ESTUDIO DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA TRANSMILENIO S.A., ACORDE A LA NORMA ISO/IEC 27001 VERSIÓN 2013

NICOLÁS QUINTERO AMAYA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
BOGOTÁ 2017

ESTUDIO DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA TRANSMILENIO S.A., ACORDE A LA NORMA ISO/IEC 27001 VERSIÓN 2013

NICOLÁS QUINTERO AMAYA

Trabajo de grado

Director:
LUIS FERNANDO ZAMBRANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
BOGOTÁ 2017

Nota de aceptación

_____

_____

_____

_____

_____

Firma del Director

_____

Firma del Asesor

_____

Firma del Jurado

Bogotá, 5 de Marzo de 2018

CONTENIDO

Pág.

TABLAS

Pág.

ANEXOS

Pág.

INTRODUCCIÓN

Debido a los avances tecnológicos la información de las empresas se ha convertido en uno de sus activos más importantes, teniendo en cuenta que se debe proteger al mayor nivel posible la seguridad, para garantizar la confidencialidad, disponibilidad e integridad.

La información de las empresas se maneja mediante diferentes formatos como archivo, correspondencia, sistemas de información, correo electrónico, bases de datos, etc. Empresas como TRANSMILENIO S.A., según el decreto 2573 de 2014 [1], deben cumplir con el componente de Seguridad y Privacidad de la Información, debido a que tratan información pública y privada, para de esta forma protegerse ante posibles amenazas de pérdida de información o acceso abusivo y daño de sus sistemas informáticos. Por lo cual surge la necesidad de implementar un modelo de seguridad de la información o medidas informáticas que permita prevenir y controlar estas insolvencias.

Con el desarrollo de este proyecto se pretende contribuir a que TRANSMILENIO S.A. cumpla con los lineamientos de Gobierno en línea, en cuanto al tema de la seguridad informática, ya que por ser una entidad del distrito está obligada a implementar un modelo que involucre el análisis de riesgos, las políticas de seguridad, controles, auditorías y las responsabilidades de todos los funcionarios de la empresa. Para le ejecución, se hará un reconocimiento de la entidad, sus objetivos, el análisis de riesgos a través de las vulnerabilidades encontradas, conocer sus fortalezas y debilidades, con el fin de encaminarla hacia la creación de controles adecuados y normalizados.

[1] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. 2014. *Decreto Número 2573.* Bogotá, D.C. : MinTic, 2014. págs. p.9. Disponible en: http://www.mintic.gov.co/portal/604/articles-14673_documento.pdf, Decreto Nacional.

1. PLANTEAMIENTO DEL PROBLEMA

La tecnología avanza a pasos agigantados y cada vez más las empresas se ven en la necesidad de manejar gran cantidad de información en diferentes formatos pero principalmente en medios electrónicos y con acceso a la red de internet, lo cual hace que su seguridad sea más vulnerable y obliga a las empresas a invertir gran cantidad de dinero y esfuerzos para salvaguardarla.

La información en las organizaciones se ve diariamente expuesta a una serie de amenazas que pueden ser muy leves o peligrosas, lo que puede llevar a la empresa a tener pérdidas económicas incalculables. Transmilenio S.A., por el gran volumen de información que maneja diariamente, como es el control de flota y el sistema de recaudo que llega a registrar transacciones por más de 5 mil millones diarios[2], le puede perjudicar gravemente cualquier falla en la seguridad de la información.

Transmilenio S.A. es una empresa pública del Distrito y se debe regir bajo los estándares de seguridad de la información del MINTIC, de acuerdo a la estrategia de Gobierno en Línea, según lo establecido en el documento Conpes 3854[3] y el decreto número 2573 de 2014[1].

¿El análisis de riesgos a los activos de información de la empresa Transmilenio S.A. permitirá reducir los ataques informáticos a la organización?

---

[2] COLOMBIA. CONTRALORÍA DE BOGOTÁ. 2016. *Informe de Auditoría de Desempeño PAD 2016 (RECAUDO) EMPRESA TRANSMILENIO S.A.* Contraloría de Bogotá. Bogotá, D.C. : s.n., 2016. p.1-50. Disponible en: http://www.transmilenio.gov.co/Publicaciones/contraloria_de_bogota_informe_de_auditoria_de_desempeno_pad_2016_recaudo, Informe resultados auditoría.

[3] COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN y CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. 2016. *Documento CONPES 3854 Política Nacional de Seguridad Digital.* CONPES. Bogotá, D.C. : s.n., 2016. págs. P.1-91. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

2. OBJETIVOS

2.1 Objetivo General

Realizar un estudio de seguridad de la información para la empresa Transmilenio S.A. de acuerdo a la norma ISO/IEC 27001 versión 2013, según los lineamientos de la Estrategia de Gobierno en Línea.

2.2 Objetivos Específicos

Realizar el levantamiento de la información a través metodologías de análisis y gestión de riesgos, normatividad, técnicas de pentesting, del estado actual de la seguridad de la empresa Transmilenio.

Determinar y aplicar las metodologías de análisis y gestión de riesgos en la empresa Transmilenio S.A.

Elaborar la propuesta de solución de seguridad para la empresa Transmilenio S.A., con base a la norma ISO/IEC 27001 versión 2013, de acuerdo a lo requerido por la Estrategia de Gobierno en Línea.

3. SITUACIÓN ACTUAL DE LA EMPRESA

Empresa: TRANSMILENIO S.A.

Actividad económica: Transporte Masivo Urbano de pasajeros

3.1 Reseña Histórica

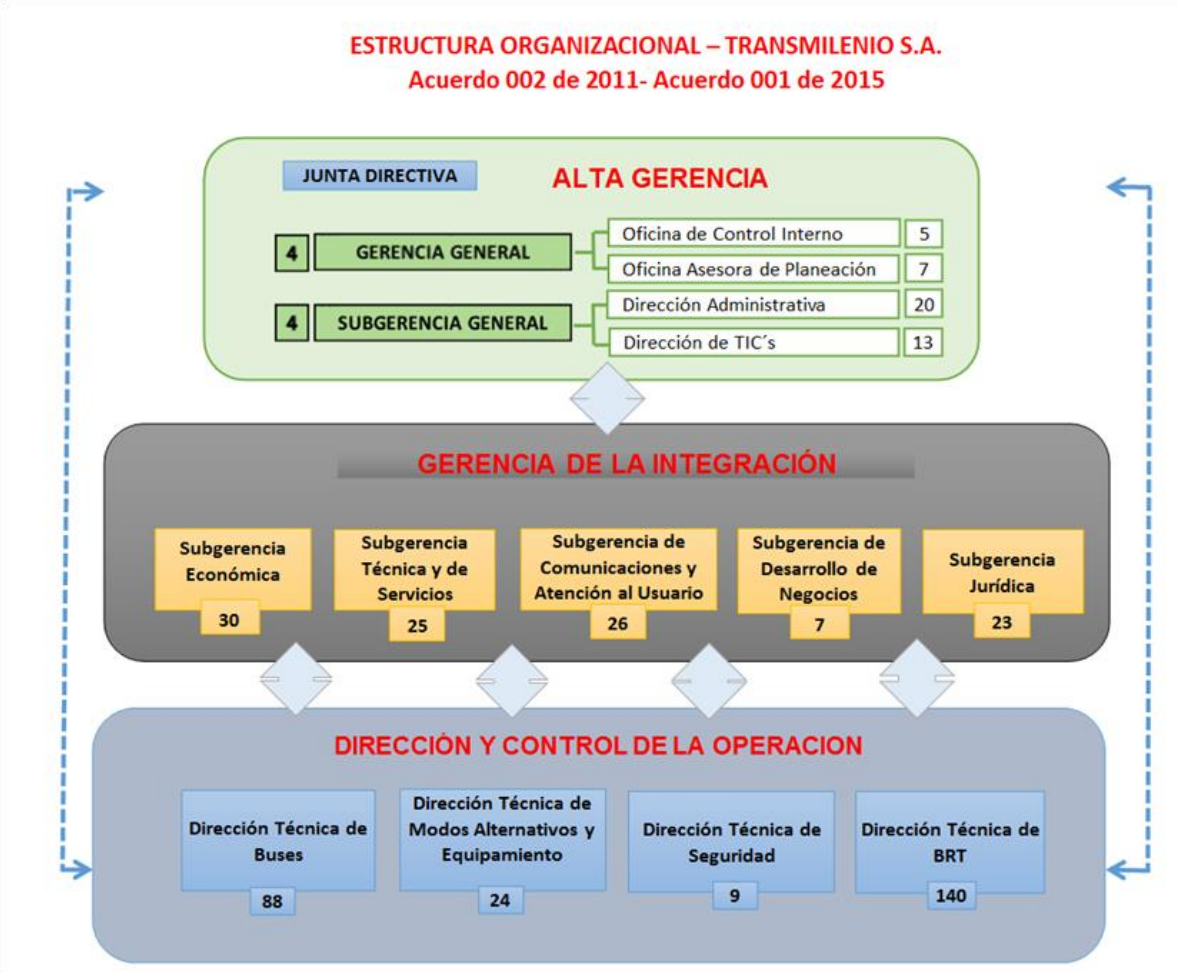
TRANSMILENIO S.A. fue creada mediante acuerdo 04 de 1999[4], que autorizó al alcalde mayor, en representación de Bogotá D.C., para participar conjuntamente con otras entidades del orden distrital en la constitución de la Empresa de Transporte de Tercer Milenio, TRANSMILENIO S.A., dada el 13 de octubre de 1999 como sociedad por acciones, bajo la forma de sociedad anónima de carácter comercial con aportes públicos. Esto con el fin de dar respuesta a la solución del problema de transporte público que enfrentaba la ciudad en ese momento y que el alcalde incluyó en su programa de gobierno como proyecto prioritario. TRANSMILENIO S.A. es el ente gestor del Sistema, la entidad encargada de coordinar los diferentes actores, planear, gestionar y controlar la prestación del servicio público de transporte masivo urbano de pasajeros, y tiene la responsabilidad de la prestación eficiente y permanente del servicio. Es así como el 18 de diciembre de 2000, se inauguró la primera ruta que comenzó a operar con 14 buses entre las calles ochenta y sexta por la troncal de la Caracas. Durante este período se entregaron las troncales: Autonorte, Calle 80 y Caracas, posteriormente se construyeron las troncales Américas, NQS, Avenida Suba, Avenida Eldorado y la Carrera 10ª. Adicionalmente se amplió la QNS Sur hasta el municipio de Soacha. Actualmente Transmilenio moviliza alrededor de 2.5 millones[5] de personas diariamente y la demanda de pasajeros sigue en aumento.

---

[4] COLOMBIA, CONCEJO DE BOGOTÁ D.C. 1999. *Acuerdo 004 de 1999. Por el cual se autoriza al Alcalde Mayor en representación del Distrito Capital para participar, conjuntamente con otras entidades del orden Distrital, en la Constitución de la Empresa de Transporte del Tercer Milenio - Transmilenio S.* Bogotá, D.C. : Concejo de Bogotá, 1999. pág. p.1. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=892, Acuerdo municipal.

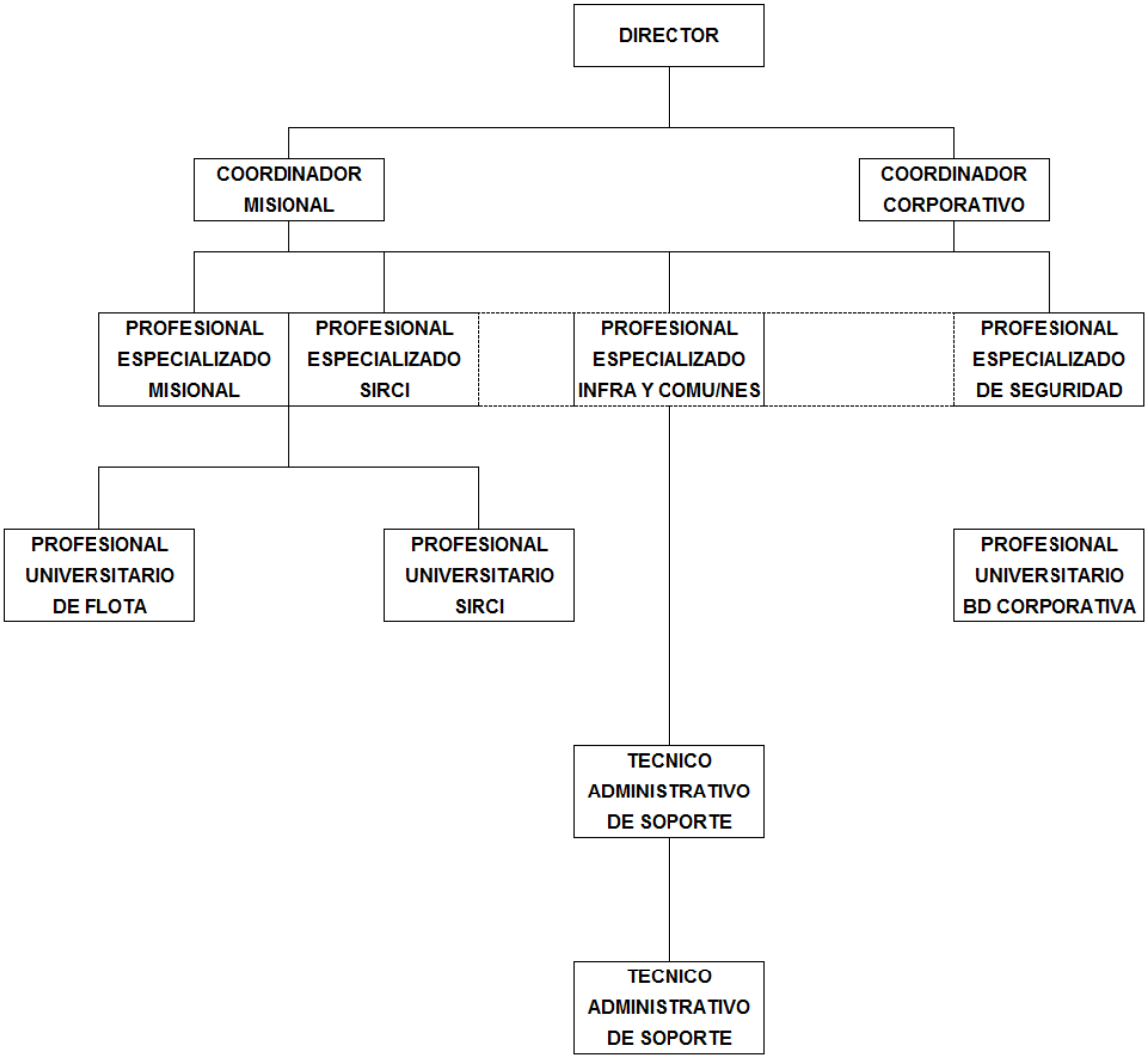
[5] COLOMBIA.CONTRALORÍA DE BOGOTÁ, D.C. 2017. *Informe de Auditoría de regularidad empresa TRANSMILENIO S.A.* Bogotá, D.C.Disponible en: http://www.transmilenio.gov.co/loader.php?lServicio=Publicaciones&lTipo=WFactionA&lFuncion=visualizar&id=14341&bd=m : s.n., 2017. pág. p.237, Informe resultados auditoría.

Fig. 1. Organigrama de TRANSMILENIO S.A.



Fuente: TRANSMILENIO S.A, (2013).

Fig. 2. Organigrama de la Dirección de TIC's



Fuente: ÁREA DE SEGURIDAD DE LA INFORMACIÓN DE TRANSMILENIO, (2017)

3.2 Objetivos de la Dirección de TIC's

La Dirección de Tecnologías de la Información y Comunicaciones tiene como objeto la gestión, planeación, mantenimiento y soporte de TIC's para la Empresa y la interlocución técnica con los diferentes agentes del sistema en los temas de materia tecnológica y de comunicaciones[6].

[6] Ibíd.

3.3 Cargos y Funciones de la Dirección de TIC's

3.3.1 Coordinador de Procesos Corporativos

Coordinar los procesos corporativos relacionados con las tecnologías de la información y las comunicaciones de TRANSMILENIO S.A., de conformidad con las políticas y normatividad vigente.

Funciones del cargo: [7]

- Planear, formular, coordinar y dirigir el avance de planes, programas y todos los procedimientos relacionados con la informática y que apoyan los procesos operativos-administrativos.

- Diseñar y coordinar programas de mantenimiento de la infraestructura de hardware, software y comunicaciones de la empresa, de acuerdo con estándares y normas de calidad y de seguridad vigentes.

- Coordinar el desarrollo e implementación de las políticas y normas de seguridad informática, de acuerdo con los lineamientos establecidos.

- Supervisar la correcta aplicación de los mecanismos y normas para el control de la legalidad y el respeto a los derechos de autos de software en los procesos corporativos, conforme a las normas concordantes.

- Coordinar las actividades relacionadas con la elaboración, implementación y ejecución de los planes de contingencia y seguridad informática de la empresa, de acuerdo con las políticas y normas de seguridad informática.

- Generar lineamientos para la atención de la mesa de ayuda corporativa en la que se administra el soporte técnico de TICs, con criterios de eficiencia, calidad y oportunidad.

[7] TRANSMILENIO S.A.. 2017. *Resolución 234 de 2017. Manual de Funciones Trabajadores Oficiales.* Transmilenio. Bogotá, D.C. : s.n., 2017. Información proporcionada por la empresa directamente.

- Coordinar la atención y búsqueda de soluciones a los requerimientos de los entes de control relacionados con las tecnologías de la información y las comunicaciones – TICs, y los requerimientos puestos a través de la mesa de ayuda corporativa, con criterios de eficiencia, calidad y oportunidad.

- Coordinar, controlar y hacer seguimiento del plan de contratación de la dirección de TICs, de acuerdo con los lineamientos establecidos.

- Supervisar los procesos de suministros de tecnologías de la información a servidores y/o contratistas para la correcta ejecución de sus labores, acorde con los procedimientos establecidos.

- Participar en la estructuración de proyectos corporativos que involucren tecnologías de la información, que le sean asignados de acuerdo con las necesidades y disponibilidades presupuestales destinadas a esta dirección.

- Prestar, siempre que sea posible, el apoyo requerido para la estructuración y elaboración de contratos y convenios relacionados con los contratos de concesión, de operación del Sistema de Transporte a cargo de la Empresa y los demás que le sean complementarios.

3.3.2 Coordinador de Procesos Misionales

Coordinar los procesos misionales relacionados con las tecnologías de la información y las comunicaciones de la empresa, de acuerdo con las políticas, obligaciones contractuales y normatividad vigente.

Funciones del cargo:[8]

- Coordinar las actividades relacionadas con el diagnóstico del funcionamiento del SIRCI, con el propósito de proponer y establecer las acciones de mejora de acuerdo con los principales aspectos de orden técnico, operativo, administrativo y comercial.

- Realizar el monitoreo a la operación del SIRCI para establecer políticas que optimicen los parámetros de medición de la operación del Sistema, de

[8] Ibíd.

acuerdo con los estándares establecidos, proponiendo acciones de mejora continua.

