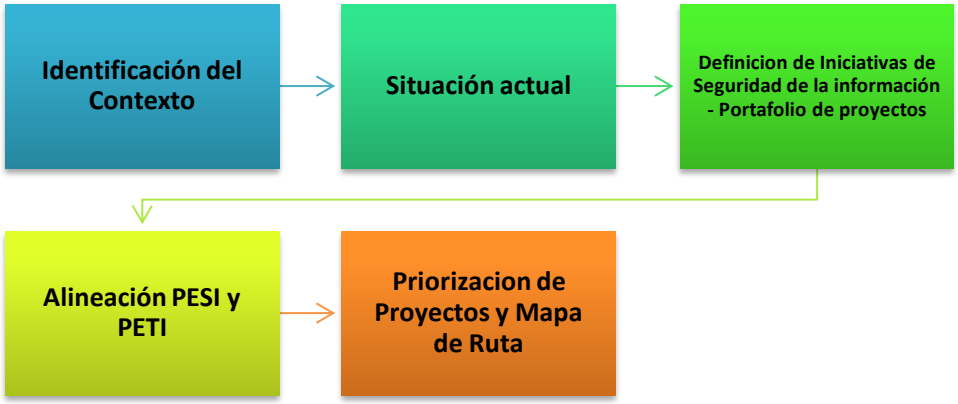


Ilustración 1. Metodología Utilizada

La metodología sigue el flujo preliminar de identificación del contexto y la situación actual en seguridad de la información en la Entidad. Con esta información se plantean las iniciativas y el portafolio de proyectos, así como su aplicación frente a los diferentes objetivos de seguridad de la información y su alineación con las definidas dentro del PETI. Con el resultado obtenido del análisis y la alineación se procede a establecer la priorización de los proyectos a corto, mediano y largo plazo, logrando establecer un mapa de ruta y las actividades a desarrollar de forma estratégica durante los siguientes 4 años.

En los numerales siguientes se abordan cada una de las fases de la metodología con el fin de lograr determinar la estrategia de seguridad de la información a adoptar por TRANSMILENIO S. A.

6.2. Identificación del 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. Cultura y valores
7. Legislación pertinente

Para llevar a cabo la identificación del contexto, la cual debe estar alineada con el Sistema de Gestión de Seguridad de la Información (SGSI), se tomó como base la identificación del contexto de la Entidad que se documentó previamente dentro del manual M-DT-004 Manual del SGSI. Este contexto corresponde al identificado durante finales del año 2021 y principios del 2022. Por lo tanto, consigna la información de contexto reciente desde diferentes aspectos, tales como el factor humano, tecnológico, ambiental, misional o de cumplimiento entre otros.

6.3. 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 la estimación del nivel de madurez se basa en las actividades para la ejecución del Autodiagnóstico del MSPI, el cual se aborda a través del diligenciamiento de un instrumento dispuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Este autodiagnóstico contempla la evaluación de los dominios de Seguridad de la Información alineados con la norma ISO/IEC 27001:2013. Estos dominios se presentan en la siguiente tabla:

Tabla 1. Dominios del autodiagnóstico alineados con la Norma ISO/IEC 27001:2013

Dominio Autodiagnóstico	Norma ISO/IEC 27001:2013
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

Por lo anterior, para lograr construir el PESI es indispensable contar con los niveles de madurez alcanzados en cada uno de los dominios a fin de plantear las prioridades sobre la implementación de controles que suplan las necesidades y mitiguen las brechas identificadas. Es importante aclarar que aunque actualmente existe la norma ISO/IEC 27001:2022, el MinTIC aún mantiene su documento de autodiagnóstico alineado con la norma ISO/IEC 27001:2013. Por lo tanto, la transición a esta versión se abordará como un proyecto dentro del PESI.