- Gestionar las actividades requeridas para avalar y supervisar el plan de implementación del SIRCI dentro de las competencias de la Dirección, de acuerdo con las especificaciones técnicas y operativas establecidas en el contrato.

- Coordinar el seguimiento de las auditorías informática y operativa de los subsistemas del SIRCI, de acuerdo con los lineamientos establecidos.

- Coordinar las actividades relacionadas con la supervisión de los contratos de interventoría de recaudo, de conformidad con las obligaciones contractuales.

- Coordinar la participación en la ejecución de los planes de contingencia y de seguridad de la información de los procesos misionales, bajo criterios de calidad, eficiencia y oportunidad.

- Participar en la estructuración de proyectos misionales que involucren tecnologías de la información, que le sean asignados de acuerdo con las necesidades y disponibilidades presupuestales destinadas a esta Dirección.

- Coordinar y brindar apoyo técnico a la ejecución, del seguimiento en las etapas de reversión, liquidación y transición de los contratos de concesión.

- Prestar, en el marco de sus competencias, el apoyo requerido para la estructuración y elaboración de contratos y convenios relacionados con los contratos de concesión de operación del Sistema de Transporte a cargo de la Empresa y los demás que le sean complementarios.

3.3.3 Profesional Especializado

Funciones del cargo:[9]

[9] Ibíd.

- Atender y resolver los requerimientos de las demás dependencias de la Empresa para el diseño, adquisición y puesta en marcha de Sistemas de Información y herramientas tecnológicas de la Empresa.

- Diseñar, dirigir, controlar y evaluar el desarrollo de los planes, programas, políticas y procedimientos informáticos en los que se soportan los procesos operativos y administrativos de la entidad, que serán medidos por indicadores de servicio.

- Diseñar y dirigir los procesos y cronogramas de mantenimiento de la infraestructura de Hardware, Software y Comunicaciones de la Empresa, de acuerdo a los estándares de normas de calidad y de seguridad.

- Asesorar los mecanismos y normas para el control de la legalidad del software y el respeto a los derechos de autor del software.

- Participar en la ejecución de los planes de contingencia y de seguridad de la información

- Supervisar la correcta aplicación de los mecanismos y normas para el control de la legalidad y el respeto a los derechos de autor de software.

- Atender y resolver los requerimientos a través de la mesa de ayuda corporativa.

- Hacer seguimiento del Plan de Contratación de la Dirección de TICs.

- Avalar la toma de decisiones relacionadas con la funcionalidad, confiabilidad, oportunidad y seguridad de la operación del software, hardware y comunicaciones de los sistemas de transporte público a cargo de la empresa.

3.3.4 Profesional Especializado Infraestructura y Comunicaciones

Funciones del cargo:[10]

[10] Ibíd.

- Atender y resolver los requerimientos de las demás dependencias de la Empresa para el diseño, adquisición y puesta en marcha de sistemas de redes de voz y datos, telecomunicaciones, circuitos de cámaras e Informadores electrónicos de la Empresa.

- Diseñar, dirigir, monitorear y hacer seguimiento de los sistemas de redes, telecomunicaciones, servidores y circuitos cerrados de televisión, usadas por la empresa.

- Acompañar y hacer interlocución técnica con los diferentes agentes del sistema, en materias de redes, telecomunicaciones, sistemas de cámaras e informadores electrónicos.

- Aplicar el diseño e implementación de las políticas del sistema de seguridad Informática para mantener en buen estado el funcionamiento de hardware y software y bienes informáticos de la empresa, en concordancia con los lineamientos de la Alta Gerencia y la normatividad vigente.

- Coordinar el soporte, actualización y mantenimiento de sistemas operativos, servidores y equipo de cómputo de TRANSMILENIO S.A.

- Responder por la mesa de ayuda corporativa en la que se administra el soporte técnico TIC´s.

- Participar en la ejecución de los planes de contingencia y de seguridad de la información.

- Supervisar la correcta aplicación de los mecanismos y normas para el control de la legalidad y el respeto a los derechos de autor de software.

- Atender y resolver los requerimientos a través de la mesa de ayuda corporativa y hacer seguimiento a los requerimientos del Help Desk del SIRCI.

3.3.5 Profesional Especializado de Bases de datos y Aplicaciones

Funciones del cargo:[11]

- Diseñar, dirigir, monitorear y hacer seguimiento de los sistemas de bases de datos y las aplicaciones misionales y de apoyo, utilizadas en TRANSMILENIO S.A.

- Gestionar y garantizar el aseguramiento de las bases de datos y aplicaciones misionales y de apoyo garantizando el cumplimiento de estándares y políticas de respaldo, así como los sistemas de recuperación ante desastres, de acuerdo con los lineamientos de la Alta Gerencia y la normatividad vigente.

- Acompañar y hacer interlocución técnica con los diferentes agentes del sistema, en materias de Bases de datos, Aplicaciones y subsistema de recaudo.

- Participar en la ejecución de los planes de contingencia y de seguridad de la información.

- Atender y resolver las dudas y consultas a usuarios internos del sistema de recaudo, y soporte administrativo, así como a los requerimientos asignados a través de la mesa de ayuda corporativa.

- Atender y resolver los requerimientos a través de la mesa de ayuda corporativa y hacer seguimiento a los requerimientos del Help Desk del SIRCI.

- Participar en procesos de auditoría informática y operativa al sistema de recaudo y del soporte administrativo de la Entidad.

- Asesorar, gestionar y administrar el soporte de las diferentes aplicaciones existentes en TRANSMILENIO S.A.

[11] Ibíd.

- Apoyar a la Entidad en la ejecución y seguimiento a las mejoras del SITP y el SIRCI en lo concerniente a sus competencias.

- Aplicar el diseño e implementación de las políticas del sistema de seguridad Informática para mantener en buen estado el funcionamiento de hardware y software y bienes informáticos de la empresa, en concordancia con los lineamientos de la Alta Gerencia y la normatividad vigente.

- Supervisar la correcta aplicación de los mecanismos y normas para el control de la legalidad y el respeto a los derechos de autor de software.

- Participar en la supervisión de contratos del SIRCI en los temas relacionados con su competencia.

3.3.6 Profesional Especializado Seguridad de Información

Funciones del cargo:[12]

- Asistir a la Entidad en la toma de decisiones sobre los aspectos relacionados con la seguridad informática y políticas de seguridad.

- Definir la estrategia de seguridad informática y sus objetivos.

- Administrar, coordinar y asegurar diariamente el proceso de seguridad Informática.

- Identificar y solucionar las necesidades y vulnerabilidades de seguridad desde el punto de vista del negocio.

- Verificar la correcta aplicación de los mecanismos y normas para el control de la legalidad y el respeto a los derechos de autor del software.

- Documentar las políticas, procedimientos de seguridad, cumpliendo con estándares internacionales y regulaciones que apliquen a la organización.

[12] Ibíd.

- Formar a la organización en cultura de la seguridad, elaborando campañas de seguridad informática de cara al usuario final.

- Interactuar con áreas de seguridad física para trabajar en conjunto en pro y mejora de la seguridad integral de TRANSMILENIO S.A.

- Implementar, configurar, mantener y operar los controles de seguridad informática tales como Firewalls, IDS, IPS, y demás dentro de su competencia.

- Monitorear el registro, modificación, remoción y des habilitación de accesos a sistemas y aplicaciones, evaluando periódicamente la efectividad de los controles y normas de seguridad.

- Diseñar y orientar la implementación de planes de contingencia y seguridad informática de la Empresa.

- Aplicar e implementar las políticas del sistema de seguridad Informática para mantener en buen estado el funcionamiento de hardware y software y bienes informáticos de la empresa, en concordancia con los lineamientos de la Alta Gerencia y la normatividad vigente.

- Atender y resolver los requerimientos a través de la mesa de ayuda corporativa.

- Participar en la supervisión de contratos del SIRCI en los temas relacionados con su competencia.

3.3.7 Profesional Universitario

Funciones del cargo:[13]

- Mantener, implementar y operar los servidores de TRANSMILENIO S.A. a nivel software y hardware.

[13] Ibíd.

- Participar en la elaboración y ejecución de planes, diseños, implementaciones y pruebas de sistemas informáticos y tecnológicos.

- Proponer alternativas de cambio y mejoramiento para las aplicaciones de tipo Servidor, para TRANSMILENIO S.A.

- Coordinar y garantizar que las aplicaciones estén disponibles a los usuarios, de acuerdo con los estándares y políticas establecidas para la calidad del servicio.

- Ejecutar la implementación de planes de contingencia y seguridad informática de la Empresa.

- Responder por la mesa de ayuda en la que se administra el soporte técnico TIC´s.

- Participar en la ejecución de los planes de contingencia y de seguridad de la información.

- Supervisar la correcta aplicación de los mecanismos y normas para el control de la legalidad y el respeto a los derechos de autor de software.

- Atender y resolver los requerimientos a través de la mesa de ayuda corporativa.

3.3.8 Técnico Administrativo Soporte en TIC's

Funciones del cargo:[14]

- Asegurar el correcto funcionamiento de la red local de datos, el hardware, equipos de impresión, equipos de comunicaciones, planta telefónica y en general la infraestructura tecnológica en que se soportan los procesos administrativos del Sistema Integrado de Transporte.

- Atender los procesos de mantenimiento preventivo y correctivo del hardware, equipos de comunicaciones y demás equipos de la

[14] Ibíd.

infraestructura tecnológica del Sistema Integrado de Transporte; así como atender a los requerimientos asignados a través de la mesa de ayuda.

- Participar de manera presencial en pruebas y validación de equipos de los sistemas del SITP y del SIRCI.

- Administrar y mantener en correcto funcionamiento los servicios de correo electrónico, acceso a Internet, aplicaciones de control de acceso, toma de copias de backups y demás servicios y herramientas tecnológicas de soporte a las labores de los usuarios.

- Suministrar herramientas de hardware y software a los servidores de la Entidad y Garantizar que la infraestructura de hardware y software estén disponibles a los usuarios, de acuerdo con los estándares y políticas establecidas para la calidad del servicio.

- Preparar, ejecutar y operar la implementación de planes de contingencia y seguridad informática de la Empresa.

- Verificar el correcto uso de los activos informáticos de la Entidad e informar las novedades al Director de TIC´s.

- Coordinar el soporte técnico y asesoría a usuarios en el uso de las herramientas tecnológicas de apoyo a las tareas diarias de los usuarios finales.

- Participar en la planeación, diseño, ejecución y evaluación de la capacitación en el uso de las herramientas de hardware, software y comunicaciones a usuarios finales.

- Instalar y desinstalar hardware y software, llevando un control de inventarios del hardware y software.

- Aplicar los mecanismos y normas para el control de la legalidad del software y el respeto a los derechos de autor del software.

- Aplicar el diseño e implementación de las políticas del sistema de seguridad Informática para mantener en buen estado el funcionamiento de hardware y

software y bienes informáticos de la empresa, en concordancia con los lineamientos de la Alta Gerencia y la normatividad vigente.

3.4 Procesos y Servicios

La Dirección de TIC's realiza los siguientes procesos:[15]

- Planeación de las TIC's: determinar las tecnologías de la información y las comunicaciones acordes a las funciones, actividades, responsabilidades y el desarrollo de la Entidad y del SITP.

- Administración de las TIC's: coordinar la operación y administración de las tecnologías de la información y las comunicaciones de la Entidad.

- Soporte a Usuarios: atender las necesidades y los requerimientos de los usuarios de las tecnologías de la información y las comunicaciones de la Entidad.

La Dirección de TIC's presta los siguientes servicios a las demás áreas de la entidad:

- Mesa de Ayuda

- Proveer herramientas de cómputo y comunicaciones a usuarios

- Cuentas de correo

- Almacenamiento en la nube

- Conectividad

- Seguimiento de contratos de concesión desde el punto de vista técnico

[15] ÁREAS DE SEGURIDAD DE LA INFORMACIÓN Y BASES DE DATOS TRANSMILENIO S.A. 2017. *Procesos y servicios de la Dirección de las TIC.* Transmilenio S.A. Bogotá, D.C. : s.n., 2017. Información suministrada directamente por Dependencias de Transmilenio S.A.

3.5 Encuesta de Seguridad en la Entidad

Para tener una visión más clara del estado actual de la seguridad de la información en la Entidad, se realizó una encuesta con el Modelo de Seguridad de la Información para la Estrategia de Gobierno en línea 2.0 que permite el levantamiento de la información de toda la infraestructura de seguridad de las empresas.

La encuesta fue respondida por los ingenieros Javier A. Castañeda, (a quien se denominará JAC), profesional Especializado Grado 06 en Seguridad de la Información y Guillermo Corredor, (a quien se denominará GC), profesional Especializado Grado 06 del área de bases de Datos. Dirección de TIC'S de la empresa TRANSMILENIO S.A.

- Infraestructura física, acceso y medio ambiente.

a. Centro de Datos. Definir qué es un centro de datos y averiguar si en la entidad existen o no.

GC: “El Datacenter se puede definir como un centro de procesamiento de datos, en el cual la información es tratada, almacenada y distribuida. Los servidores que hacen parte del Datacenter, deben estar en estado óptimo de funcionamiento. Transmilenio S.A. cuenta con un Datacenter Administrativo, administrado por la entidad”

b. Control de Acceso. Definir control de acceso y averiguar si en la entidad se utilizan.

JAC: “Es un mecanismo de seguridad que permite verificar la identidad del usuario y aprobar el acceso en caso de que esté autorizado o rechazarlo si no lo está.

De acuerdo al informe de seguridad del año 2017 para Transmilenio S.A., realizado por la empresa Password, las oficinas de la Entidad están dotadas con mecanismos de contacto y biométricos, suficientes para controlar el acceso a los pisos de la entidad”

c. Barreras. ¿Existen barreras físicas que aíslen las áreas coyunturales de la entidad?

JAC: “Las barreras físicas son estructuras que impiden la libre movilidad y son un componente importante en la seguridad. Las oficinas de Transmilenio están cubiertas por barreras físicas como puertas custodiadas por personal de seguridad que impiden el libre acceso al edificio, torniquetes de control de acceso, puertas con sistemas de control de acceso y vigiladas por guardas de seguridad, el Datacenter Administrativo cuenta con puerta de seguridad protegida por mecanismos de control de acceso, biométricos y cámaras de seguridad”.

d. CCTV. ¿Se utiliza circuito cerrado de televisión?

JAC: “Las oficinas de Transmilenio cuentan con un CCTV, el cual cubre toda la edificación, y se encuentra monitoreado las 24 horas por personal de seguridad, adicionalmente el edificio cuenta con CCTV que cubre todas las áreas comunes, incluido los ascensores”.

e. Cableado y Canaletas

Eléctrico: Existencia y estado del cableado eléctrico

GC: “Las instalaciones locativas cuentan con cableado nuevo, de acuerdo a la norma RETIE (Reglamento Técnico de Instalaciones Eléctricas)”, el cual fue

creado por el Decreto 18039 de 2004[16], del Ministerio de Minas y Energía. El objetivo de este reglamento es establecer medidas que garanticen la seguridad de las personas, vida animal y vegetal y la preservación del medio ambiente, previniendo, minimizando o eliminado los riesgos de origen eléctrico.

Datos: Existencia y estado del cableado de datos

JAC: “Las oficinas cuentan con cableado estructurado categoría 6A".

f. Seguridad Perimetral. ¿Existe un Firewall en la entidad?

JAC: “Sí, la Entidad cuenta con un Firewall Next Generatión, así mismo se complementa la seguridad informática con una herramienta Punto Final y correlación de datos”.

g. Switch. Averiguar cómo está construida la red de área local en cuanto a equipos activos.

GC: “La red cuenta con Switchs tipo POE para el acceso y Switchs Core Next Generatión. Adicionalmente hay treinta (30) Swichs de borde, distribuidos en todos los pisos de la sede Administrativa de Transmilenio S.A., los cuales están conectados con un backbone de fibra, entre cada uno de los pisos”.

h. Aire Acondicionado. ¿Necesitan y utilizan aire acondicionado?

[16] COLOMBIA. MINISTERIO DE MINAS Y ENERGÍA. 2004. *Resolución 18 0398 Por la cual se expide el Reglamento Técnico de Instalaciones eléctricas-RETIE.* Bogotá, D.C. : s.n., 2004. págs. p.1-122. Obtenido de: https://www.minminas.gov.co/documents/10180/23517/22074-2284.pdf.

GC: “Sí, se cuenta con un sistema de aire acondicionado en el Datacenter Administrativo, compuesto por dos acondicionadores, los cuales trabajan en esquemas de alta disponibilidad”.

i. Reguladores y UPS. ¿Hay reguladores y UPS?

GC: “Sí, el Datacenter Administrativo cuenta con una UPS de 100 KVA, la cual soporta la carga del Datacenter Administrativo y de las estaciones de trabajo de todos los pisos que ocupa la entidad”.

j. Planta de Emergencia. ¿Hay planta de generación de emergencia?

GC: “Si, el edificio cuenta con una planta que tiene una capacidad de generación de 1000 KVA, suficiente para proveer el servicio de energía a los 18 pisos de la edificación”.

- Lógico

k. Actualización de Servidores. ¿Se actualizan y parchan con regularidad los servidores?
JAC: “Si, esta labor se realiza con regularidad por políticas de seguridad”

¿Cuál de los métodos siguientes utilizan?
i. YUM
ii. WSUS
iii. Manual

JAC: “Manual”

l. Pruebas de Intrusión. Definir qué son pruebas de intrusión y averiguar si se han hecho o se hacen con regularidad.

JAC: “Son pruebas que se realizan en la empresa, sometiendo los métodos de protección a una situación real, con el fin de verificar su efectividad.
En Transmilenio, por políticas de seguridad, el área de TIC’s realiza pruebas de vulnerabilidad cada año, utilizando Ethical Hacking e Ingeniería Social”

- Metodológico.

Averiguar cuáles de los siguientes puntos metodológicos existe y se utilizan en la entidad.

m. Políticas. ¿Hay un manual como tal?
GC: “Sí, Transmilenio cuenta con políticas de Seguridad de la Información, las cuales están publicadas en la Intranet, y disponibles para todos los funcionarios de la Entidad”.

n. Procedimientos

GC: “Sí, Transmilenio tiene los siguientes procedimientos para la Gestión de TIC’s, los cuales están publicados en la intranet para el acceso de todos los funcionarios de la Entidad:

P-DT-002-1 Administración Bases de Datos Administrativas
P-DT-003 Especificación y gestión de requerimientos para solicitud de desarrollo de software
P-DT-004 Gestión Ambiente de Pruebas de Software
P-DT-005 Compra y Actualización del Software
P-DT-007-2 Procedimiento Administración Usuarios

P-DT-008 Mantenimiento de los Equipos de Computo
P-DT-009 Soporte Técnico a usuarios Finales
P-DT-010 Monitoreo del uso de medios
P-DT-011 Otorgar acceso a los medios
P-DT-012 Intercambio Seguro Información”

o. Normas. ¿Cuáles?