A continuación, se presenta la metodología para llevar a cabo el autodiagnóstico:

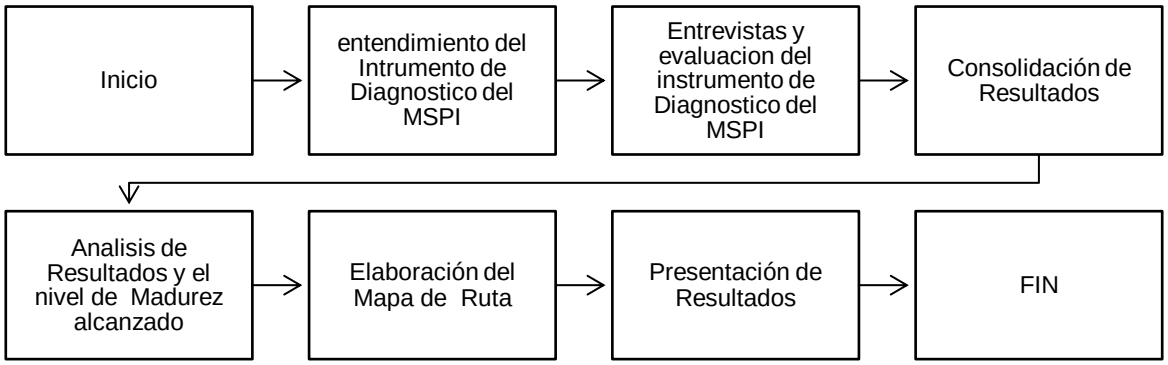


Ilustración 2. Metodología utilizada para realizar el Autodiagnóstico

Como resultado, el nivel de madurez permite establecer las bases para la mejora continua de la Seguridad de la Información de TRANSMILENIO S. A., e identificar las iniciativas en este campo, las cuales se alinean con las necesidades identificadas dentro del Plan Estratégico de Tecnologías de Información y las Comunicaciones (PETI). A continuación, se presenta el resultado del autodiagnóstico, por cada uno de los dominios a corte de junio 2024:



Ilustración 3. Diagrama de brechas tipo radar por Dominio (corte junio 2024)

Analizando el gráfico, se puede observar que los dominios con mayor nivel de madurez son el *A.5 Política de seguridad de la información* (Optimizado), y A.6 Organización de la Seguridad de la información (Optimizado), sin embargo, los dominios que se encuentran en un porcentaje entre 40 y 60, que son aquellos donde se deben enfocar los esfuerzos de mejora (en estado Repetible y Efectivo) son los siguientes:

- Criptografía (Repetible)

Como resumen, el nivel de madurez alcanzado por TRANSMILENIO S. A. está en **80%**, lo que significa que la Entidad en encuentra en un nivel Optimizado, los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. Existe formación y comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, pero podría existir la probabilidad de errores. Los controles son efectivos y se aplican constantemente. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo en algunos casos no es la indicada.

A continuación, se presenta la evaluación de efectividad de controles.

Tabla 2. Resultados por Dominio

No.	Evaluación de Efectividad de controles			
	Dominio	Calificación Actual	Calificación Objetivo	Evaluación de efectividad
A.5	Políticas de seguridad de la información	100	100	OPTIMIZADO
A.6	Organización de la seguridad de la información	88	100	OPTIMIZADO
A.7	Seguridad de los recursos humanos	88	100	OPTIMIZADO
A.8	Gestión de activos	82	100	OPTIMIZADO
A.9	Control de acceso	85	100	OPTIMIZADO
A.10	Criptografía	40	100	REPETIBLE
A.11	Seguridad física y del entorno	80	100	GESTIONADO
A.12	Seguridad de las operaciones	82	100	OPTIMIZADO
A.13	Seguridad de las comunicaciones	80	100	GESTIONADO
A.14	Adquisición, desarrollo y mantenimiento de sistemas	72	100	GESTIONADO
A.15	Relaciones con los proveedores	80	100	GESTIONADO
A.16	Gestión de incidentes de seguridad de la información	80	100	GESTIONADO
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	80	100	GESTIONADO
A.18	Cumplimiento	87,5	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		80	100	OPTIMIZADO

Nivel de cumplimiento Ciclo PHVA

De igual forma, como parte de la medición del Autodiagnóstico se realiza la evaluación del ciclo PHVA donde se evalúan los aspectos del ciclo PHVA del MSPI, los cuales están alineados con los requisitos de la norma ISO/IEC 27001:2013 a continuación se presentan los resultados del ciclo PHVA:

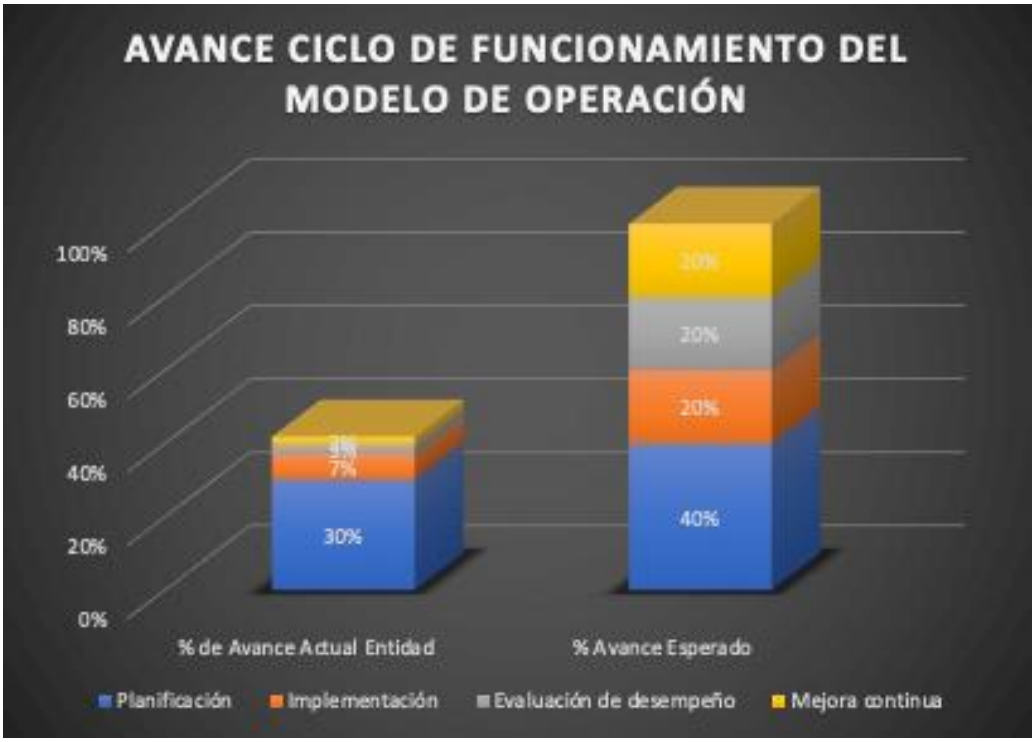


Ilustración 4. Resultado grafico del cumplimiento ISO/IEC 27001:2013 Ciclo PHVA

La ilustración anterior permite identificar que existen oportunidades de mejora con respecto a los requisitos (4 al 10) de la norma ISO/IEC 27001:2013 en cuanto a los aspectos de implementación, evaluación de desempeño y mejora continua. Por consiguiente, estos aspectos serán objeto de mejora y trabajo dentro de la hoja de ruta y mapa de proyectos para los siguientes 4 años.

Como resultado final de la revisión se identificó un porcentaje de cumplimiento del **42%** para el Ciclo PHVA, y de igual forma como se mencionó anteriormente, se identificó un cumplimiento del 80% en los dominios de control. Así mismo, en comparación con la evaluación realizada en el año 2018 se identificó un 17% en el ciclo PHVA y un 33% en los dominios de control, lo que permite determinar que hubo un incremento por encima del 50% en ambos frentes durante los 4 años. Por lo anterior, es perentorio que el portafolio de proyectos de seguridad de la información que se ejecutará durante el periodo objeto del presente PESI incluya un proyecto que permita el fortalecimiento y mejoramiento del sistema de gestión de seguridad de la información para TRANSMILENIO S. A., en donde se contemple el fortalecimiento de los aspectos de auditorías internas y mejora continua así como la documentación y medición de eficiencia de los controles pertenecientes a los dominios de control que se encuentran en estado repetible y efectivo.

6.4. Definición de iniciativas de seguridad de la información

Teniendo en cuenta el resultado anterior, se identificaron las iniciativas de seguridad de la información, las cuales se encuentran alineadas con el Plan Estratégico Institucional y con los resultados de la calificación obtenida en el autodiagnóstico del MSPI presentado anteriormente en la situación actual. Es importante aclarar que las iniciativas están enmarcadas dentro de los controles de seguridad 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 80%.