GC: “Sí, Transmilenio se rige por las normas del Estado Colombiano que aplican para las empresas públicas. Para aplicar la norma debidamente, la Entidad dispone de un Normograma que está disponible en la Intranet, para todos los funcionarios de la empresa. Con respecto a la Dirección de TIC’s, las normas que aplican son las siguientes:

Directiva 011 2012[17]: Promoción y uso del software libre en el Distrito Capital.
Acuerdo 279 2007[18]: "Por el cual se dictan los lineamientos para la Política de Promoción y Uso del Software libre en el Sector Central, el Sector Descentralizado y el Sector de las Localidades del Distrito Capital".
Resolución 305 2008[19]: Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.

[17] ALCALDÍA DE BOGOTÁ. 2012. *Directiva 011.* Bogotá, D.C. : s.n., 2012. pág. P.12. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=50214.
[18] COLOMBIA. CONCEJO DE BOGOTÁ. 2007. *Acuerdo 279.* Bogotá, D.C. : s.n., 2007. pág. p.15. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=23574.

[19] COMISIÓN DISTRITAL DE SISTEMAS CDS DE BOGOTÁ, D.C. 2008. *Resolución 305.* Bogotá, D.C. : s.n., 2008. págs. p-15. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=33486.

Ley 1581 2012[20]: Por la cual se dictan disposiciones generales para la protección de datos personales.

Resolución Reglamentaria 020 2006[21]: "Por medio de la cual se prescriben los métodos y se establece la forma, términos y procedimientos para la rendición de la cuenta y la presentación de informes, se reglamenta su revisión y se unifica la información que se presenta a la Contraloría de Bogotá D.C.".

Decreto 2693 2012[22]: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

Ley 1273 2009[23]: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones entre otras disposiciones.

Ley 1712 2014[24]: Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información púbica nacional y se dictan otras disposiciones.

---

[20] COLOMBIA. CONGRESO DE LA REPÚBLICA. 2012. *Ley estatutaria 1581.* Bogotá, D.C. : s.n., 2012. p. 18. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.

[21] CONTRALORÍA DE BOGOTÁ. 2006. *Resolución reglamentaria 020. Por medio de la cual se prescriben los métodos y se establece la forma, términos y procedimientos para la rendición de la cuenta y la presentación de informes, se reglamenta su revisión y se unifica la información que se pres.* Bogotá, D.C. : s.n., 2006. pág. p. 20. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=21844.

[22] PRESIDENCIA DE LA REPÚBLICA. 2012. *Decreto 2693. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.* . Bogotá, D.C. : s.n., 2012. p. 25. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51198.

[23] COLOMBIA. CONGRESO DE LA REPÚBLICA. 2012. *Ley estatutaria 1581.* Bogotá, D.C. : s.n., 2012. pág. p. 18. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.

[24] CONGRESO DE COLOMBIA. 2014**.** *Ley 1712. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras*

Decreto 619 2007[25]: "Por el cual se establece la Estrategia de Gobierno Electrónico de los organismos y de las entidades de Bogotá, Distrito Capital y se dictan otras disposiciones".

Decreto 316 2008[26]: "Por medio del cual se modifica parcialmente el artículo 3° del Decreto Distrital 619 de 2007 que adoptó las acciones para el desarrollo de la Estrategia Distrital de Gobierno Electrónico".

Decreto 2573 2014[1]: "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".

Ley 527 1999[27]: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Decreto 1747 2000[28]: Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.

Resolución 419 2015[29]: Por la cual se expide el Reglamento que regula el desarrollo y aplicación de las TIC al Sistema Integrado del Transporte Público SITP o al sistema de Información, Recaudo, Control de flota e Información al usuario - SIRCI y al sistema Inteligente de Transporte Masivo.

---

disposiciones. Bogotá, D.C. : s.n., 2014. pág. p. 19. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882.

[25] ALCALDÍA MAYOR DE BOGOTÁ. 2007**.** *Decreto 619.* Bogotá, D.C. : s.n., 2007. pág. p. 20. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=28134.

[26] ALCALDÍA DE BOGOTÁ. 2008. *Decreto 316.* Bogotá, D.C. : s.n., 2008. pág. p. 19. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=32819.

[27] CONGRESO DE COLOMBIA. 1999**.** *Ley 527.* Bogotá, D.C. : s.n., 1999. pág. p. 16. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

[28] PRESIDENCIA DE LA REPÚBLICA. 2000. *Decreto 1747.* Bogotá, D.C : s.n., 2000. págs. p-25. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4277.

[29] MINISTERIO DE AGRICULTURA Y DESARROLLO RURAL. 2015. *Resolución No. 419.* Bogotá, D.C. : s.n., 2015. pág. p. 15. Obtenido de: https://www.minagricultura.gov.co/Normatividad/Resoluciones/Resolucion%20No%20000419%20de%202015.pdf.

Directiva Presidencial 04 2012[30]: Eficiencia Administrativa y Lineamientos de la Política Cero Papel en la Administración Pública.

Decreto 1078 2015 [31] : Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Decreto 415 2016[32]: Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

Resolución 003 2017[33]: Por la cual se adopta la Guía de sitios Web para las entidades del Distrito Capital y se dictan otras disposiciones.

Circular 025 2017[34]: Inventarios de aplicaciones móviles distritales.

---

[30] PRESIDENCIA DE LA REPÚBLICA. 2012. *Decreto 2693. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.* . Bogotá, D.C. : s.n., 2012. pág. p. 25. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51198.

[31] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. 2015. *Decreto Número 1078. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.* Bogotá, D.C. : s.n., 2015. págs. p.1-172. Disponible en: http://www.mintic.gov.co/portal/604/articles-9528_documento.pdf.

[32] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. 2016. *Decreto No. 415.* Presidencia de la República. Bogotá, D.C. : s.n., 2016. pág. p. 4. Obtenido de: http://es.presidencia.gov.co/normativa/normativa/DECRETO%20415%20DEL%2007%20DE%20MARZO%20DE%202016.pdf.

[33] COMISIÓN DISTRITAL DE SISTEMAS CDS. 2017. *Resolución 003.* Bogotá, D.C. : s.n., 2017. págs. P.10. Obtenido de: http://secretariageneral.gov.co/transparencia/marco-legal/normatividad/resolucion-003-2017.

[34] MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL. 2017. *Circular 0025.* Bogotá. D.C. : s.n., 2017. págs. p.1-7. Obtenido de: https://www.minsalud.gov.co/Normatividad_Nuevo/Circular%20No.%20025%20de%202017.pdf.

p. Concientización. ¿Hacen regularmente procesos de concienciación en lo referente a seguridad de la información?

GC: “Sí, se realizan campañas por la intranet, charlas de capacitación y se entregan objetos como vasos, pocillos, pad mause, entre otros, con mensajes impresos relacionados a la seguridad de la información”.

q. ¿Se hace inducción a los empleados nuevos?

GC: “Sí, Transmilenio cuenta con un programa de inducción de una semana para los empleados que ingresan a laborar en la empresa, y con una plataforma web para la reinducción, la cual se aplica anualmente a todos los funcionarios y contratistas de la entidad”.

r. Acuerdos de Confidencialidad. ¿Los hay como tal o están embebidos en el contrato laboral?

GC: “Sí, la mayoría de ellos se encuentran embebidos en el contrato laboral, y los otros son documentos que se anexan al contrato, dependiendo de la información que va a manejar el funcionario”.

s. Código de Buena Conducta. ¿Existe?

GC: “Si existe el código de ética de Transmilenio S.A., el cual se encuentra publicado en la Intranet al alcance de todos los funcionarios de la entidad”.

3.6 Técnicas de Pentesting

La empresa Transmilenio S.A. realiza anualmente mediante proceso licitatorio con empresas especializadas, Técnicas de Pentesting, con el fin de llevar a cabo análisis de vulnerabilidades.

En Junio de 2017 se llevaron a cabo las últimas pruebas, según contrato CTO232-17, cuyo objeto fue: “Contratar la prestación de servicios a través de una empresa especializada, para la realización de un test de intrusión (Ethical Hacking), con el fin de detectar las posibles vulnerabilidades de seguridad de la red de datos de TRANSMILENIO S.A. en los segmentos que el ente gestor determine”, las cuales arrojaron como resultados vulnerabilidades en servidores, sistemas operativos, sitio web y la red inalámbrica.

Una vez determinadas las vulnerabilidades, la empresa Password, encargada de ejecutar las pruebas, generó un plan de acción para ser ejecutado por la empresa Transmilenio S.A., y así minimizar los riesgos a los cuales se evidenció que está expuesta.

Las conclusiones de los resultados del test son las siguientes:

“Se evidenciaron elementos con información expuesta sobre los pasillos y corredores, de los pisos evaluados, específicamente en los pisos 4, 5 y 6 del edificio.

Se evidenciaron cantidades considerables de información física en los escritorios desatendidos de los funcionarios.

Se evidenció la presencia de líquidos y material inflamable en áreas críticas de la entidad.

Se observó que los dispositivos de almacenamiento externo utilizados por los funcionarios de la entidad, no se encuentran debidamente protegidos, posibilitando su robo o manipulación.

Se evidenciaron mecanismos de contacto y biométricos, suficientes para controlar el acceso a los pisos de la entidad.

Se encontró que la información se deja desatendida en las trituradoras o impresoras, posibilitando su fuga de información, por parte de personal no autorizado.

Se evidenció que Transmilenio S.A. está protegido contra ataques de Phishing, en la identificación del envío de correos masivos desde un solo dominio.

Se informó por parte de Transmilenio S.A., que algunos de sus empleados, dieron aviso del correo falso que estaba llegando a sus bandejas de entrada.

Se concluye que Transmilenio S.A., cuenta con medidas de seguridad, que bloquean los dominios externos que envían correos masivos a sus funcionarios, con el objetivo de mitigar ataques de ingeniería social y correos de Spam.

Recomendaciones

Establecer políticas para el control de acceso en áreas seguras, permitiendo su buen uso y control de los visitantes.

Establecer la política de escritorio limpio en áreas sensibles, con el objetivo de minimizar el riesgo de fuga de información pura.

Seleccionar el papel reciclaje que será utilizado para impresión de borradores en las impresoras de los pisos, 5, 6 y 7.

Establecer controles de acceso biométricos o por contacto, a todas las impresoras de la entidad, con el objetivo de impedir la aparición de huérfanas, y minimizar el riesgo por fuga de información.

Divulgar las políticas de seguridad de la información, a todos los funcionarios de la entidad, con el objetivo de lograr su adopción y generar una cultura enfocada a la protección de la información.

4. JUSTIFICACIÓN

TRANSMILENIO S.A. es una empresa pública del Distrito y se debe regir bajo los estándares de seguridad de la información del MINTIC, de acuerdo a los lineamientos de la Estrategia de Gobierno en Línea, según lo establecido en el decreto número 2573 de 2014[1].

El documento Conpes 3854[3] hace referencia al conjunto de políticas estratégicas que soportan los objetivos de Gobierno en Línea como la “Protección de información del individuo” y la “credibilidad y confianza en el Gobierno en Línea”. Establece como elementos fundamentales de la seguridad de la información para los Organismos Gubernamentales:

La disponibilidad de la información y los servicios.
La integridad de la información y los datos.
Confidencialidad de la información.
Autenticidad.
No repudio.

Es necesario que Transmilenio S.A. establezca un modelo de seguridad acorde a los lineamientos del Programa Gobierno en Línea, debido a que es un requerimiento regulatorio, según lo establecido en el decreto 2573[1] artículo 10, el cual cita los plazos que tienen las entidades obligadas a implementar las actividades establecidas en el Manual de Gobierno en línea, lo que hace que sea de vital importancia su desarrollo e implementación para la empresa.

La no aplicación de esta investigación u otras medidas similares que lleven a una solución de seguridad informática a la empresa Transmilenio S.A., acorde a los lineamientos de gobierno en línea, conllevan a que no pueda garantizar la confidencialidad, integridad y disponibilidad de la información, y se verá expuesta

a riesgos informáticos, al igual que a las sanciones que el gobierno determine por el incumplimiento a las normas de seguridad de la información, vigentes para las entidades públicas, como es La Estrategia de Gobierno en Línea.

5. ALCANCE Y DELIMITACIÓN DEL PROYECTO

El alcance y las limitaciones están determinados de forma que permite acotar el análisis y diseño del modelo de seguridad de la información para la empresa TRANSMILENIO S.A. los cuales se describen a continuación:

5.1 Alcance

El alcance del presente proyecto, abarca el diseño del modelo de seguridad de la información para la empresa TRANSMILENIO S.A, de acuerdo a los lineamientos de la estrategia de gobierno en línea exigidos a esta entidad, basado en la norma ISO/IEC 27001[35] versión 2013 y está dirigido de acuerdo al mapa de procesos de la empresa. El trabajo cubrirá todos aquellos aspectos a tener en cuenta en relación a estándares, procedimientos, normas y medidas relacionadas con tecnología, que permitan asegurar las principales características que debe tener la información. Estas características son: integridad, disponibilidad y confidencialidad.

El alcance del proyecto abarca la parte corporativa de la entidad, es decir, no incluye activos informáticos, procesos, etc. de empresas externas como contratistas, entre otras que tengan alguna relación directa o indirecta con TRANSMILENIO S.A.

5.2 Limitaciones

Las limitaciones están determinadas en el análisis y diseño del modelo de seguridad de la información para la empresa TRANSMILENIO S.A, basado en la

[35] ISO. 2006. *Norma Técnica ISO 27001.* ISO. 2006. págs. 45. Obtenido de: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf.

norma ISO/IEC 27001 versión 2013, pero no abarca la parte de la implementación del modelo dentro de la empresa.

El proyecto plantea controles, que serán indispensables para proteger los activos de información más importantes de la entidad, con base a la norma ISO/IEC 27001 versión 2013. Se aclara que si ocurre algún cambio en la legislación vigente que exija nuevas medidas y controles, el presente modelo no podrá abarcar esa necesidad contractual que tendría la entidad. Para lo cual se necesitaría actualizarlo y direccionarlo a los nuevos cambios legislativos para dar cumplimiento.

6. MARCO REFERENCIAL

6.1 Antecedentes

La principal fuente será la norma ISO/IEC 27001[36] versión 2013, que contiene los lineamientos necesarios para la implementación de sistemas de Gestión de seguridad Informática SGSI.

De igual forma, los lineamientos de la Estrategia de Gobierno en Línea, según decreto número 2573 de 2014 del documento Conpes 3701 que hace referencia al conjunto de políticas estratégicas que soportan los objetivos de Gobierno en Línea relacionados con la disponibilidad, integridad y confidencialidad de la información. El Ministerio de Tecnologías de la Información y las Telecomunicaciones en Colombia también se ha unido para crear un modelo de seguridad para las entidades del Estado con el fin de que sirva como guía para construir el SGSI. Mediante la página web de la entidad se explican y detallan los lineamientos requeridos para cumplir el objetivo.

También se consultará el Modelo de Seguridad SGSI 2012, con título, Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0, autor, Centro de Investigación de Telecomunicaciones – CINTEL.

La Guía para la Implementación de Seguridad de la Información en una MIPYME, del MINTIC.

Otras guías del MINTIC para el desarrollo e implementación del SGSI:

[36] ISO. 2006. *Norma Técnica ISO 27001.* ISO. 2006. págs. 45. Obtenido de: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf.

Guía 1: Guía Metodológica de Pruebas de Efectividad.

Guía 2: Elaboración de la política general de seguridad y privacidad de la información.

Guía 3: Procedimientos de Seguridad de la información.

Guía 4: Roles y responsabilidades.

Guía 5: Guía para la gestión y clasificación de activos de información.

Otra fuente de consulta para el presente proyecto, es la Tesis de la universidad Católica de Perú con título Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo[37], del autor Hans Ryan Espinoza Aguinaga.

6.2 Marco Teórico

6.2.1 Seguridad Informática

La seguridad informática es la que se encarga de brindar soluciones técnicas de protección de la información, como por ejemplo la implementación de un firewall, los antivirus, solución de anomalías, entre otros[38].

[37] ESPINOZA, HANS RYAN. 2013. *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo.* Facultad de ciencias e Ingeniería, Universidad Católica del Perú. Lima : s.n., 2013. págs. 1-69. Recuperado de: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/4957/ESPINOZA_HANS_ANALISIS_SISTEMA_GESTION_SEGURIDAD_INFORMACION_ISO_IEC%2027001_2005_COMERCIALIZACION_PRODUCTOS_CONSUMO_MASIVO.pdf?sequence=1&isAllowed=y, Tesis Pregrado.

[38] ISO. 2006. *Norma Técnica ISO 27001.* ISO. 2006. págs. 45. Obtenido de: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf.

6.2.2 Seguridad de la Información

Seguridad de la información se refiere a las normas de seguridad, los riesgos, las amenazas. Se puede definir como las políticas a seguir para la protección de la información de manera que se disminuyan los riesgos y las amenazas[39].

6.2.3 Diferencia Entre Seguridad Informática y Seguridad de la Información

La diferencia radica en que la seguridad informática es la acción que se realiza, es decir, instalar las herramientas como por ejemplo el antivirus o el Firewall, mientras que la seguridad de la información es la parte escrita o teórica de los procedimientos o normas a seguir[40].

6.2.4 SGSI

El Sistema de Gestión de Seguridad Informática comprende el Diseño, Implementación y Mantenimiento de normas y procesos de la entidad, con el fin de preservar los principios de la seguridad Informática como son la confidencialidad, integridad y disponibilidad de los activos informáticos[41]

6.2.5 Magerit

La metodología de análisis y gestión de riesgos de los sistemas de información Magerit, fue creada por el Consejo Superior de Administración Electrónica, está compuesta por un método, un catálogo y una guía de técnicas. Sus objetivos están enfocados a concientizar a las empresas y las personas responsables de la información, de que existen riesgos y la necesidad de gestionarlos, ofreciendo un método para analizarlos, lograr descubrir y planificar el tratamiento oportuno para así mantener un buen control de dichos riesgos, llevando a la empresa a estar preparada para procesos de evaluación, auditoría y certificación.

---

[39] Ibíd.
[40] Ibíd.
[41] Ibíd.

Para aplicar esta metodología se requiere seguir una serie de pasos estructurados como son conocer la empresa realizando visitas; hacer entrevistas con el fin de tener una idea más clara de lo que se va a evaluar; luego se deben identificar los activos de información agrupados por tipos de acuerdo de su función; luego se requiere hacer una valoración de dichos activos, según la metodología la valoración debe ser de acuerdo a cinco dimensiones, confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Una vez realizada la valoración se debe proceder a identificar todas las amenazas que puedan causar daño en alguna de las dimensiones a los activos de información. Posterior a esto, se requiere hacer la identificación de las salvaguardas para minimizar al máximo el riesgo y así aumentar el nivel de seguridad de la información en la empresa.[42]

6.2.6 GEL

El GEL o Gobierno en Línea es una estrategia liderada por el Ministerio de las TIC (Tecnologías de la Información y las Comunicaciones), está constituida por un conjunto de instrumentos normativos, técnicos y de políticas públicas con el objetivo de promover la construcción de un estado transparente, eficiente y participativo el cual busca brindar un mejor servicio en línea a los ciudadanos mediante el aprovechamiento de las TIC.[43]

6.2.7 SASIGEL

El Sistema Administrativo de Seguridad de la Información para Gobierno en línea (SASIGEL) se encuentra apoyado en el modelo de Seguridad de la Información para las entidades del Estado, las cuales buscan tomar acciones estratégicas y

---

[42] ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. 2012**.** *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid : s.n., 2012. págs. p.1-127. Obtenido de: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

[43] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. 2015. *Manual Estrategia de Gobierno en Línea.* Bogotá, D.C. : s.n., 2015. págs. p. 1-37. Obtenido de: http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf.

definir los lineamientos para la implementación, seguimiento, y mantenimiento del modelo de seguridad de la información en las entidades públicas y privadas que proveen los servicios de gobierno en línea.

El SASIGEL, permite cumplir con los principios establecidos en Ley 1341 de 2009[44] correspondientes a la protección de la información, credibilidad y confianza en el Gobierno en línea. Para el cumplir con estos principios se requiere que los servicios de gobierno en línea cumplan con los elementos fundamentales de seguridad de la información (Disponibilidad, integridad y confidencialidad de la información).

6.2.8 Normas ISO/IEC

Una norma es un conjunto de reglas escritas en un documento y que son el resultado del consenso entre las partes interesadas, las cuales deben ser aprobadas por un organismo de normalización.

ISO es un Organismo Internacional reconocido, dedicado a desarrollar reglas de normalización en diferentes campos, entre ellos la informática.

IEC es un Organismo Internacional reconocido, dedicado a desarrollar reglas de normalización en el campo de la electrónica.
El conjunto de normas ISO/IEC 27000 contiene todos los requisitos y normas para la especificación de sistemas de gestión de la seguridad de la información SGSI, con el fin de que sea aplicado en las empresas, para la elaboración del sistema de gestión de la seguridad de la información, valoración de riesgos y controles.

---

[44] CONGRESO DE LA REPÚBLICA. 2009. *Ley 1341.Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.* Presidencia de la República. Bogotá, D.C. : s.n., 2009. pág. p. 15. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913.

El conjunto de normas ISO/IEC 27000 también comprende la ISO/IEC 27001, la cual se constituye como la principal de la serie y de acuerdo a esta norma, la seguridad informática es la preservación de la integridad, disponibilidad y confidencialidad de la información. La finalidad de esta norma es proporcionar el modelo para diseñar, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información SGSI.[45]

6.3 Marco Conceptual

Para mejor comprensión de este proyecto, se relaciona a continuación la definición de algunos términos de la seguridad informática:

6.3.1 Activo Informático

Es cualquier información o elemento empleado para su tratamiento como los equipos, sistemas, personal, infraestructura física, soportes, etc., que tenga algún valor para la empresa.

6.3.2 Amenaza

Causa potencial de cualquier incidente que pueda provocar daños a uno o varios activos informáticos o a la empresa.

6.3.3 Análisis de Riesgo

Proceso para comprender la naturaleza del riesgo y determinar su nivel de afectación.

6.3.4 Riesgo

Es el efecto de la incertidumbre sobre los objetivo.

[45] ICONTEC. Reglamento del Servicio de Normalización de ICONTEC

6.3.5 Integridad

Propiedad de salvaguardar la exactitud y estado completo de los activos de información.

6.3.6 Disponibilidad

Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

6.3.7 Confidencialidad

Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados.

6.4 Marco Legal

Normas ISO/IEC 27000 y 27001[46], provee toda la normatividad acerca de la seguridad de la información y el ciclo de vida del SGSI.

Ley 1273 de 2009[47], la cual adiciona dos capítulos al Código Penal Colombiano:
Capitulo Primero: De los atentados contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos.
Capitulo Segundo: De los atentados informáticos y otras infracciones. Esta ley está ligada a la ISO27000, lo cual ubica a Colombia a la vanguardia en legislación de seguridad informática.

---

[46] ISO. 2006. *Norma Técnica ISO 27001.* ISO. 2006. págs. 45. Obtenido de: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf.

[47] COLOMBIA. CONGRESO DE LA REPÚBLICA. 2009. *Ley 1273.* Bogotá, D.C. : s.n., 2009. pág. p. 15. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.

La Ley 603 de 2000[48] también contiene la protección de los derechos de autor en Colombia. El software es un activo, además está protegido por el Derecho de Autor y obliga a las empresas a declarar si los problemas de software son o no legales.

Ley estatutaria 1266 2008[49], en esta ley se establecen las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

La ley 1341[50] del 30 de julio de 2009, por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Ley estatutaria 1581[51] de 2012 de protección de datos personales, sancionada siguiendo los lineamientos establecidos por el Congreso de la República.
Decreto 1377 de 2013[52] Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.

---

[48] CONGRESO DE COLOMBIA. 2000. *Ley 603.* Bogotá, D.C. : s.n., 2000. pág. p.12. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960.

[49] CONGRESO DE COLOMBIA. 2008. *Ley estatutaria 1266.* Bogotá, D.C. : s.n., 2008. pág. p. 24. Obtenido de: https://www.uiaf.gov.co//recursos_user///2014/OAJ/Ley%20Estatutaria%201266%20de%202008%20Habeas%20Data.pdf.

[50] CONGRESO DE LA REPÚBLICA. 2009. *Ley 1341.Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.* Presidencia de la República. Bogotá, D.C. : s.n., 2009. pág. p. 15. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913

[51] COLOMBIA. CONGRESO DE LA REPÚBLICA. 2012. *Ley estatutaria 1581.* Bogotá, D.C. : s.n., 2012. p. 18. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.

[52] PRESIDENCIA DE LA REPÚBLICA. 2012. *Decreto 1377. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.* Bogotá, D.C. : s.n., 2012. p. 12. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646.

Decreto número 1151 de 2008[53], artículo 3°. Principios aplicables a la Estrategia de Gobierno en Línea:

- ✓ Gobierno centrado en el ciudadano.
- ✓ Visión unificada del estado.
- ✓ Acceso equitativo y multicanal.
- ✓ Protección de la información del individuo.
- ✓ Credibilidad y confianza en el Gobierno en Línea.

Decreto número 1151 de 2008, artículo 5°, el cual lista las siguientes fases de Gobierno en Línea:

- ✓ Fase de Información en Línea: Es la fase inicial del GEL en la cual las entidades habilitan sus propios sitios web para proveer información en línea.
- ✓ Fase de Interacción en Línea: Es la fase en la cual se habilita la comunicación de dos vías con las consultas en línea e interacción con servidores públicos.
- ✓ Fase de Transacción en Línea: Es la fase en la que se suministran transacciones electrónicas.
- ✓ Fase de Transformación en Línea: Durante esta fase se realizan cambios en la forma de operar de las entidades, con ventanillas virtuales y el uso de la Intranet Gubernamental.
- ✓ Fase de Democracia en Línea: Es la fase en la cual se incentiva a la ciudadanía a participar de manera activa en la toma de decisiones del estado y la construcción de políticas públicas.

---

[53] MINISTERIO DE COMUNICACIONES DE COLOMBIA. 2008. *Decreto 1151.* Bogotá, D.C. : s.n., 2008. pág. p.3. Obtenido de: http://artesaniasdecolombia.com.co/Documentos/Contenido/8561_decreto_1151_de_2008.pdf.

7. MARCO METODOLÓGICO

Para el desarrollo del presente proyecto se hará uso de la metodología Magerit 3.0, la cual proporciona las guías y procedimientos completos para la elaboración del análisis y la gestión de los riesgos. Esta metodología fue elaborada por el Consejo Superior de Administración Electrónica y aporta en forma clara y concreta el método, técnicas y procedimientos con sus respectivos instrumentos que se utilizan para dar respuesta a cada uno de los interrogantes planteados en los objetivos específicos y responde al "CÓMO HACERLO".

De acuerdo a la metodología de desarrollo, este proyecto se clasifica como investigación aplicada por su objeto de estudio. De igual forma por la fuente de investigación, corresponde a una investigación de campo, toda vez que la información es tomada bajo las técnicas de observación, entrevistas y análisis de documentos.

Igualmente, se seguirá la metodología PHVA, la cual contempla las fases de Planificar, Hacer, Verificar y Actuar. Con base a esta metodología se hará el diagnóstico, el cual consiste en identificar el estado actual de la empresa, establecer el nivel de madurez y hacer el levantamiento de la información.

8. PRODUCTO RESULTADO A ENTREGAR

8.1 Resultados del Proyecto

Como resultados del presente proyecto se generó una propuesta la cual presenta como solución la seguridad de la información corporativa para la empresa Transmilenio S.A. Esta propuesta está basada en la norma NTC ISO/IEC 27001 en su versión 2013, de acuerdo a lo requerido por la Estrategia de Gobierno en Línea.

Una vez se realiza el diagnóstico inicial a la compañía basado en encuestas, entrevistas y observación, se procede a determinar la metodología de análisis de riesgos la cual se aplicará en la empresa basada en el documento “Metodología de análisis de riesgo. Tras realizar un análisis de riesgos de seguridad de la información se puede conocer el estado actual de los riesgos y generar una propuesta que permita evidenciar la necesidad de implementar una solución de seguridad de la información.

8.2 Entregables

Para la realización del proyecto ESTUDIO DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA TRANSMILENIO S.A. ACORDE A LA NORMA ISO/IEC 27001 VERSIÓN 2013, se proponen los siguientes entregables:

- ✓ Encuesta sobre el estado actual de la seguridad de la Información.
- ✓ Documento metodología de análisis de riesgo con enfoque en seguridad de la información.
- ✓ Matriz de análisis de riesgos.

- ✓ Declaración de aplicabilidad determinando el nivel de cumplimiento de los dominios.
- ✓ Propuesta de solución de seguridad de la información para la empresa Transmilenio S.A.

9. CONCLUSIONES Y RECOMENDACIONES

La caracterización de la metodología MAGERIT en su versión 3, es de gran importancia ya que permite definir con gran minucia las amenazas en los activos de la empresa Transmilenio, los cuales están parametrizados en rangos específicos de valoración permitiendo tener posibles soluciones para aquellos riesgos que se puedan prever según lo evaluado.

A partir de la identificación de los activos más importantes y críticos para la organización, se pueden establecer prioridades en tiempos de solución de materialización de amenazas.

La conceptualización y la caracterización de las amenazas y riesgos, según la valoración de los activos de la empresa, contribuye a establecer el criterio de priorización de la atención de una falla en la organización. Esto permite establecer salvaguardas según el modelo de la metodología MAGERIT.

Se puede evidenciar que es necesario en las empresas aplicar dominios y controles del estándar ISO/IEC 27001, para así establecer un control y seguridad de la información.

Los dominios y controles del estándar ISO/IEC 27001 buscan dar un control a todos los estados de seguridad que se encuentran en la Entidad de tal manera que se cuide el activo más preciado, el cual es la información.

Las listas de chequeo permiten verificar de forma cruzada si los dominios del estándar ISO/IEC 27001 se encuentran implementados, de tal forma que se alineen con las políticas y necesidades de cada organización.

De acuerdo al trabajo realizado, se evidencia que la empresa tiene un cumplimiento en la mayoría de los dominios por encima del 90%, sin embargo, se

requiere un seguimiento y mejora en los ítems restantes para alcanzar el cumplimiento total. En el caso del dominio de Organización de la seguridad de la Información, el cual tiene un cumplimiento del 83%, se requiere atención prioritaria en las partes externas con relación a la seguridad de los móviles, la cual tiene una política de seguridad, pero sólo con un cumplimiento del 60/100, y las medidas de seguridad para dichos móviles solo cumplen en 40/100. Por lo tanto, se requiere reforzar esa parte de forma inmediata.

Es prioritario que la Entidad disponga los recursos necesarios para la ejecución del Plan General de Trabajo para la implementación de la Estrategia de Gobierno en Línea (GEL) planteado en este documento, con el fin de ejecutarlo de acuerdo al cronograma, para así ponerse al día con lo requerido por el MINTIC.

10. BIBLIOGRAFÍA

ALCALDÍA DE BOGOTÁ. 2008. *Decreto 316.* Bogotá, D.C. : s.n., 2008. pág. p. 19. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=32819.

ALCALDÍA DE BOGOTÁ. 2012. *Directiva 011.* Bogotá, D.C. : s.n., 2012. p.12. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=50214.

ALCALDÍA MAYOR DE BOGOTÁ. 2007. *Decreto 619.* Bogotá, D.C. : s.n., 2007. p. 20. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=28134.

ÁREA DE SEGURIDAD DE LA INFORMACIÓN DE TRANSMILENIO. 2017. *Organigrama Dirección de TIC Transmilenio.* Bogotá, D.C. : s.n., 2017.

ÁREAS DE SEGURIDAD DE LA INFORMACIÓN Y BASES DE DATOS TRANSMILENIO S.A. 2017. *Procesos y servicios de la Dirección de las TIC.* Transmilenio S.A. Bogotá, D.C. : s.n., 2017. Información suministrada directamente por Dependencias de Transmilenio S.A.

COLOMBIA, CONCEJO DE BOGOTÁ D.C. 1999. *Acuerdo 004 de 1999. Por el cual se autoriza al Alcalde Mayor en representación del Distrito Capital para participar, conjuntamente con otras entidades del orden Distrital, en la Constitución de la Empresa de Transporte del Tercer Milenio - Transmilenio S.* Bogotá, D.C. : Concejo de Bogotá, 1999. p.1. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=892, Acuerdo municipal.

COLOMBIA. CONCEJO DE BOGOTÁ. 2007. *Acuerdo 279.* Bogotá, D.C. : s.n., 2007. p.15. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=23574.

COLOMBIA. CONGRESO DE LA REPÚBLICA. 2009. *Ley 1273.* Bogotá, D.C. : s.n., 2009. p. 15. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.

—. 2012. *Ley estatutaria 1581.* Bogotá, D.C. : s.n., 2012. p. 18. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.

COLOMBIA. CONTRALORÍA DE BOGOTÁ. 2016. *Informe de Auditoría de Desempeño PAD 2016 (RECAUDO) EMPRESA TRANSMILENIO S.A.* Contraloría de Bogotá. Bogotá, D.C. : s.n., 2016. p.1-50. Disponible en: http://www.transmilenio.gov.co/Publicaciones/contraloria_de_bogota_informe_de_auditoria_de_desempeno_pad_2016_recaudo, Informe resultados auditoría.

COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN y CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. 2016. *Documento CONPES 3854 Política Nacional de Seguridad Digital.* CONPES. Bogotá, D.C. : s.n., 2016. p.1-91. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

COLOMBIA. MINISTERIO DE MINAS Y ENERGÍA. 2004. *Resolución 18 0398 Por la cual se expide el Reglamento Técnico de Instalaciones eléctricas-RETIE.* Bogotá, D.C. : s.n., 2004. p.1-122. Obtenido de: https://www.minminas.gov.co/documents/10180/23517/22074-2284.pdf.

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. 2014. *Decreto Número 2573.* Bogotá, D.C. : MinTic, 2014.

p.9. Disponible en: http://www.mintic.gov.co/portal/604/articles-14673_documento.pdf, Decreto Nacional.

COLOMBIA.CONTRALORÍA DE BOGOTÁ, D.C. 2017. *Informe de Auditoría de regularidad empresa TRANSMILENIO S.A.* Bogotá, D.C.Disponible en: http://www.transmilenio.gov.co/loader.php?lServicio=Publicaciones&lTipo=WFactionA&lFuncion=visualizar&id=14341&bd=m : s.n., 2017. p.237, Informe resultados auditoría.

COMISIÓN DISTRITAL DE SISTEMAS CDS DE BOGOTÁ, D.C. 2008. *Resolución 305.* Bogotá, D.C. : s.n., 2008. p-15. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=33486.

COMISIÓN DISTRITAL DE SISTEMAS CDS. 2017. *Resolución 003.* Bogotá, D.C. : s.n., 2017. p.10. Obtenido de: http://secretariageneral.gov.co/transparencia/marco-legal/normatividad/resolucion-003-2017.

CONGRESO DE COLOMBIA. 2014. *Ley 1712. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.* Bogotá, D.C. : s.n., 2014. p. 19. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882.

CONGRESO DE COLOMBIA. 1999. *Ley 527.* Bogotá, D.C. : s.n., 1999. p. 16. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276.

CONGRESO DE COLOMBIA. 2000. *Ley 603.* Bogotá, D.C. : s.n., 2000. p.12. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960.

CONGRESO DE COLOMBIA. 2008. *Ley estatutaria 1266.* Bogotá, D.C. : s.n., 2008. p. 24. Obtenido de:

https://www.uiaf.gov.co//recursos_user///2014/OAJ/Ley%20Estatutaria%201266%20de%202008%20Habeas%20Data.pdf.

CONGRESO DE LA REPÚBLICA. 2009. *Ley 1341.Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.* Presidencia de la República. Bogotá, D.C. : s.n., 2009. p. 15. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913.

CONTRALORÍA DE BOGOTÁ. 2006. *Resolución reglamentaria 020. Por medio de la cual se prescriben los métodos y se establece la forma, términos y procedimientos para la rendición de la cuenta y la presentación de informes, se reglamenta su revisión y se unifica la información que se pres.* Bogotá, D.C. : s.n., 2006. p. 20. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=21844.

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. 2016. *Decreto No. 415.* Presidencia de la República. Bogotá, D.C. : s.n., 2016. p. 4. Obtenido de: http://es.presidencia.gov.co/normativa/normativa/DECRETO%20415%20DEL%2007%20DE%20MARZO%20DE%202016.pdf.

ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. 2012. *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid : s.n., 2012. p.1-127. Obtenido de: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

ESPINOZA, HANS RYAN. 2013. *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una*

empresa de producción y comercialización de productos de consumo masivo. Facultad de ciencias e Ingeniería, Universidad Católica del Perú. Lima : s.n., 2013. págs. 1-69. Recuperado de: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/4957/ESPINOZA_HANS_ANALISIS_SISTEMA_GESTION_SEGURIDAD_INFORMACION_ISO_IEC%2027001_2005_COMERCIALIZACION_PRODUCTOS_CONSUMO_MASIVO.pdf?sequence=1&isAllowed=y, Tesis Pregrado.

ISO. 2006. *Norma Técnica ISO 27001.* ISO. 2006. págs. 45. Obtenido de: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf.

MINISTERIO DE AGRICULTURA Y DESARROLLO RURAL. 2015. *Resolución No. 419.* Bogotá, D.C. : s.n., 2015. p. 15. Obtenido de: https://www.minagricultura.gov.co/Normatividad/Resoluciones/Resolucion%20No%20000419%20de%202015.pdf.

MINISTERIO DE COMUNICACIONES DE COLOMBIA. 2008. *Decreto 1151.* Bogotá, D.C. : s.n., 2008. p.3. Obtenido de: http://artesaniasdecolombia.com.co/Documentos/Contenido/8561_decreto_1151_de_2008.pdf.