De igual forma, los objetivos estratégicos de seguridad de la información que se desean cumplir a través del PESI son:

- **Gobierno o Modelo de seguridad de información:** lograr desplegar un modelo de arquitectura de seguridad que permita gobernar los aspectos de seguridad de la información en TRANSMILENIO S. A.
- **Gestión de riesgos de Seguridad:** identificar y gestionar los riesgos de seguridad digital así como los planes de tratamiento de riesgos en las diferentes dependencias de TRANSMILENIO S. A. siguiendo los planes progresivos de incorporación dentro del SGSI.
- **Desarrollo y gestión del programa de seguridad de la información:** estructurar un programa de seguridad de la información que brinde la ruta para adoptar las diferentes iniciativas al interior de la Entidad e incluya los aspectos de mejora continua en seguridad digital.
- **Gestión de incidentes de seguridad de la información:** fortalecer la estrategia de gestión de incidentes de seguridad digital, de tal forma que se mejore la detección y corrección de eventos e incidentes que afecten la confidencialidad, integridad y disponibilidad de la información.

De acuerdo con lo anterior, a continuación, se presentan las iniciativas y su alineación con los objetivos estratégicos de seguridad de la información.

Tabla 3.Iniciativas de Seguridad de la información frente a los objetivos estratégicos de Seguridad de la Información

INICIATIVAS	DESCRIPCIÓN 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 para incluir y ajustar los aspectos identificados como mejora en los últimos 4 años y con una visión estratégica para el siguiente periodo. Estas políticas buscan abordar temas en profundidad como el teletrabajo, el trabajo remoto, el uso de la nube, los aspectos de ciberseguridad y tecnologías de la Entidad que facilitan el trabajo.	X			
I.02	Definir e implementar la arquitectura de seguridad para la Entidad, tomando como base el Modelo de Arquitectura Empresarial (MAE) u otras metodologías.	X			
I.03	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 de cualquier proyecto de tecnología o gestión de información en la Entidad.	X			
I.04	Diseñar y documentar un plan anual de cultura y sensibilización en Seguridad de la Información para funcionarios, contratistas proveedores y terceros de TRANSMILENIO S. A.	X			

INICIATIVAS	DESCRIPCIÓN 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	Aplicar la gestión de activos de información en cada uno de los procesos o dependencias de la Entidad de acuerdo con la incorporación progresiva dentro del SGSI. Esta iniciativa busca consolidar toda la información de activos y su valoración dentro de la herramienta de SGSI.			X	
I.06	Aplicar la gestión de riesgos de seguridad digital para cada uno de los procesos o dependencias que se incorporen progresivamente dentro del SGSI. Incluyendo la gestión del plan de tratamiento de riesgos.		X		
I.07	Diseñar y documentar las pruebas al plan de recuperación de desastres, ante escenarios de fallas de las tecnologías, garantizando que se mantengan los controles de seguridad.	X		X	
I.08	Definir y establecer y adoptar la metodología de desarrollo seguro alineada con estándares internacionales de desarrollo seguro, así como adoptarla por las áreas de desarrollo de software de la Entidad.			X	
I.09	Definir y establecer la estrategia de gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos, etc.), así como a las funciones de negocio que requieren el uso de privilegios.			X	

INICIATIVAS	DESCRIPCIÓN 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.10	Implementar la gestión centralizada de usuarios para todos los aplicativos del negocio. Esto contempla la solución de gestión de identidades y de usuarios privilegiados al interior de la Entidad.			X	
I.11	Aplicar la gestión de seguridad de la información en los proveedores, con el fin de verificar que los controles de seguridad, los acuerdos de servicio definidos y demás requerimientos de seguridad que se exigen en los contratos están siendo implementados, operados y mantenidos.			X	
I.12	Implementar una solución de borrado seguro de información así como establecer los lineamientos de aplicación de esta solución en la Entidad.				X
I.13	Establecer e implementar una solución de gestión de vulnerabilidades tanto a nivel de infraestructura como a nivel de aplicaciones web.				X
I.14	Realizar pruebas de Hacking Ético sobre la infraestructura tecnológica de la Entidad.				X
I.15	Implementar una solución que permita la transferencia segura de archivos, mediante protocolos de cifrado.			X	
I.16	Implementar una solución de DLP (Data Loss Prevention), con el fin de controlar y monitorear el intercambio de información confidencial y/o sensible.			X	