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. 2015. *Manual Estrategia de Gobierno en Línea.* Bogotá, D.C. : s.n., 2015. p. 1-37. Obtenido de: http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf.

MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL. 2017. *Circular 0025.* Bogotá. D.C. : s.n., 2017. p.1-7. Obtenido de:

https://www.minsalud.gov.co/Normatividad_Nuevo/Circular%20No.%20025%20de%202017.pdf.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. 2015. *Decreto Número 1078. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.* Bogotá, D.C. : s.n., 2015. p.1-172. Disponible en: http://www.mintic.gov.co/portal/604/articles-9528_documento.pdf.

PRESIDENCIA DE LA REPÚBLICA. 2012. *Decreto 1377. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.* Bogotá, D.C. : s.n., 2012. p. 12. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646.

PRESIDENCIA DE LA REPÚBLICA. 2000. *Decreto 1747.* Bogotá, D.C : s.n., 2000. p-25. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4277.

PRESIDENCIA DE LA REPÚBLICA. 2012. *Decreto 2693. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones. .* Bogotá, D.C. : s.n., 2012. p. 25. Obtenido de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51198.

PRESIDENCIA DE LA REPÚBLICA. 2012. *Directiva Presidencial No. 4. Eficiencia Administrativa y lineamientos de la política cero papel en la administración pública.* Bogotá, D.C. : s.n., 2012. pág. p.3. Obtenido de: http://wsp.presidencia.gov.co/Normativa/Directivas/Documents/direc0404032012.pdf.

TRANSMILENIO S.A. 2013. Organigrama de Transmilenio. *Transmilenio.gov.* [En línea] 26 de 08 de 2013. [Citado el: 20 de Febrero de 2018.] http://www.transmilenio.gov.co/Publicaciones/la_entidad/estructura_organizacional/Organigrama.

TRANSMILENIO S.A. 2017. *Resolución 234 de 2017. Manual de Funciones Trabajadores Oficiales.* Transmilenio. Bogotá, D.C. : s.n., 2017. Información proporcionada por la empresa directamente.

11. ANEXOS

11.1 Anexo A: Carta de Autorización

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DISTRITAL DE MOVILIDAD
TRANSMILENIO S.A.

Bogotá D.C., 18 de octubre de 2016

Señores:
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
Atn. Ing. Ramses Rios Lampariello
Líder Nacional Especialización en Seguridad Informática
Bogotá D.C.

Asunto: Autorización Trabajo de Grado- Dirección de TIC´s TRANSMILENIO S.A

Respetado Ingeniero Ríos:

Por medio de la presente me permito informar que el ingeniero NICOLÁS QUINTERO AMAYA, identificado con Cédula de Ciudadanía No. 3.028.797 de Gachancipá, se encuentra autorizado para adelantar en esta Entidad, la investigación requerida para la elaboración del trabajo de grado, en el tema de Análisis y Diseño de un Modelo de Seguridad de la Información aplicable a TRANSMILENIO S.A., con el objetivo de optar por el título de Especialista en Seguridad Informática.
El ingeniero QUINTERO reportará para los fines pertinentes a la Dirección de Tecnologías de la Información y la Comunicación.

Atentamente,

JAVIER A. CASTAÑEDA
Profesional Especializado Grado 06
Seguridad de la Información
Dirección de TIC'S - TRANSMILENIO S.A.

Código: 802.02

R-DA-005 Enero de 2016

Avenida Eldorado No. 66-63
PBX: (57) 220 3000
Fax: (57) 3249870 - 80
Código postal: 111321
www.transmilenio.gov.co
Información: Línea 195

BOGOTÁ MEJOR PARA TODOS

11.2 Anexo B: Inventario de Activos

De acuerdo al Modelo de Seguridad de la Información para la Estrategia de Gobierno en línea 2.0, TRANSMILENIO S.A., debe mantener un inventario actualizado de los activos de información de la entidad, al igual debe propender por conservar la confidencialidad, integridad y disponibilidad de los activos de información determinando sus responsables, y su ubicación. En cuanto a la clasificación de los activos de información, ésta se hace con base en la metodología Magerit 3.0 Guía 2, la cual establece una codificación de acuerdo al tipo de activo, y señala que se debe incluir por lo menos la descripción, localización y propietario.

- ✓ [D] Datos / Información
- ✓ [S] Servicios
- ✓ [SW] Software - Aplicaciones informáticas
- ✓ [HW] Equipamiento informático (hardware)
- ✓ [COM] Redes de comunicaciones
- ✓ [Media] Soportes de información
- ✓ [AUX] Equipamiento auxiliar
- ✓ [L] Instalaciones
- ✓ [P] Personal

Tabla 1. Listado de Activos Informáticos Transmilenio S.A.

Tipo	Descripción	Propietario
DIRECCIÓN ADMINISTRATIVA		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Intranet	TIC's
[SW]	KASPERSKY	TIC's
[SW]	Office 2010	TIC's
[SW]	Office 2013	TIC's
[SW]	Otros Free	Administrativa
[SW]	SIAF (SP-ERP)	TIC's

Tabla 1. (Continuación).

Tipo	Descripción	Propietario
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's
DIRECCIÓN TÉCNICA DE BRT		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Creative Cloud	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Arcgis	TIC's
[SW]	Autocad	TIC's
[SW]	IBM SPSS	TIC's
[SW]	Intranet	TIC's
[SW]	KASPERSKY	TIC's
[SW]	Office 2010	TIC's
[SW]	Office 2013	TIC's
[SW]	Office 365	TIC's
[SW]	Otros Free	BRT
[SW]	SIAF (SP-ERP)	TIC's
[SW]	Transcad	TIC's
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's
DIRECCIÓN TÉCNICA DE BUSES		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Arcgis	TIC's
[SW]	Autocad	TIC's
[SW]	Cliente Oracle-Home	TIC's
[SW]	IBM SPSS	TIC's
[SW]	Intranet	TIC's
[SW]	KASPERSKY	TIC's
[SW]	Office 2010	TIC's
[SW]	Office 2013	TIC's

Tabla 1. (Continuación).

Tipo	Descripción	Propietario
[SW]	Otros Free	Buses
[SW]	SIAF (SP-ERP)	TIC's
[SW]	SQL Developer	TIC's
[SW]	Transcad	TIC's
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's
CENTRO DE CONTROL		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Intranet	Comunicaciones
[SW]	KASPERSKY	TIC's
[SW]	Office 2010	TIC's
[SW]	Otros Free	C. Control
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's
SUBGERENCIA DE COMUNICACIONES		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Creative Cloud	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Intranet	TIC's
[SW]	KASPERSKY	TIC's
[SW]	Office 2010	TIC's
[SW]	Office 2013	TIC's
[SW]	Otros Free	TIC's
[SW]	SIAF (SP-ERP)	TIC's
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's

Tabla 1. (Continuación).

Tipo	Descripción	Propietario
CONTRALORÍA		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Intranet	Comunicaciones
[SW]	KASPERSKY	TIC's
[SW]	Office 2010	TIC's
[SW]	Office 2013	TIC's
[SW]	Otros Free	Contraloría
[SW]	SIAF (SP-ERP)	TIC's
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's
CONTROL DISCIPLINARIO		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Intranet	TIC's
[SW]	KASPERSKY	TIC's
[SW]	Office 2013	TIC's
[SW]	Otros Free	Disciplinario
[SW]	SIAF (SP-ERP)	TIC's
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's
CONTROL INTERNO		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Intranet	TIC's
[SW]	KASPERSKY	TIC's
[SW]	Office 2010	TIC's
[SW]	Office 2013	TIC's
[SW]	Otros Free	Interno

Tabla 1. (Continuación).

Tipo	Descripción	Propietario
[SW]	SIAF (SP-ERP)	TIC's
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's
CORPOSISTEMA		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Intranet	TIC's
[SW]	KASPERSKY	TIC's
[SW]	Office 2013	TIC's
[SW]	Otros Free	Corposistema
[SW]	Winrar	TIC's
[D]	CAT	TIC's
CORRESPONDENCIA		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Intranet	TIC's
[SW]	KASPERSKY	TIC's
[SW]	Office 2010	TIC's
[SW]	Office 2013	TIC's
[SW]	Otros Free	Correspondencia
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's
SUBGERENCIA ECONÓMICA		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Cliente Oracle-Home	TIC's
[SW]	IBM SPSS	TIC's
[SW]	Intranet	TIC's
[SW]	KASPERSKY	TIC's

Tabla 1. (Continuación).

Tipo	Descripción	Propietario
[SW]	Office 2010	TIC's
[SW]	Office 2013	TIC's
[SW]	Otros Free	Económica
[SW]	Remuneración de agentes	TIC's
[SW]	SIAF (SP-ERP)	TIC's
[SW]	Transcad	TIC's
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's
EMISORA		
[HW]	PC (Escritorio)	Emisora
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	KASPERSKY	TIC's
[SW]	Office 2013	TIC's
[SW]	Otros Free	Emisora
[SW]	Winrar	TIC's
[SW]	CAT	TIC's
GERENCIA GENERAL		
[HW]	PC (Escritorio)	Usuario
[HW]	PC (Portátil)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Intranet	TIC's
[SW]	KASPERSKY	TIC's
[SW]	Office 2013	TIC's
[SW]	Otros Free	Gerencia
[SW]	SIAF (SP-ERP)	TIC's
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's
IMPRESORAS		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's

Tabla 1. (Continuación).

Tipo	Descripción	Propietario
[SW]	Adobe Flash Player	TIC's
[SW]	Aranda	TIC's
[SW]	Office 2010	TIC's
[SW]	Otros Free	Soporte
[SW]	Winrar	TIC's
SUBGERENCIA JURÍDICA		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Intranet	TIC's
[SW]	KASPERSKY	TIC's
[SW]	Office 2010	TIC's
[SW]	Office 2013	TIC's
[SW]	Otros Free	Jurídica
[SW]	SIAF (SP-ERP)	TIC's
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's
DIRECCIÓN DE MODOS ALTERNATIVOS		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Autocad	TIC's
[SW]	Intranet	TIC's
[SW]	KASPERSKY	TIC's
[SW]	Office 2010	TIC's
[SW]	Office 2013	TIC's
[SW]	Otros Free	Modos
[SW]	SIAF (SP-ERP)	TIC's
[SW]	Transcad	TIC's
[SW]	Vissim	TIC's
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's

Tabla 1. (Continuación).

Tipo	Descripción	Propietario
NEGOCIOS		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Creative Cloud	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Cliente Oracle-Home	TIC's
[SW]	Intranet	TIC's
[SW]	KASPERSKY	TIC's
[SW]	Office 2010	TIC's
[SW]	Office 2013	TIC's
[SW]	Otros Free	Negocios
[SW]	SIAF (SP-ERP)	TIC's
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's
PORTALES		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Intranet	TIC's
[SW]	KASPERSKY	TIC's
[SW]	Office 2013	TIC's
[SW]	Otros Free	Portales
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's
RECEPCIÓN		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Office 2007	TIC's
[SW]	Otros Free	Recepción
[SW]	Winrar	TIC's
SOPORTE TÉCNICO		
[HW]	PC (Escritorio)	Usuario

Tabla 1. (Continuación).

Tipo	Descripción	Propietario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Aranda	TIC's
[SW]	Intranet	TIC's
[SW]	KASPERSKY	TIC's
[SW]	Office 2013	TIC's
[SW]	Office 365	TIC's
[SW]	Otros Free	Soporte
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's
DIRECCIÓN TÉCNICA Y DE SERVICIOS		
[HW]	PC (Escritorio)	Usuario
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Arcgis	TIC's
[SW]	Autocad	TIC's
[SW]	Cliente Oracle-Home	TIC's
[SW]	Emme	TIC's
[SW]	IBM SPSS	TIC's
[SW]	Intranet	TIC's
[SW]	KASPERSKY	TIC's
[SW]	Office 2010	TIC's
[SW]	Office 2013	TIC's
[SW]	Office 365	TIC's
[SW]	Otros Free	Técnica
[SW]	SIAF (SP-ERP)	TIC's
[SW]	Transcad	TIC's
[SW]	Vissim	TIC's
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's
DIRECCIÓN DE TIC's		
[HW]	Aire acondicionado	TIC's

Tabla 1. (Continuación).

Tipo	Descripción	Propietario
[HW]	Firewall Sonic Wall	TIC's
[HW]	PC (Escritorio)	Usuario
[HW]	PC (Portátil)	Usuario
[HW]	Planta telefónica	TIC's
[HW]	Servidores	TIC's
[SW]	Acrobat Reader	TIC's
[SW]	Adobe Flash Player	TIC's
[SW]	Aranda	TIC's
[SW]	Arcgis	TIC's
[SW]	Cliente Oracle-Home	TIC's
[SW]	IBM SPSS	TIC's
[SW]	Intranet	TIC's
[SW]	KASPERSKY	TIC's
[SW]	Office 2010	TIC's
[SW]	Office 2013	TIC's
[SW]	Office 365	TIC's
[SW]	Otros Free	TIC's
[SW]	SIAF (SP-ERP)	TIC's
[SW]	SQL Developer	TIC's
[SW]	TOAD	TIC's
[SW]	Transcad	TIC's
[SW]	Winrar	TIC's
[D]	CAT	TIC's
[D]	Cordis	TIC's
[D]	Royal	TIC's
[COM]	Concentradores	TIC's
[COM]	Firewall físico	TIC's
[COM]	Switch de borde (25)	TIC's
[COM]	Switch de Core	TIC's
[COM]	Unidad SAN	TIC's
[COM]	UPS	TIC's
[AUX]	Antenas	TIC's
[AUX]	Cableado	TIC's
[AUX]	Generador Eléctrico	TIC's
[AUX]	Mobiliario	TIC's
[AUX]	Otros equipos auxiliares	TIC's

Tabla 1. (Continuación).

Tipo	Descripción	Propietario
[AUX]	Radios	TIC's
[AUX]	Sistema de alimentación ininterrumpida	TIC's
[AUX]	Sistemas de vigilancia	TIC's
[L]	Centro de procesamiento	TIC's
[P]	Director	TIC's
[P]	Profesional Se Seguridad	TIC's
[P]	Profesional de Bases de Datos	TIC's
[P]	Otros profesionales	TIC's
[P]	Técnicos	TIC's
[P]	Soporte	TIC's

Fuente: Transmilenio S.A. Inventario de Activos diciembre 2016

Siguiendo el modelo de la metodología Magerit en su versión 3.0 se presenta la traducción de los activos más relevantes, de acuerdo al estándar de la metodología para luego proceder a su valoración y análisis.

[SW] Aplicaciones (Software)

Según la metodología Magerit 3.0, se puede definir el Software como se muestra a continuación:

Tabla 2. Aplicaciones (Software)

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[SIS]	Aplicaciones	[SIS_TMRAG]	Remuneración de agentes
[DBMS]	Gestión de base de datos	[DBMS_TMBD]	Base de Datos
[SUB]	Desarrollo a medida	[SUB_TMSIA]	SIAF (SP-ERP)
[SUB]	Desarrollo a medida	[SUB_TMTOA]	TOAD
[OTR]	Otros Software	[OTR_TMCOR]	Cordis
[OTR]	Otros Software	[SUB_TMCAT]	CAT

Tabla 2. (Continuación).

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[AV]	Antivirus	[AV_TMKAS]	Kaspersky

Fuente: El Autor

[HW] Equipos

La empresa posee los siguientes equipos, los cuales se definirán de acuerdo a la metodología

Tabla 3. Hardware

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[HOST]	Grandes Equipos	[HOST_TM]	Equipos Terminales Usuarios
[NETWORK]	Soportes de la red	[NETWORK_TM]	Equipos y dispositivos de red
[SDB]	Servidores	[SDB_TM]	Servidores
[PRINT]	Medios de impresión	[PRINT_TM]	Impresoras

Fuente: El Autor

[COM] Comunicaciones

Lo siguientes medios de comunicación se encuentran en la empresa y se definen según la metodología:

Tabla 4. Comunicaciones

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[ROUTER]	Enrutadores	[ROUTER_TM]	Concentradores
[SWITCH]	Conmutadores	[SWITCH_TM]	Switch de borde (25)
[SWITCH]	Conmutadores	[SWITCH_TM]	Switch de Core
[LAN]	Red LAN	[LAN_TM]	Red interna networking
[BP]	Dispositivos de Frontera	[BP_TM]	Firewall Físico

Fuente: El Autor

[MEDIA] Soportes de información

La entidad tiene los siguientes soportes de información

Tabla 5. Soportes de información

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[SAN]	Almacenamiento de red	[SAN _TM]	Unidad SAN

Fuente: El Autor

[AUX] Equipamiento Auxiliar

Se tiene el siguiente equipamiento auxiliar

Tabla 6. Equipamiento auxiliar

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[GEN]	Generador Eléctrico	[GEN_TM]	Generador de energía
[CABLING]	Cableado	[CABLING_TM]	Red interna
[MOB]	Mobiliario	[MOB_TM]	Muebles
[SISVG]	Sistema de Vigilancia	[SISVG_TM]	Vigilancia
[ANT]	Antenas	[ANT_TM]	Antenas
[RAD]	Radios	[RAD_TM]	Radios
[SAI]	Sistema de alimentación ininterrumpida	[SAI_TM]	UPS
[AUXOTR]	Otros Equipos Auxiliares	[AUXOTR_TM]	Otros Equipos

Fuente: El Autor

11.3 Anexo C: Valoración de Activos

No todos los activos relacionados anteriormente tienen suficiente la importancia, esto depende de la vulnerabilidad a la que se someten, por lo tanto, es necesario aplicar una calificación cualitativa, la cual se toma de referencia del catálogo de elementos del libro 2 de la metodología MAGERIT en su versión 3.0 según la dimensionalidad.

Tabla 7. Tabla de Valoración

Rango	Valor	Criterio
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: Magerit Versión 3.0

Dimensiones

[D] disponibilidad

[I] integridad de los datos

[C] confidencialidad de los datos

[A] autenticidad de los usuarios y de la información

[T] trazabilidad del servicio y de los datos.

A continuación, se presentan cada uno de los activos con su correspondiente calificación de acuerdo a las dimensiones anteriormente mencionadas, lo que permite identificar la importancia de cada uno de los activos.