INICIATIVAS	DESCRIPCIÓN 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.17	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web.			X	
I.18	Implementar herramientas de seguridad para monitorear el comportamiento de activos de información críticos. Estas herramientas se pueden enmarcar en soluciones de SIEM, Inteligencia artificial, señuelos o monitoreo de disponibilidad entre otros.				X
I.19	Operar y mantener el Sistema de Gestión de Seguridad de la Información (SGSI) a través de una transición a la ISO/IEC 27001:2022, un mapa de ruta y su seguimiento periódico por el grupo de seguridad de la Información.			X	
I.20	Asegurar el uso y adaptación y entornos de computación en la nube.			X	
I.21	Mejorar los indicadores del sistema de gestión de seguridad de la información (SGSI).	X			

6.5. Portafolio de proyectos

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 4. Portafolio de proyectos de Seguridad de la información.

PROYECTO	DESCRIPCIÓN DEL PROYECTO	INICIATIVA	DESCRIPCIÓN DE LA INICIATIVA	ESTADO	¿REQUIERE RECURSOS FINANCIEROS?
P01	Arquitectura de Seguridad dentro del marco de Arquitectura Empresarial.	I.01	Actualizar el manual de políticas de seguridad y privacidad de la información para incluir y ajustar los aspectos identificados como mejora en los últimos 4 años y con una visión estratégica para el siguiente periodo. Estas políticas buscan abordar temas en profundidad como el teletrabajo, el trabajo remoto, el uso de la nube y tecnologías de la Entidad que facilitan el trabajo.	NO INICIADO	NO
		I.02	Definir e implementar la arquitectura de seguridad para la Entidad, tomando como base el Modelo de Arquitectura Empresarial (MAE) u otras metodologías.		
P02	Seguridad de la Información en la gestión de proyectos y proveedores	I.03	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 de cualquier proyecto de tecnología o gestión de información en la Entidad.	INICIADO	NO
		I.11	Aplicar la gestión de seguridad de la información en los proveedores, con el fin de verificar que los controles de seguridad, los acuerdos de servicio definidos y demás requerimientos de seguridad que se exigen en los contratos están siendo implementados, operados y mantenidos.		
P03	Sensibilización en Seguridad de la Información	I.04	Diseñar y documentar un plan anual de cultura y sensibilización en Seguridad de la Información para funcionarios, contratistas proveedores y terceros de TRANSMILENIO S. A.	INICIADO	NO
P04	Gestión de riesgos de seguridad digital en los activos críticos de la Entidad.	I.05	Aplicar la gestión de activos de información en cada uno de los procesos o dependencias de la Entidad de acuerdo con la incorporación progresiva dentro del SGSI. Esta iniciativa busca consolidar toda la información de activos y su valoración dentro de la herramienta de SGSI.	INICIADO	NO
		I.06	Aplicar la gestión de riesgos de seguridad digital para cada uno de los procesos o dependencias que se incorporen progresivamente dentro del SGSI. Incluyendo la gestión del plan de tratamiento de riesgos.		
P05	Adopción de la Recuperación de desastres	I.07	Diseñar y documentar las pruebas al plan de recuperación de desastres, ante escenarios de fallas de las tecnologías, garantizando que se mantengan los controles de seguridad.	INICIADO	SI

PROYECTO	DESCRIPCIÓN DEL PROYECTO	INICIATIVA	DESCRIPCIÓN DE LA INICIATIVA	ESTADO	¿REQUIERE RECURSOS FINANCIEROS?
P06	Seguridad en Desarrollo de software	I.08	Definir y establecer y adoptar la metodología de desarrollo seguro alineada con estándares internacionales de desarrollo seguro, así como adoptarla por las áreas de desarrollo de software de la Entidad.	INICIADO	SI
P07	Gestión de Identidades y de usuarios privilegiados	I.09	Definir y establecer la estrategia de gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos, etc.), así como a las funciones de negocio que requieren el uso de privilegios.	NO INICIADO	SI
		I.10	Implementar la gestión centralizada de usuarios para todos los aplicativos del negocio. Esto contempla la solución de gestión de identidades y de usuarios privilegiados al interior de la Entidad.		
P08	Borrado seguro de equipos	I.12	Implementar una solución de borrado seguro de información, así como establecer los lineamientos de aplicación de esta solución en la Entidad.	NO INICIADO	SI
P09	Gestión de vulnerabilidades y Ethical hacking	I.13	Establecer e implementar una solución de gestión de vulnerabilidades tanto a nivel de infraestructura como a nivel de aplicaciones web.	INICIADO	SI
		I.14	Realizar pruebas de Hacking Ético sobre la infraestructura tecnológica de la Entidad.		
P10	SEGURIDAD EN LA transferencia de información	I.15	Implementar una solución que permite la transferencia segura de archivos, mediante protocolos de cifrado.	NO INICIADO	SI
		I.16	Implementar una solución de DLP (Data Loss Prevention), con el fin de controlar y monitorear el intercambio de información confidencial y/o sensible.		
P11	Firewall de aplicaciones (WAF)	I.17	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web.	NO INICIADO	SI
P12	Monitoreo de Seguridad	I.18	Implementar herramientas de seguridad para monitorear el comportamiento de activos de información críticos. Estas herramientas se pueden enmarcar en soluciones de SIEM, Inteligencia artificial, señuelos o monitoreo de disponibilidad entre otros.	INICIADO	SI
P13	Gestión del SGSI	I.19	Operar y mantener el Sistema de Gestión de Seguridad de la Información (SGSI) a través de una transición a la ISO/IEC 27001:2022, un mapa de ruta y su seguimiento periódico por el grupo de seguridad de la Información.	INICIADO	SI
P14	Aseguramiento de información	I.20	Asegurar el uso y adaptación y entornos de computación en la nube.	INICIADO	SI

PROYECTO	DESCRIPCIÓN DEL PROYECTO	INICIATIVA	DESCRIPCIÓN DE LA INICIATIVA	ESTADO	¿REQUIERE RECURSOS FINANCIEROS?
P15	Mejora continua	I.21	Mejorar los indicadores del sistema de gestión de seguridad de la información (SGSI).	INICIADO	NO

6.6. Alineación del PESI y PETI

La alineación del PESI con el PETI busca sincronizar los objetivos estratégicos de TI (PETI), 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, con los objetivos del PESI, que permiten asegurar la confidencialidad, integridad y disponibilidad de los activos de información. Para realizar esta alineación, a continuación, se presentan los objetivos de TI que están directamente involucrados en el plan estratégico de Seguridad de la Información.

Tabla 5. Objetivos PETI

ID	Objetivo PETI
1.	Administrar los esquemas de almacenamiento bajo los estándares de seguridad y mantenerlos disponibles para la utilización de los usuarios.
2.	Optimizar el escenario del sistema de gestión de seguridad de la información en la entidad alineado a los retos operativos como a los asociados a los retos estratégico-misional enmarcados en el nuevo SIR.
3.	Mantener una infraestructura tecnológica actualizada y disponible de hardware y software al servicio de funcionarios y colaboradores de la Entidad.
4.	Liderar la implementación de la estrategia de Seguridad y Privacidad de la Información en la Entidad, de acuerdo con los lineamientos de la política de Gobierno Digital con el fin de disminuir la probabilidad de ocurrencia de incidentes de seguridad de la información a partir de la aplicación eficaz de la gestión del riesgo.
5.	Apoyar técnicamente el desarrollo de la estrategia de gestión de la información, con el fin de garantizar su seguridad, calidad, clasificación y completitud, para su aprovechamiento en la toma de decisiones.
6.	Participar en la construcción y despliegue de los planes de continuidad de negocio y de recuperación de desastres, en lo relacionado con el componente tecnológico y sus estrategias de recuperación de los servicios, lo anterior acorde con las fases definidas en TRANSMILENIO S. A.