Tabla 8. Valoración Aplicaciones

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de seguridad	Criterio
APLICACIONES					
[SIS]	Aplicaciones	[SIS_TMRMA]	Remuneración de agentes	Integridad	9
				Confidencialidad	9
				Autenticidad	9
				Trazabilidad	9
[DBMS]	Gestión de base de datos	[DBMS_TMBD]	Base de Datos	Disponibilidad	10
				Integridad	9
				Confidencialidad	9
				Autenticidad	9
				Trazabilidad	9
[SUB]	Desarrollo a medida	[SUB_TMSIA]	SIAF (SP-ERP)	Disponibilidad	9
				Confidencialidad	7
[SUB]	Desarrollo a medida	[SUB_TMTOA]	TOAD	Disponibilidad	9
				Confidencialidad	7
[OTR]	Otros Software	[OTR_TMCOR]	Cordis	Trazabilidad	7
[OTR]	Otros Software	[SUB_TMCAT]	CAT	Trazabilidad	7
[AV]	Antivirus	[AV_TMKAS]	Kaspersky	Trazabilidad	7

Fuente: El Autor

Tabla 9. Valoración Equipos y comunicaciones

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de seguridad	Criterio
EQUIPOS					
[NETWORK]	Soportes de la red	[NETWORK_TM]	Equipos y dispositivos de red	Integridad	9
				Confidencialidad	9
				Autenticidad	9
				Trazabilidad	9
[HOST]	Grandes Equipos	[HOST_TM]	Equipos Terminales Usuarios	Trazabilidad	6
[SDB]	Servidores	[SDB_TM]	Servidores	Trazabilidad	8
[PRINT]	Medios de impresión	[PRINT_TM]	Impresoras	Trazabilidad	8
COMUNICACIONES					
[ROUTER]	Enrutadores	[ROUTER_TM	Concentrado	Trazabilidad	8
[SWITCH]	Conmutadores	[SWITCH_TM]	Switch de borde (25)	Trazabilidad	8
[SWITCH]	Conmutadores	[SWITCH_TM]	Switch de Core	Trazabilidad	8
[LAN]	Red LAN	[LAN_TM]	Red interna	Trazabilidad	7
[BP]	Dispositivos de Frontera	[BP_TM]	Firewall Físico	Integridad	9
				Confidencialidad	9
				Autenticidad	9
				Trazabilidad	9

Fuente: El Autor

Tabla 10. Valoración Equipos Auxiliares y Soportes de Información

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de seguridad	Criterio
EQUIPOS AUXILIARES					
[GEN]	Generador Eléctrico	[GEN_TM]	Generador de energía	Disponibilidad	7
[CABLING]	Cableado	[CABLING_TM]	Red interna	Disponibilidad	7
[MOB]	Mobiliario	[MOB_TM]	Muebles	Disponibilidad	7
[SISVG]	Sistema de Vigilancia	[SISVG_TM]	Vigilancia	Disponibilidad	7
[ANT]	Antenas	[ANT_TM]	Antenas	Disponibilidad	7
[RAD]	Radios	[RAD_TM]	Radios	Disponibilidad	7
[SAI]	Sistema de alimentación ininterrumpida	[SAI_TM]	UPS	Disponibilidad	7
[AUXOTR]	Otros Equipos Auxiliares	[AUXOTR_TM]	Otros Equipos	Disponibilidad	7
SOPORTES DE INFORMACION					
[SAN]	Almacenamiento de red	[SAN _TM]	Unidad SAN	Integridad	7
				Confidencialidad	7

Fuente: El Autor

11.4 Anexo D: Caracterización de las Amenazas

Magerit en su versión 3.0, clasifica las amenazas en cuatro grupos:

[N] Desastres Naturales: Sucesos que pueden ocurrir sin intervención del ser humano.

[I] De origen industrial: Eventos que pueden ocurrir de forma accidental y se derivan de las actividades humanas.

[E] Errores y fallos no intencionados: son fallas que no son intencionales las cuales son causadas por las personas.

[A] Ataque intencionados: Fallas que son causadas por personas de forma deliberada.

La identificación de las amenazas se realiza con base en el rango indicado en la metodología Magerit, y se determinan las amenazas con sus respectivas valoraciones.

Escala de rango de frecuencia de amenazas

Tabla 11. Tabla de valoración por vulnerabilidad

Vulnerabilidad	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada semana	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Fuente: Magerit Versión 3.0

Escala de rango porcentual de impactos en los activos para cada dimensión de seguridad.

Tabla 12. Tabla de valoración por impacto

Impacto	Valor cuantitativo
Muy alto	100
Alto	75
Medio	50
Bajo	20
Muy bajo	5

Fuente: Magerit Versión 3.0

Tabla 13. Valoración de Amenazas

RELACIÓN DE AMENAZA POR ACTIVO IDENTIFICANDO SU FRECUENCIA E IMPACTO							
Activo	Amenazas	Fre	Impacto por cada dimensión				
			[A]	[C]	[I]	[D]	[T]
[SIS_TMRMA] Remuneración de agentes	[A.6] Abusivo de privilegios de acceso	10	100	100	100	100	100
	[A.23] Manipulación del hardware	10	100	100	100	100	100
[DBMS_TMBD] Base de Datos	[A.6] Abusivo de privilegios de acceso	5	100	100	100	100	100
	[A.23] Manipulación del hardware	5	100	100	100	100	100
[SUB_TMSIA] SIAF (SP-ERP)	[A.6] Abusivo de privilegios de acceso	5	25	25	25	25	25
	[A.23] Manipulación del hardware	5	25	10	25	25	25
[SUB_TMTOA] TOAD	[A.7] Uso no previsto	5	100	100	100	100	100
	[A.11] Acceso no autorizado	5	100	100	100	100	100
[OTR_TMCOR] Cordis	[A.7] Uso no previsto	5	100	100	100	100	100
	[A.11] Acceso no autorizado	5	100	100	100	100	100
	[A.14] Interceptación de información (escucha)	5	100	100	100	100	100
[SUB_TMCAT] CAT	[A.7] Uso no previsto	5	100	100	100	100	100
	[A.11] Acceso no autorizado	5	100	100	100	100	100
	[A.14] Interceptación de información (escucha)	5	100	100	100	100	100
[AV_TMKAS] Kaspersky	[E.15] Alteración de la información	5	50	100	100	100	50
	[A.15] Modificación de la información	5	50	100	100	100	50
	[A.25] Robo de equipos	10	50	100	100	100	50

Tabla 13. (Continuación).

[NETWORK_TM] Equipos y dispositivos de red	[A.23] Manipulación de equipos	10	20	20	20	100	20
	[A.24] Denegación de servicio	5	20	20	20	100	20
	[A.14] Interceptación de información (escucha)	5	20	20	20	100	20
[HOST_TM] Equipos Terminales Usuarios	[A.7] Uso no previsto	5	20	20	20	100	20
	[A.11] Acceso no autorizado	5	20	20	20	100	20
	[A.23] Manipulación de equipos	5	20	20	20	100	20
[SDB_TM] Servidores	[A.7] Uso no previsto	5	20	20	20	100	20
	[A.11] Acceso no autorizado	5	20	20	20	100	20
	[A.23] Manipulación de equipos	5	20	20	20	100	20
[PRINT_TM] Impresoras	[A.7] Uso no previsto	10	5	5	5	100	5
	[A.11] Acceso no autorizado	10	5	5	5	100	5
	[A.23] Manipulación de equipos	5	5	5	5	100	5
[ROUTER_TM] Concentradores	[A.23] Manipulación de equipos	5	100	100	100	100	100
	[A.24] Denegación de servicio	5	100	100	100	100	100
	[A.14] Interceptación de información (escucha)	5	100	100	100	100	100
[SWITCH_TM] Switch de borde (25)	[A.23] Manipulación de equipos	5	100	100	100	100	100
	[A.24] Denegación de servicio	5	100	100	100	100	100
	[A.14] Interceptación de información (escucha)	5	100	100	100	100	100

Tabla 13. (Continuación).

[SWITCH_TM] Switch de core	[A.23] Manipulación de equipos	5	100	100	100	100	100
	[A.24] Denegación de servicio	5	100	100	100	100	100
	[A.14] Interceptación de información (escucha)	5	100	100	100	100	100
[LAN_TM] Red interna networking	[A.23] Manipulación de equipos	10	100	100	100	100	100
	[A.24] Denegación de servicio	10	100	100	100	100	100
	[A.14] Interceptación de información (escucha)	10	100	100	100	100	100
[BP_TM] Firewall Físico	[A.23] Manipulación de equipos	10	100	100	100	100	100
	[A.24] Denegación de servicio	10	100	100	100	100	100
	[A.14] Interceptación de información (escucha)	10	100	100	100	100	100
[SAN _TM] Unidad SAN	[E.04] Errores de configuración	5	50	100	100	100	50
	[A.6] Abusivo de privilegios de acceso	5	50	100	100	100	100
	[E.02] Errores del administrador	5	50	100	100	100	100
[GEN_TM] Generador de energía	[N.01] Fuego	10	50	50	50	75	50
	[N.02] Daños por agua	10	50	50	50	75	50
	[N] Desastres naturales	10	50	50	50	75	50
	[I.06] Corte del suministro eléctrico	10	50	50	50	75	50
[CABLING_TM] Red interna	[N.01] Fuego	10	50	50	50	75	50
	[N.02] Daños por agua	10	50	50	50	75	50
	[N] Desastres naturales	10	50	50	50	75	50
	[I.06] Corte del suministro eléctrico	10	50	50	50	75	50

Tabla 13. (Continuación).

[RAD_TM] Radios	[N.01] Fuego	10	50	50	50	75	50
	[N.02] Daños por agua	10	50	50	50	75	50
	[N] Desastres naturales	5	50	50	50	75	50
	[I.06] Corte del suministro eléctrico	10	50	50	50	75	50
[SAI_TM] UPS	[N.01] Fuego	5	50	50	50	75	50
	[N.02] Daños por agua	5	50	50	50	75	50
	[N.] Desastres naturales	5	50	50	50	75	50
	[I.06] Corte del suministro eléctrico	5	50	50	50	75	50
[AUXOTR_TM] Otros Equipos	[N.01] Fuego	5	50	50	50	75	50
	[N.02] Daños por agua	5	20	50	50	75	20
	[N] Desastres naturales	5	50	50	50	75	50
	[I.06] Corte del suministro eléctrico	5	50	50	20	75	50

Fuente: El Autor

11.5 Anexo E: Valoración de Riesgos

El valor NR (Nivel de Riesgo) obedece al Mapa de Riesgos:

Tabla 14. Mapa Nivel de Riesgo

Riesgo = Probabilidad * Impacto						
Probabilidad	5	5	10	15	25	40
	4	4	8	12	20	32
	3	3	6	9	15	24
	2	2	4	6	10	16
	1	1	2	3	5	8
		1	2	3	5	8
		Impacto				

Fuente: Magerit 3.0

Tabla 15. Cálculo Nivel de Riesgos

Nivel de Riesgo	
4	Extremo
3	Intolerable
2	Tolerable
1	Aceptable

Fuente: Magerit 3.0

Estimación del impacto teniendo en cuenta la siguiente tabla:

Tabla 16. Estimación Impacto

Impacto		Degradación		
		1%	50%	100%
VALOR DEL ACTIVO	Muy alto	3	5	8
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy bajo	1	1	1

Fuente: Magerit 3.0

La siguiente tabla presenta la relación de amenaza por activo, identificando su nivel de riesgo:

Tabla 17. Amenazas por activo con Nivel de Riesgo

Activo	Amenazas	Frecuencia	Impacto Medio	Impacto estimado	Riesgo	NR	
[SIS_TMRMA] Remuneración de agentes	[A.6] Abusivo de privilegios de acceso	10	100%	3	30	4	Extremo
	[A.23] Manipulación del hardware	10	100%	2	20	4	Extremo
[DBMS_TMBD] Base de Datos	[A.6] Abusivo de privilegios de acceso	5	100%	2	10	3	Intolerable
	[A.23] Manipulación del hardware	5	100%	1	5	2	Tolerable
[SUB_TMSIA] SIAF (SP-ERP)	[A.6] Abusivo de privilegios de acceso	5	25%	3	15	4	Extremo
	[A.23] Manipulación del hardware	5	22%	2	10	3	Intolerable
[SUB_TMTOA] TOAD	[A.7] Uso no previsto	5	100%	2	10	3	Intolerable
	[A.11] Acceso no autorizado	5	100%	1	5	2	Tolerable
[OTR_TMCOR] Cordis	[A.7] Uso no previsto	5	100%	1	5	2	Tolerable
	[A.11] Acceso no autorizado	5	100%	1	5	2	Tolerable
	[A.14] Interceptación de información (escucha)	5	100%	1	5	2	Tolerable
[SUB_TMCAT] CAT	[A.7] Uso no previsto	5	100%	2	10	3	Intolerable
	[A.11] Acceso no autorizado	5	80%	5	25	4	Extremo
	[A.14] Interceptación de información (escucha)	5	80%	5	25	4	Extremo

Tabla 17. (Continuación).

[AV_TMKAS] Kaspersky	[E.15] Alteración de la información	5	80%	1	5	2	Tolerable
	[A.15] Modificación de la información	10	80%	1	10	3	Intolerable
	[A.25] Robo de equipos	10	36%	3	30	4	Extremo
[NETWORK_TM] Equipos y dispositivos de red	[A.23] Manipulación de equipos	5	36%	2	10	3	Intolerable
	[A.24] Denegación de servicio	5	36%	1	5	2	Tolerable
	[A.14] Interceptación de información (escucha)	5	36%	1	5	2	Tolerable
[HOST_TM] Equipos Terminales Usuarios	[A.7] Uso no previsto	5	36%	1	5	2	Tolerable
	[A.11] Acceso no autorizado	5	36%	1	5	2	Tolerable
	[A.23] Manipulación de equipos	5	36%	1	5	2	Tolerable
[SDB_TM] Servidores	[A.7] Uso no previsto	5	36%	5	25	4	Tolerable
	[A.11] Acceso no autorizado	5	36%	3	15	4	Extremo
	[A.23] Manipulación de equipos	10	24%	3	30	4	Extremo
[PRINT_TM] Impresoras	[A.7] Uso no previsto	10	24%	5	50	4	Extremo
	[A.11] Acceso no autorizado	5	24%	2	10	3	Intolerable
	[A.23] Manipulación de equipos	5	100%	3	15	4	Extremo
[ROUTER_TM] Concentradores	[A.23] Manipulación de equipos	5	100%	3	15	4	Extremo
	[A.24] Denegación de servicio	5	100%	1	5	2	Tolerable
	[A.14] Interceptación de información (escucha)	5	100%	1	5	2	Tolerable
[SWITCH_TM] Switch de borde (25)	[A.23] Manipulación de equipos	5	100%	1	5	2	Tolerable
	[A.24] Denegación de servicio	5	100%	2	10	3	Intolerable

Tabla 17. (Continuación).

	[A.14] Interceptación de información (escucha)	10	100%	2	20	4	Extremo
[SWITCH_TM] Switch de core	[A.23] Manipulación de equipos	10	100%	2	20	4	Extremo
	[A.24] Denegación de servicio	10	100%	5	50	4	Extremo
	[A.14] Interceptación de información (escucha)	10	100%	2	20	4	Extremo
[LAN_TM] Red interna networking	[A.23] Manipulación de equipos	10	100%	2	20	4	Extremo
	[A.24] Denegación de servicio	10	100%	1	10	3	Intolerable
	[A.14] Interceptación de información (escucha)	5	100%	2	10	3	Intolerable
[BP_TM] Firewall Físico	[A.23] Manipulación de equipos	5	100%	2	10	3	Intolerable
	[A.24] Denegación de servicio	5	100%	5	25	4	Extremo
	[A.14] Interceptación de información (escucha)	5	80%	3	15	4	Extremo
[SAN _TM] Unidad SAN	[E.04] Errores de configuración	5	90%	3	15	4	Extremo
	[A.6] Abusivo de privilegios de acceso	5	90%	5	25	4	Extremo
	[E.02] Errores del administrador	10	55%	3	30	4	Extremo
[GEN_TM] Generador de energía	[N.01] Fuego	10	55%	3	30	4	Extremo
	[N.02] Daños por agua	10	55%	5	50	4	Extremo
	[N] Desastres naturales	10	55%	2	20	4	Extremo
	[I.06] Corte del suministro eléctrico	10	55%	3	30	4	Extremo

Tabla 17. (Continuación).

[CABLING_TM] Red interna	[N.01] Fuego	10	55%	3	30	4	Extremo
	[N.02] Daños por agua	10	55%	1	10	3	Intolerable
	[N] Desastres naturales	10	55%	1	10	3	Intolerable
	[I.06] Corte del suministro eléctrico	10	55%	1	10	3	Intolerable
[RAD_TM] Radios	[N.01] Fuego	10	55%	2	20	4	Extremo
	[N.02] Daños por agua	5	55%	2	10	3	Intolerable
	[N] Desastres naturales	10	55%	2	20	4	Extremo
	[I.06] Corte del suministro eléctrico	5	55%	5	25	4	Extremo
[SAI_TM] UPS	[N.01] Fuego	5	55%	2	10	3	Intolerable
	[N.02] Daños por agua	5	55%	2	10	3	Intolerable
	[N.] Desastres naturales	5	55%	1	5	2	Tolerable
	[I.06] Corte del suministro eléctrico	5	55%	2	10	3	Intolerable
[AUXOTR_TM] Otros Equipos	[N.01] Fuego	5	43%	2	10	3	Intolerable
	[N.02] Daños por agua	5	55%	5	25	4	Extremo
	[N] Desastres naturales	5	49%	3	15	4	Extremo
	[I.06] Corte del suministro eléctrico	5	49%	3	15	4	Extremo

Fuente: El Autor

11.6 Anexo F: Matriz de Riesgos Residuales

La estimación del riesgo residual acumulado indica la medida en que las amenazas afectan a los activos de orden superior que dependen de dicho activo. El cálculo de la matriz del riesgo residual se hace con base a la siguiente información:

Tabla 18. Parámetros para el cálculo de Amenazas

Probabilidad		Impacto: Menor 1	Moderado 2	Importante 3	Catastrófico 4
Casi seguro	1	Medio	Alto	Critico	Critico
Muy Probable	0,75	Medio	Medio	Alto	Critico
Probable	0,5	Bajo	Medio	Medio	Alto
Poco Probable	0,25	Bajo	Bajo	Medio	Alto

Critico
Alto
Medio
Bajo

Fuente: Magerit 3.0

Tabla 19. Nivel de aceptabilidad

Criterio	Acciones
Critico	Atención de inmediato
Alto	
Medio	Aceptar
Bajo	

Fuente: Magerit 3.0

Para la identificación del Impacto y el Riesgo Residual se utilizaron las siguientes abreviaturas:

Impacto: IM = Importante, CA = Catastrófico, MO = Moderado

Riesgo Residual: CR = Crítico, AL = Alto, ME = Medio, BA = Bajo

Tabla 20. Evaluación Riesgo Residual

Activo	Amenazas	Frecuencia	Impacto Medio	Impacto estimado	Riesgo	NR		Probabilidad	Impacto	Riesgo Residual
[SIS_TMRMA] Remuneración de agentes	[A.6] Abusivo de privilegios de acceso	10	100%	3	30	4	Extremo	C S	CA	CR
	[A.23] Manipulación del hardware	10	100%	2	20	4	Extremo	C S	CA	CR
[DBMS_TMBD] Base de Datos	[A.6] Abusivo de privilegios de acceso	5	100%	2	10	3	Intolerable	C S	IM	CR
	[A.23] Manipulación del hardware	5	100%	1	5	2	Tolerable	C S	MO	AL
[SUB_TMSIA] SIAF (SP-ERP)	[A.6] Abusivo de privilegios de acceso	5	25%	3	15	4	Extremo	C S	CA	CR
	[A.23] Manipulación del hardware	5	22%	2	10	3	Intolerable	C S	IM	CR
[SUB_TMTOA] TOAD	[A.7] Uso no previsto	5	100%	2	10	3	Intolerable	C S	IM	CR
	[A.11] Acceso no autorizado	5	100%	1	5	2	Tolerable	C S	MO	AL
[OTR_TMCOR] Cordis	[A.7] Uso no previsto	5	100%	1	5	2	Tolerable	C S	MO	AL
	[A.11] Acceso no autorizado	5	100%	1	5	2	Tolerable	C S	MO	AL
	[A.14] Interceptación de información (escucha)	5	100%	1	5	2	Tolerable	C S	MO	AL
[SUB_TMCAT] CAT	[A.7] Uso no previsto	5	100%	2	10	3	Intolerable	C S	IM	CR
	[A.11] Acceso no autorizado	5	80%	5	25	4	Extremo	C S	CA	CR

Tabla 20. (Continuación).

	[A.14] Interceptación de información (escucha)	5	80%	5	25	4	Extremo	CS	CA	CR
[AV_TMKAS] Kaspersky	[E.15] Alteración de la información	5	80%	1	5	2	Tolerable	CS	MO	AL
	[A.15] Modificación de la información	10	80%	1	10	3	Intolerable	CS	IM	CR
	[A.25] Robo de equipos	10	36%	3	30	4	Extremo	CS	CA	CR
[NETWORK_TM] Equipos y dispositivos de red	[A.23] Manipulación de equipos	5	36%	2	10	3	Intolerable	CS	IM	CR
	[A.24] Denegación de servicio	5	36%	1	5	2	Tolerable	CS	IM	CR
	[A.14] Interceptación de información (escucha)	5	36%	1	5	2	Tolerable	CS	MO	AL
[HOST_TM] Equipos Terminales Usuarios	[A.7] Uso no previsto	5	36%	1	5	2	Tolerable	CS	IM	CR
	[A.11] Acceso no autorizado	5	36%	1	5	2	Tolerable	CS	IM	CR
	[A.23] Manipulación de equipos	5	36%	1	5	2	Tolerable	CS	IM	CR
[SDB_TM] Servidores	[A.7] Uso no previsto	5	36%	5	25	4	Tolerable	CS	IM	CR
	[A.11] Acceso no autorizado	5	36%	3	15	4	Extremo	CS	CA	CR
	[A.23] Manipulación de equipos	10	24%	3	30	4	Extremo	CS	CA	CR
[PRINT_TM] Impresoras	[A.7] Uso no previsto	10	24%	5	50	4	Extremo	CS	CA	CR
	[A.11] Acceso no autorizado	5	24%	2	10	3	Intolerable	CS	IM	CR

Tabla 20. (Continuación).

	[A.23] Manipulación de equipos	5	100%	3	15	4	Extremo	CS	CA	CR
[ROUTER_TM] Concentradores	[A.23] Manipulación de equipos	5	100%	3	15	4	Extremo	CS	CA	CR
	[A.24] Denegación de servicio	5	100%	1	5	2	Tolerable	CS	MO	AL
	[A.14] Interceptación de información (escucha)	5	100%	1	5	2	Tolerable	CS	MO	AL
[SWITCH_TM] Switch de borde (25)	[A.23] Manipulación de equipos	5	100%	1	5	2	Tolerable	CS	MO	AL
	[A.24] Denegación de servicio	5	100%	2	10	3	Intolerable	CS	IM	CR
	[A.14] Interceptación de información (escucha)	10	100%	2	20	4	Extremo	CS	CA	CR
[SWITCH_TM] Switch de core	[A.23] Manipulación de equipos	10	100%	2	20	4	Extremo	CS	CA	CR
	[A.24] Denegación de servicio	10	100%	5	50	4	Extremo	CS	CA	CR
	[A.14] Interceptación de información (escucha)	10	100%	2	20	4	Extremo	CS	CA	CR
[LAN_TM] Red interna networking	[A.23] Manipulación de equipos	10	100%	2	20	4	Extremo	CS	CA	CR
	[A.24] Denegación de servicio	10	100%	1	10	3	Intolerable	CS	IM	CR

Tabla 20. (Continuación).

	[A.14] Interceptación de información (escucha)	5	100%	2	10	3	Intolerable	CS	IM	CR
[BP_TM] Firewall Físico	[A.23] Manipulación de equipos	5	100%	2	10	3	Intolerable	CS	IM	CR
	[A.24] Denegación de servicio	5	100%	5	25	4	Extremo	CS	CA	CR
	[A.14] Interceptación de información (escucha)	5	80%	3	15	4	Extremo	CS	CA	CR
[SAN _TM] Unidad SAN	[E.04] Errores de configuración	5	90%	3	15	4	Extremo	CS	CA	CR
	[A.6] Abusivo de privilegios de acceso	5	90%	5	25	4	Extremo	CS	CA	CR
	[E.02] Errores del administrador	10	55%	3	30	4	Extremo	CS	CA	CR
[GEN_TM] Generador de energía	[N.01] Fuego	10	55%	3	30	4	Extremo	CS	CA	CR
	[N.02] Daños por agua	10	55%	5	50	4	Extremo	CS	CA	CR
	[N] Desastres naturales	10	55%	2	20	4	Extremo	CS	CA	CR
	[I.06] Corte del suministro eléctrico	10	55%	3	30	4	Extremo	CS	CA	CR
[CABLING_TM] Red interna	[N.01] Fuego	10	55%	3	30	4	Extremo	CS	CA	CR
	[N.02] Daños por agua	10	55%	1	10	3	Intolerable	CS	IM	CR
	[N] Desastres naturales	10	55%	1	10	3	Intolerable	CS	IM	CR
	[I.06] Corte del suministro eléctrico	10	55%	1	10	3	Intolerable	CS	IM	CR

Tabla 20. (Continuación).

[RAD_TM] Radios	[N.01] Fuego	10	55%	2	20	4	Extremo	CS	CA	CR
	[N.02] Daños por agua	5	55%	2	10	3	Intolerable	CS	IM	CR
	[N] Desastres naturales	10	55%	2	20	4	Extremo	CS	CA	CR
	[I.06] Corte del suministro eléctrico	5	55%	5	25	4	Extremo	CS	CA	CR
[SAI_TM] UPS	[N.01] Fuego	5	55%	2	10	3	Intolerable	CS	IM	CR
	[N.02] Daños por agua	5	55%	2	10	3	Intolerable	CS	IM	CR
	[N.] Desastres naturales	5	55%	1	5	2	Tolerable	CS	MO	AL
	[I.06] Corte del suministro eléctrico	5	55%	2	10	3	Intolerable	CS	IM	CR
[AUXOTR_TM] Otros Equipos	[N.01] Fuego	5	43%	2	10	3	Intolerable	CS	IM	CR
	[N.02] Daños por agua	5	55%	5	25	4	Extremo	CS	CA	CR
	[N] Desastres naturales	5	49%	3	15	4	Extremo	CS	CA	CR
	[I.06] Corte del suministro eléctrico	5	49%	3	15	4	Extremo	CS	CA	CR

Fuente: El Autor

11.7 Anexo G: Dominios y Controles del Estándar ISO/IEC 27001

De acuerdo a los activos de la empresa Transmilenio S.A., se evaluaron los siguientes dominios:

Tabla 21. Dominios y Controles a Evaluar

Dominios a evaluar	Controles
A.5 POLITICAS DE LA SEGURIDAD DE LA INFORMACIÓN	A.5.1. Políticas de Seguridad de Información
	A.5.1.1 Políticas para la seguridad
	A.5.1.2 Revisión de las políticas para la seguridad de la información
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A.6.1. Organización de la Seguridad de Información
	A.6.1.1 Roles y responsabilidades para la seguridad de la información
	A.6.1.2 Separación de deberes
	A.6.1.3 Contacto con las autoridades
	A.6.1.4 Contacto con grupos de interés especial
	A.6.1.5 Seguridad de la Información en la gestión de
	proyectos
	A.6.2.1 Política para dispositivos móviles
	A.6.2.2 Teletrabajo
A.7 ADMINISTRACION DE ACTIVOS	A.7.1. Responsabilidad por Activos
	A.7.1.1 Inventario de Activos
	A.7.1.2 Propiedad de Activos
	A.7.1.3 Uso aceptable de Activos
	A.7.2. Clasificación de la Información
	A.7.2.1 Directrices de Clasificación
	A.7.2.2 Etiquetado y manejo de información
A.9 SEGURIDAD FISICA Y DEL ENTORNO	A.9.1. Áreas Seguras
	A.9.1.1 Perímetro de Seguridad Física
	A.9.1.2 Controles Físicos de Entrada
	A.9.1.3 Aseguramiento de Oficinas, Salas de Servidores e Instalaciones

Tabla 21. (Continuación).

	A.9.1.4 Protección contra Amenazas Exteriores y Ambientales/Climáticas
	A.9.1.5 Trabajando en Áreas Seguras
	A.9.1.6 Zonas de Acceso Público, Entrega y Descarga
	9.2 Equipamiento de Seguridad
	A.9.2.1 Equipamiento y Protección del Sitio
	A.9.2.2 Utilidades Soportadas
	A.9.2.3 Cableado de Seguridad
	A.9.2.4 Mantenimiento de Equipos
	A.9.2.5 Aseguramiento de Equipos fuera de las Oficinas
	A.9.2.6 Disposiciones de Seguridad de Reutilización de Equipos
	A.9.2.7 Autorizaciones de Sacar Equipos
A.10 GESTION DE COMUNICACIONES Y OPERACIONES	10.1. Procedimientos y Responsabilidades Operativas
	A.10.1.1 Documentación de Procedimientos Operativos
	A.10.1.2 Manejo de Cambios
	A.10.1.3 Segregación de Tareas
	A.10.1.4 Separación de desarrollo, test e instalaciones operativas
	10.2. Manejo de Entrega de Servicios Tercerizados
	A.10.2.1 Entrega de Servicios
	A.10.2.2 Monitoreo y revisión de servicios tercerizados
	A.10.2.3 Manejo de Cambios de servicios tercerizados
	10.3. Planeamiento y Aceptación de Sistemas
	A.10.3.1 Gestión de la Capacidad
	A.10.3.2 Aceptación de Sistemas
	10.4. Protección contra código malicioso y móvil
	A.10.4.1 Controles contra código malicioso
	A.10.4.2 Controles contra código móvil
	10.5. Copias de Respaldo
	A.10.5.1 Respaldo de la Información
	10.6. Administración de la Seguridad de la Red
	A.10.6.1 Controles de Red

Tabla 21. (Continuación).

	A.10.6.2 Seguridad en los Servicios de Red
	10.7. Manejo de Medios
	A.10.7.1 Manejo de medios removibles
	A.10.7.2 Disposición de los medios
	A.10.7.3 Procedimientos de manejo de la información
	A.10.7.4 Seguridad en la Documentación de los Sistemas
	10.8. Intercambio de Información
	A.10.8.1 Políticas y Procedimientos de intercambio de información
	A.10.8.2 Acuerdos de Intercambio
	A.10.8.3 Medios físicos en tránsito
	A.10.8.4 Mensajería Electrónica
	A.10.8.5 Sistema de información empresarial
	10.9. Servicios de Comercio Electrónico
	A.10.9.1 Comercio Electrónico
	A.10.9.2 Transacciones On-line
	A.10.9.3 Información disponible públicamente
	10.10. Monitoreo
	A.10.10.1 Registros de Auditoría
	A.10.10.2 Uso de Sistemas de Monitoreo
	A.10.10.3 Protección de los Logs
	A.10.10.4 Log de actividades de Administradores y Operadores
	A.10.10.5 Registro de Fallas
	A.10.10.6 Sincronización de relojes
A.11 CONTROL DE ACCESO	11.1 Requerimientos del Negocio para Control de Acceso
	A.11.1.1 Política de Control de Acceso
	11.2 Administración de Accesos de Usuarios

Tabla 21. (Continuación).

	A.11.2.1 Registro de Usuarios
	A.11.2.2 Gestión de Privilegios
	A.11.2.3 Administración de Contraseñas de Usuarios
	A.11.2.4 Revisión de Roles de Usuarios
	11.3 Responsabilidades de Usuarios
	A.11.3.1 Uso de Password
	A.11.3.2 Equipos desatendidos de Usuarios
	A.11.3.3 Política de Escritorio Limpio y Pantalla Limpia
	11.4 Control de Acceso a la Red
	A.11.4.1 Políticas sobre Servicios de Red
	A.11.4.2 Autenticaciones de Usuarios para conexiones externas
	A.11.4.3 Identificación de equipamientos en la red
	A.11.4.4 Diagnóstico Remoto y configuración de protección de puertos
	A.11.4.5 Segregación en la Red
	A.11.4.6 Control de Conexiones de Red
	A.11.4.7 Control de Ruteo de Red
	11.5 Control de Acceso a las Aplicaciones y a la Información
	A.11.5.1 Restricción de Acceso a la Información
	A.11.5.2 Aislamiento de Sistemas Sensibles
A.12 DESARROLLO, ADQUISICION Y MANTENIMIENTO DE SISTEMAS DE INFORMACION	12.1 Requerimientos de Seguridad de los Sistemas de Información
	A.12.1.1 Análisis y Especificaciones de Requerimientos de Seguridad
	12.2 Procesamiento Correcto en Aplicaciones
	A.12.2.1 Validación de Datos de Entrada
	A.12.2.2 Control de Procesamiento Interno
	A.12.2.3 Integridad de Mensajería
	A.12.2.4 Validación de Datos de Salida
	12.3 Controles Criptográficos
	A.12.3.1 Políticas de Uso de Controles Criptográficos
	A.12.3.2 Manejo de Claves
	11.4 Seguridad de los Archivos de Sistemas
	A.12.4.1 Control de Software Operativo
	A.12.4.2 Protección de Datos de Prueba de Sistemas
	A.12.4.3 Control de Acceso a Código Fuente

Tabla 21. (Continuación).

	12.5 Seguridad en el Desarrollo y Servicios de Soporte
	A.12.5.1 Procedimientos de Control de Cambios
	A.12.5.2 Revisión Técnica de Aplicaciones luego de Cambios en el Sistema Operativo
	A.12.5.3 Restricciones en Cambios de Paquetes de Software
	A.12.5.4 Fuga de Información
	A.12.5.5 Desarrollo de Software Tercerizado
	11.6 Gestión de Vulnerabilidades Técnicas
	A.12.6.1 Control de Vulnerabilidades Técnicas
A.13 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	A.13.1 Reportando Eventos de Seguridad y Vulnerabilidades
	A.13.1.1 Reportando Eventos de Seguridad de la Información
	A.13.1.2 Reportando Vulnerabilidades de la Seguridad
	A.13.2 Gestión de Incidentes de Seguridad de la Información y Proceso de Mejoras
	A.13.2.1 Responsabilidades y Procedimientos
	A.13.2.2 Aprendiendo de los Incidentes de Seguridad de la Información
	A.13.2.3 Recolección de Evidencia
A.14 GESTION DE LA CONTINUIDAD DEL NEGOCIO	14.1 Aspectos de Seguridad en la Gestión de la Continuidad del Negocio
	A.14.1.1 Incluyendo Seguridad en el Proceso de Gestión de Continuidad del Negocio
	A.14.1.2 Continuidad del Negocio y Evaluación de Riesgos
	A.14.1.3 Desarrollo e Implementación de Planes de Continuidad incluyendo Seguridad de la Información
	A.14.1.4 Business continuity planning framework
	A.14.1.5Prueba, Mantenimiento y Reevaluando Planes de Continuidad del Negocio
A.15 CUMPLIMIENTO	15.1 Cumplimiento con Requerimientos Legales
	A.15.1.1 Identificación de Legislación Aplicable
	A.15.1.2 Derechos de Propiedad Intelectual
	A.15.1.3 Protección de los Registros
	A.15.1.4 Protección de los Datos y privacidad de los datos personales

Tabla 21. (Continuación).

	A.15.1.5 Prevención del mal uso de las instalaciones de procesamiento
	A.15.1.6 Regulación de Controles Criptográficos
	15.2 Cumplimiento con Requerimientos Legales
	A.15.2.1 Cumplimiento con las políticas, estándares y regulaciones técnicas
	A.15.2.2 Chequeo de Cumplimiento Técnico
	15.3 Consideraciones de Auditoría de Sistemas
	A.15.3.1 Controles de Auditoría de los Sistemas de Información
	A.15.3.2 Protección de la información contra las herramientas de auditoría

Fuente: El Autor

11.8 Anexo H: Lista de Chequeo por Dominio

Para establecer el estado actual de los dominios en la empresa se realizó levantamiento de la información mediante una lista de chequeo, con la siguiente estructura:

Tabla 22. Estructura formato Lista de chequeo

Control	Aspecto a verificar	Aprobada	Publicada	Nivel cumplimiento						Observaciones
				0	1	2	3	4	5	

Fuente: El Autor

Para la evaluación de cada dominio, se estableció el siguiente rango de calificación:

Tabla 23. Rangos de cumplimiento en %

1 a 25	No Cumplido
26 a 75	Implementando
76 a 100	Cumplido

Fuente: El Autor

11.9 Anexo I: Evaluación de Dominios ISO 27001

Tabla 24. Evaluación de Dominios ISO 27001

Referencia		Área de Auditoría, objetivo y pregunta		Estado (%)
Checklist	**Estándar**	**Sección**	**Pregunta de Auditoría**	
Política de Seguridad				
1.1	**5.1**	**Políticas de Seguridad de Información**		
1.1.1	5.1.1	Políticas para la seguridad de la información	¿La organización ha definido un conjunto de políticas para la seguridad de la información?	90
			¿Este conjunto de políticas están aprobadas por la dirección?	100
			¿Este conjunto de políticas se ha divulgado y notificado a los funcionarios y partes interesadas?	100
1.1.2	5.1.2	Revisión de las políticas para la seguridad de la información	¿La entidad ha establecido intervalos planificados para la revisión de las políticas relacionadas con la seguridad de la información?	80
Organización de la Seguridad de Información				
2.1	**6.1**	**Organización Interna**		
2.11	6.11	Gestión de Compromiso con la Seguridad de Información	Si la alta gerencia presta soporte activo a las medidas de seguridad en la entidad. Esto puede ser realizado por direcciones claras, compromiso demostrado, asignaciones explícitas y conocimiento de los temas relacionados con la seguridad informática.	100
2.1.2	6.1.2	Separación de deberes	¿Se tiene separados los deberes a nivel de la operación del proceso de gestión tecnológica y del SGSI?	100

Tabla 24. (Continuación).