Los anteriores objetivos del PETI, están relacionados con el Sistema de Gestión de Seguridad de la Información (SGSI).

Tabla 6. Alineación de objetivos del PESI con los objetivos PETI

ID	Objetivo del PESI	ID	Objetivo PETI
1	Gobierno o Modelo de seguridad de información: Lograr desplegar un modelo de arquitectura de seguridad que permita gobernar los aspectos de seguridad de la información en TRANSMILENIO S. A.	2	Optimizar el escenario del sistema de gestión de seguridad de la información en la entidad alineado a los retos operativos como a los asociados a los retos estratégico-misional enmarcados en el nuevo SIR
2	Gestión de riesgos de Seguridad: Identificar y gestionar los riesgos de seguridad digital así como los planes de tratamiento de riesgos en las diferentes dependencias de TRANSMILENIO S. A. siguiendo los planes progresivos de incorporación dentro del SGSI.	5	Apoyar técnicamente el desarrollo de la estrategia de gestión de la información, con el fin de garantizar su seguridad, calidad, clasificación y completitud, para su aprovechamiento en la toma de decisiones
3	Desarrollo y gestión del programa de seguridad de la información. Estructurar un programa de seguridad de la información que brinde la ruta para adoptar las diferentes iniciativas al interior de la Entidad e incluya los aspectos de mejora continua en seguridad digital.	3	Mantener una infraestructura tecnológica actualizada y disponible de hardware y software al servicio de funcionarios y colaboradores de la Entidad
		1	Administrar los esquemas de almacenamiento bajo los estándares de seguridad y mantenerlos disponibles para la utilización de los usuarios.
		4	Liderar la implementación de la estrategia de Seguridad y Privacidad de la Información en la Entidad, de acuerdo con los lineamientos de la política de Gobierno Digital con el fin de disminuir la probabilidad de ocurrencia de incidentes de seguridad de la información a partir de la aplicación eficaz de la gestión del riesgo
4	Gestión de incidentes de seguridad de la información: Fortalecer la estrategia de gestión de incidentes de seguridad digital, de tal forma que se mejore la detección y corrección de eventos e incidentes que afecten la confidencialidad, integridad y disponibilidad de la información.	6	Participar en la construcción y despliegue de los planes de continuidad de negocio y de recuperación de desastres, en lo relacionado con el componente tecnológico y sus estrategias de recuperación de los servicios, lo anterior acorde con las fases definidas en TRANSMILENIO S. A.

6.7. Priorización de proyectos y mapa de ruta

Una vez identificado el resultado del Autodiagnóstico del MSPI, el planteamiento de las iniciativas y los proyectos de Seguridad de la información que abordan las iniciativas es necesario establecer la priorización de cada proyecto. Para esto, se definió como primer criterio la prioridad en los objetivos estratégicos de seguridad de la información, los cuales a su vez extienden dicha prioridad a las respetivas iniciativas que fueron alineadas con cada uno. Por lo anterior, el orden quedaría establecido de la siguiente forma:

Tabla 7. Criterio inicial para la priorización de los proyectos

Prioridad	Objetivos estratégicos de Seguridad de la Información (PESI)
1	Gobierno o Modelo de seguridad de información: Lograr desplegar un modelo de arquitectura de seguridad que permita gobernar los aspectos de seguridad de la información en TRANSMILENIO S. A.
2	Gestión de riesgos de Seguridad: Identificar y gestionar los riesgos de seguridad digital así como los planes de tratamiento de riesgos en las diferentes dependencias de TRANSMILENIO S. A. siguiendo los planes progresivos de incorporación dentro del SGSI.
3	Gestión de incidentes de seguridad de la información: Fortalecer la estrategia de gestión de incidentes de seguridad digital, de tal forma que se mejore la detección y corrección de eventos e incidentes que afecten la confidencialidad, integridad y disponibilidad de la información.
4	Desarrollo y gestión del programa de seguridad de la información. Estructurar un programa de seguridad de la información que brinde la ruta para adoptar las diferentes iniciativas al interior de la Entidad e incluya los aspectos de mejora continua en seguridad digital.

6.7.1. Mapa de ruta de proyectos del PESI

A continuación, se presenta el mapa de ruta de proyectos del PESI de acuerdo con la prioridad de los proyectos, los cuales se han venido desarrollando a partir de la vigencia 2022 y hasta la vigencia 2025 así.

Tabla 8. Mapa de Ruta de Proyectos del PESI (2022 – 2025)

PROYECTO	DESCRIPCIÓN DEL PROYECTO	INICIATIVA	RESUMEN INICIATIVA	2022	2023	2024	2025
P01	Arquitectura de Seguridad dentro del marco de Arquitectura Empresarial.	I.01	Actualizar el manual de políticas de seguridad y privacidad.	X			
		I.02	Definir e implementar la arquitectura de seguridad.	X			
P02	Seguridad de la Información en la gestión de proyectos y proveedores	I.03	Seguridad de la información en el ciclo de vida de los proyectos.	X	X	X	X
		I.11	Gestión de seguridad de la información en los proveedores.	X	X	X	X
P03	Sensibilización en Seguridad de la Información	I.04	Plan anual de cultura y sensibilización en Seguridad.	X	X	X	X
P04	Gestión de riesgos de seguridad digital en los activos críticos de la Entidad.	I.05	Gestión de activos de información.	X	X	X	X
		I.06	Gestión de riesgos de seguridad digital.	X	X	X	X
P05	Adopción de la Recuperación de desastres	I.07	Plan de recuperación de desastres.	X	X		

PROYECTO	DESCRIPCIÓN DEL PROYECTO	INICIATIVA	RESUMEN INICIATIVA	2022	2023	2024	2025
P06	Seguridad en Desarrollo de software	I.08	Metodología de desarrollo seguro.		X		
P07	Gestión de Identidades y de usuarios privilegiados	I.09	Estrategia de gestión de usuarios privilegiados.			X	
		I.10	Gestión centralizada de usuarios			X	
P08	Borrado seguro de equipos	I.12	Solución de borrado seguro.				X
P09	Gestión de vulnerabilidades y Ethical hacking	I.13	Solución de gestión de vulnerabilidades.		X		
		I.14	Hacking Ético.	X	X	X	X
P10	Seguridad en la transferencia de información	I.15	Solución de transferencia segura de archivos.				X
		I.16	Solución de DLP.				X
P11	Firewall de aplicaciones (WAF)	I.17	Firewall de aplicaciones Web.		X		
P12	Monitoreo de Seguridad	I.18	Herramienta SIEM, señuelos, monitoreo de red con inteligencia artificial.		X	X	
P13	Gestión del SGSI	I.19	Sistema de Gestión de Seguridad de la Información (SGSI) como una transición a la ISO/IEC 27001:2022.	X	X	X	X
P14	Aseguramiento de información	I.20	Asegurar entornos de computación en la nube.	X			
P15	Mejora continua	I.21	Indicadores del SGSI.		X	X	X

7. CONCLUSIONES

El presente plan parte de la identificación del estado actual en seguridad de la información que actualmente tiene la Entidad, dentro del cual se identificaron las brechas y puntos débiles que deben mejorarse para lograr alcanzar el estado “Optimizado” de los controles.

Por lo anterior, las iniciativas y proyectos se definieron teniendo en cuenta dichos puntos débiles, así como su capacidad de implementación durante la vigencia del mismo.

Para lograr lo antes expuesto y teniendo en cuenta que es importante contar con el apoyo y la aprobación de la Alta Dirección de TRANSMILENIO S. A. así como con el compromiso de todas las áreas involucradas en el proceso, la Entidad ha expedido la resolución 355 de 2022 que oficializa la adopción de la estrategia de seguridad a través de diferentes documentos y procesos que permiten mitigar las brechas identificadas. Esta resolución se alinea totalmente con el presente plan toda vez que se soporta en los lineamientos de la política de gobierno digital y la resolución 500 de 2021 emitida por el Ministerio de Tecnología y las Comunicaciones (MinTIC). Por lo anterior, la ejecución

del PESI facilitará el cumplimiento a las políticas ya definidas, así como de los requisitos establecidos por el gobierno colombiano.

8. ANEXOS

Anexo 1. Mapa de Ruta de Proyectos del PESI