2.1.3	6.1.3	Asignación de Responsabilidades de Seguridad de Información	¿Se han identificado las autoridades relacionadas con el cumplimiento de la ley? ¿Las autoridades de supervisión y organismos de regulación?	100
			¿Se tiene identificado como reportar los incidentes de seguridad de la información asociados a violación de la ley?	95
2.1.4	6.1.4	Contacto con grupos de interés especial	¿Hay relación directa con grupos de interés especial? ¿Asociaciones de profesionales especialistas en todo lo relacionado con la seguridad de la información?	70
2.1.5	6.1.5	Seguridad de la Información en la gestión de proyectos	¿En la gestión de proyectos se trata la seguridad de la información independiente del tipo de proyecto?	75
2.2	**6.2**	**Partes Externas**		
2.2.1	6.2.1	Política para dispositivos móviles	¿Se adoptó una política para dispositivos móviles?	60
			¿La entidad cuenta con medidas de seguridad para gestionar los riesgos que se puedan presentar por el uso de dispositivos móviles?	40
2.2.2	6.2.2	Teletrabajo	¿Se ha implementado una política de teletrabajo en la organización?	100
			¿Se tienen medidas que soportan la seguridad de la información, a la que se tiene acceso para desempeñar labores de teletrabajo?	90
Administración de Activos				
3.1	**7.1**	**Responsabilidad por Activos**		
3.1.1	7.1.1	Inventario de Activos	¿Los activos informáticos más importantes son debidamente identificados y se lleva inventario o se mantiene un registro ordenado?	100
3.1.2	7.1.2	Propiedad de Activos	¿Los activos de la entidad tienen un dueño asignado?	90

Tabla 24. (Continuación).

3.1.3	7.1.3	Uso aceptable de Activos	¿Se tiene una clasificación adecuada de la información, de tal forma que se garantice su confidencialidad, integridad y disponibilidad de la misma en la organización?	95
3.2	**7.2**	**Clasificación de la Información**		
3.2.1	7.2.1	Directrices de Clasificación	¿Se tienen medidas de seguridad adecuadas que proporcionen una protección adecuada en cada activo de la organización?	80
3.2.2	7.2.2	Etiquetado y manejo de información	¿La entidad cuenta con una CMD que proporcione una visión global de la configuración de sus Cis y la relación entre cada uno de ellos?	100
			¿Los activos de la organización tienen definidos claramente los responsables según el nivel de circunstancias?	100
Seguridad física y ambiental				
5,1	**9,1**	**Áreas Seguras**		
5.1.1	9.1.1	Perímetro de Seguridad Física	¿Existen mecanismos de control de acceso implementados con respecto al acceso a los sitios de procesamiento de información? Algunos ejemplos son controles biométricos, tarjetas de acceso, separación por muros, control de visitantes, etc.	90
5.1.2	9.1.2	Controles Físicos de Entrada	¿La entidad cuenta con controles de acceso que restringen la entrada y solo puede ingresar personal autorizado a las diferentes áreas de la empresa?	95
5.1.3	9.1.3	Aseguramiento de Oficinas, Salas de Servidores e Instalaciones	¿Las instalaciones donde se alojan los servidores y demás equipos de procesamiento (routers, switches, etc.), están aseguradas bajo llave que garantice su seguridad?	100

Tabla 24. (Continuación).

5.1.4	9.1.4	Protección contra Amenazas Exteriores y Ambientales/Climáticas	¿Se tienen implementadas protecciones o resguardos contra manifestaciones, fuego, inundaciones, temblores, explosiones y otras formas provocadas por el hombre o desastres naturales?	100
			¿Existe alguna amenaza potencial en los locales vecinos del lugar donde se encuentran las instalaciones?	100
5.1.5	9.1.5	Trabajando en Áreas Seguras	¿La entidad cuenta con procedimientos determinados e implementados sobre cómo trabajar en las áreas seguras?	100
5.1.6	9.1.6	Zonas de Acceso Público, Entrega y Descarga	¿Con relación a las zonas de acceso público, donde cualquier persona puede acceder sin restricción, estas están aisladas de las demás zonas de procesamiento de información o que contengan equipos delicados que requieran algún nivel de seguridad para su protección?	100
5,2	**9,2**	**Equipamiento de Seguridad**		
5.2.1	9.2.1	Equipamiento y Protección del Sitio	¿Se protegen los equipos con el fin de reducir el riesgo de acceso no autorizado o daños ambientales?	90
5.2.2	9.2.2	Utilidades Soportadas	¿Se mantienen protegidos los equipos contra fallas eléctricas y otras fallas que pudieran tener redundancia?	100
			¿Qué mecanismos de protección eléctrica son utilizados? ¿Alimentación múltiple, UPS, generador de backup, etc.?	100
5.2.3	9.2.3	Cableado de Seguridad	El cableado de comunicaciones y suministro eléctrico está debidamente protegido contra daños y/o intercepción?	100
			¿Existen controles adicionales de seguridad con respecto al transporte de información crítica? Por ej. Encriptado en las comunicaciones.	100
5.2.4	9.2.4	Mantenimiento de Equipos	¿Se realiza mantenimiento preventivo periódicamente a los equipos de modo que se asegure la disponibilidad e integridad?	80

Tabla 24. (Continuación).

			¿En la realización de mantenimientos, se respetan los intervalos de tiempos y recomendaciones de los fabricantes?	100
			¿El personal encargado de realizar los mantenimientos está capacitado y autorizado?	100
Seguridad física y ambiental				
5.2.4	9.2.4	Mantenimiento de Equipos	¿Los logs de alertas de los equipos, se revisan continuamente con el fin de detectar y corregir posibles fallas, especialmente en los discos?	100
			¿Cuándo los equipos son enviados fuera de la entidad, se aplican los controles adecuados?	100
			¿La entidad cuenta con pólizas de seguros que cubren la totalidad de los equipos, y los requerimientos de la Compañía de Seguros se encuentran diligenciados apropiadamente?	100
5.2.5	9.2.5	Aseguramiento de Equipos fuera de las Oficinas	¿Existen mecanismos de seguridad para controlar y mitigar los riesgos a los que están expuestos los equipos que se encuentran fuera de la entidad?	70
			¿Los equipos utilizados fuera de la entidad cuentan con autorización de los directivos?	100
5.2.6	9.2.6	Disposiciones de Seguridad de Reutilización de Equipos	¿Los procesos de reutilización o baja de equipos, cuentan con procedimientos de verificación de almacenamiento con respecto a datos y software licenciado, y el borrado total antes de su entrega?	100
5.2.7	9.2.7	Autorizaciones de Sacar Equipos	¿La entidad ha implementado controles con respecto a que ningún equipo, información y software sea retirado de las instalaciones sin la debida autorización?	100

Tabla 24. (Continuación).

Gestión de Comunicaciones y Operaciones				
6.1	**10,1**	**Procedimientos y Responsabilidades Operativas**		
6.1.1	10.1.1	Documentación de Procedimientos Operativos	¿Se documentan los procedimientos operativos y se encuentran actualizados y disponibles para todos los usuarios que puedan necesitarlos?	80
			¿Estos procedimientos son registrados en documentos formales y cualquier cambio necesita la autorización de los directivos?	75
6.1.2	10.1.2	Manejo de Cambios	¿Los cambios en los equipos de procesamiento de información son debidamente controlados?	100
6.1.3	10.1.3	Segregación de Tareas	¿Las tareas y responsabilidades están debidamente separadas de modo que se reduzcan las oportunidades de alteración de información o mal uso de los sistemas de información?	100
6.1.4	10.1.4	Separación de desarrollo, test e instalaciones operativas	¿Hay una separación ente los equipos de desarrollo y pruebas y los equipos operacionales? Por ejemplo, el equipo de producción debe estar separado del equipo de desarrollo. Es importante que en lo posible estén en segmentos de red distintos unos del otro.	100
6.2	**10,2**	**Manejo de Entrega de Servicios Tercerizados**		
6.2.1	10.2.1	Entrega de Servicios	¿Existen medidas que son tomadas para asegurar que los controles de seguridad, niveles de servicio y entrega sean incluidos y verificados en los contratos de servicios con terceros, así como su revisión periódica de cumplimiento?	95
6.2.2	10.2.2	Monitoreo y revisión de servicios tercerizados	¿Se monitorean y revisan regularmente los servicios, reportes y registros proveídos por terceros?	70
			¿Se evidencian los controles de auditoría realizados a intervalos regulares sobre reportes, servicios y registros suministrados por terceros?	50

Tabla 24. (Continuación).

6.2.3	10.2.3	Manejo de Cambios de servicios tercerizados	¿Se gestionan los cambios en el suministro de servicios, la mejora en las políticas de seguridad de información, mantenimiento, procedimientos y controles?	80
			¿Se tienen en cuenta sistemas de negocio críticos, procesos involucrados y re-evaluación de riesgos?	100
6.3	**10.3**	**Planeamiento y Aceptación de Sistemas**		
6.3.1	10.3.1	Gestión de la Capacidad	¿Las capacidades de procesamiento de los sistemas son monitoreadas con base a la demanda y proyectadas con base a futuros requerimientos, de tal forma que se pueda asegurar que la capacidad de almacenamiento y proceso estén disponibles?	100
			Por Ejemplo el monitoreo de espacio en disco, Memoria RAM, CPU en los servidores críticos.	
6.3.2	10.3.2	Aceptación de Sistemas	¿Existen criterios establecidos para la aceptación de nuevos sistemas de información, actualizaciones y cambios de mejoras con nuevas versiones? ¿Se realizan pruebas antes de la aceptación de los mismos?	100
6.4	**10.4**	**Protección contra código malicioso y móvil**		
6.4.1	10.4.1	Controles contra código malicioso	¿Se desarrollan e implementan procedimientos de alerta a los usuarios, sobre detección, prevención y recuperado de información, relacionado con ataques de código malicioso	80
6.4.2	10.4.2	Controles contra código móvil	¿El código móvil solo debe ser utilizado después de ser autorizado y únicamente en caso de ser necesario?	75

Tabla 24. (Continuación).

			¿Las configuraciones del código móvil autorizado se realzan y operan de acuerdo a las Políticas de Seguridad? ¿Se previene la ejecución del código móvil no autorizado?	
			(El Código Móvil se transfiere de una computadora a otra y se ejecuta automáticamente. Realiza funciones específicas sin intervención del usuario y está asociado a un gran número de servicios de middleware)	
6.5	**10.5**	**Copias de Respaldo**		
6.5.1	10.5.1	Respaldo de la Información	¿Se realizan periódicamente copias de respaldo de la información y software de acuerdo con las políticas de backup?	100
			¿En caso de que ocurriera un desastre o fallo de medios, se puede recuperar toda la información y el software esencial?	100
6.6	**10.6**	**Administración de la Seguridad de la Red**		
6.6.1	10.6.1	Controles de Red	¿La red es adecuadamente administrada y controlada para protegerse de tretas y en orden a mantener la seguridad de los sistemas y aplicaciones en uso a través de la red, incluyendo la información en tránsito?	100
			¿Existen controles implementados para asegurar el tránsito de la información en la red y evitar que esta sea leída o accesada de forma no autorizada?	100

Tabla 24. (Continuación).

6.6.2	10.6.2	Seguridad en los Servicios de Red	¿Se identifican e incluyen en todos los acuerdos de servicios de red, las características de seguridad informática, niveles de servicio y requerimientos de administración?	100
			¿La capacidad del proveedor de servicios de red de proporcionar los servicios de forma segura, es determinada y regularmente monitoreada y se tienen derechos de auditoría acordada para medir niveles de servicio?	100
6.7	**10.7**	**Manejo de Medios**		
6.7.1	10.7.1	Manejo de medios removibles	¿Existen procedimientos para el manejo de medios removibles como cintas, diskettes, tarjetas de memoria, lectores de CD, pendrives, etc.?	100
			¿Se encuentran documentados y definidos claramente los procedimientos y niveles de autorización?	100
6.7.2	10.7.2	Disposición de los medios	¿Existen procedimientos formalmente establecidos para la eliminación de forma segura de aquellos medios que ya no sean requeridos?	100
6.7.3	10.7.3	Procedimientos de manejo de la información	¿El manejo de almacenamiento de la información está soportado mediante procedimientos?	90
			Estos procedimientos incluyen temas como: ¿el mal uso de la información y la protección contra el acceso no autorizado?	80
6.7.4	10.7.4	Seguridad en la Documentación de los Sistemas	¿Se encuentra protegida contra acceso no autorizado la documentación de los sistemas?	100
6.8	**10.8**	**Intercambio de Información**		
6.8.1	10.8.1	Políticas y Procedimientos de intercambio de información	¿La protección de la información está asegurada mediante políticas formales, procedimientos y/o controles?	100

Tabla 24. (Continuación).

			¿Estos procedimientos y/o controles abarcan el uso de equipos de comunicación en el intercambio de información?	100
6.8.2	10.8.2	Acuerdos de Intercambio	¿Entre la entidad y partes externas hay acuerdos de intercambios de información y software?	75
			¿En los acuerdos relacionados con la seguridad de la información, se evidencia la sensibilidad y criticidad de la información?	70
6.8.3	10.8.3	Medios físicos en transito	Los medios físicos que contengan información es protegida contra acceso no autorizado, mal uso o corrupción de datos durante el transporte entre las organizaciones	100
6.8.4	10.8.4	Mensajería Electrónica	¿Se protege debidamente la información que se envía por mensajería electrónica?	100
			(Entiéndase como Mensajería Electrónica email, intercambio electrónico de datos, mensajería instantánea, entre otros.)	
6.8.5	10.8.5	Sistema de información empresarial	¿Hay tendencia a fortalecer la protección de información asociada con la interconexión de sistemas de negocio, mediante el desarrollo de políticas y procedimientos?	90
6.9	**10.9**	**Servicios de Comercio Electrónico**		
6.9.1	10.9.1	Comercio Electrónico	¿La información envuelta en el comercio electrónico cruza a través de redes públicas y está protegida contra actividades fraudulentas, posibles disputas contractuales o cualquier acceso no autorizado que permita lectura o manipulación de esos datos?	100
			¿La aplicación de controles criptográficos es tenida en cuenta en los controles de seguridad?	100

Tabla 24. (Continuación).

			¿Se incluyen acuerdos entre socios comerciales sobre el comercio electrónico, que comprometa a ambas partes en la negociación de los términos convenidos, incluidos los detalles de los temas relacionados con la seguridad de la información?	90
6.9.2	10.9.2	Transacciones On-line	¿La información relacionada con transacciones en línea se encuentra protegida contra transmisiones incompletas, mal ruteo, alteración de mensajería, divulgación no autorizada, duplicación no autorizada o replicación?	100
6.9.3	10.9.3	Información disponible públicamente	¿La información disponible públicamente se encuentra protegida de tal forma que se garantice su integridad contra modificación no autorizada?	100
6.1	**10.1**	**Monitoreo**		
6.10.1	10.10.1	Registros de Auditoría	¿Se conservan los Backups históricos de los registros de auditoría con las actividades de los usuarios, excepciones, eventos de seguridad de información, de tal forma que se pueda realizar investigaciones futuras y monitoreo de acceso?	100
			¿Se tienen en consideración medidas de protección a la privacidad en el mantenimiento de registros de auditoría?	100
6.10.2	10.10.2	Uso de Sistemas de Monitoreo	¿Los equipos de procesamiento de datos cuentan con procedimientos de monitoreo?	100
			¿Se revisa regularmente de forma periódica el resultado de la actividad de monitoreo?	100
			¿Los niveles de monitoreo requeridos por los equipos de procesamiento de información son determinados por un análisis de riesgos?	100
6.10.3	10.10.3	Protección de los Logs	¿Se encuentran bien protegidos los equipos que contienen los registros y logs de auditoría, contra el acceso no autorizado y posibles manipulaciones?	100

Tabla 24. (Continuación).

6.10.4	10.10.4	Log de actividades de Administradores y Operadores	¿En los logs quedan registradas las actividades de los Administradores y Operadores de sistemas?	100
			¿Los logs son revisados regularmente?	100
6.10.5	10.10.5	Registro de Fallas	¿Las fallas son registradas en logs, y luego analizadas y acciones apropiadas realizadas en consecuencia?	100
			¿Los niveles de registros en logs requeridos para cada sistema individual son determinados con base a análisis de riesgos y la degradación de performance es tenida en cuenta?	90
6.10.6	10.10.6	Sincronización de relojes	¿Todos los sistemas de información tienen sincronizados los relojes con base a una misma fuente de tiempo exacta acordada?	80
Access Control				
7.1	**11.1**	**Requerimientos del Negocio para Control de Acceso**		
7.1.1	11.1.1	Política de Control de Acceso	¿La entidad se basa en los requerimientos de seguridad de la empresa para la elaboración de las políticas de control de acceso?	100
			¿Las políticas de control de acceso tienen en cuenta los controles de acceso lógicos y físicos?	100
			¿Usuarios y proveedores de servicios conocen claramente los requisitos de la empresa relacionados con el control de acceso?	70
7.2	**11.2**	**Administración de Accesos de Usuarios**		
7.2.1	11.2.1	Registración de Usuarios	¿Existen procedimientos formales para activar y desactivar usuarios con acceso a los sistemas?	90

Tabla 24. (Continuación).

7.2.2	11.2.2	Gestión de Privilegios	¿Se restringe y controlan los privilegios en los sistemas de información, con base en las necesidades de uso y se cuenta con un esquema formal de autorización?	100
7.2.3	11.2.3	Administración de Contraseñas de Usuarios	¿Existe un proceso de gestión formal para la asignación y reasignación de contraseñas?	100
			¿Hay procesos de solicitud a los usuarios para que firmen acuerdos de confidencialidad relacionados con el password?	40
7.2.4	11.2.4	Revisión de Roles de Usuarios	Los privilegios y derechos de acceso son revisados con regularidad, como por ejemplo cada mes, cada dos meses, etc., dependiendo de la importancia de cada privilegio?	100
7.3	**11.3**	**Responsabilidades de Usuarios**		
7.3.1	11.3.1	Uso de Password	¿Existen prácticas de seguridad en la entidad para que los usuarios puedan crear y realizar mantenimiento de contraseñas seguras?	70
7.3.2	11.3.2	Equipos desatendidos de Usuarios	¿Los procedimientos y requisitos de seguridad para proteger los equipos desatendidos, son de conocimiento de los usuarios y terceros? Por ejemplo: Configurar terminación automática de sesiones por tiempo de inactividad o salir del sistema cuando las sesiones son terminadas.	90
7.3.3	11.3.3	Política de Escritorio Limpio y Pantalla Limpia	¿La entidad ha implementado políticas de escritorio limpio, relacionadas con papeles y dispositivos de almacenamiento removibles?	75
			¿La entidad ha implementado políticas de pantalla limpia en los equipos de procesamiento de información?	80
7.4	**11.4**	**Control de Acceso a la Red**		

Tabla 24. (Continuación).

7.4.1	11.4.1	Políticas sobre Servicios de Red	¿Los usuarios acceden únicamente a los servicios de red que han sido específicamente autorizados?	100
			¿La entidad cuenta con políticas de seguridad relacionadas con la red y los servicios de red?	100
7.4.2	11.4.2	Autenticaciones de Usuarios para conexiones externas	¿El acceso remoto de los usuarios es controlado con mecanismos apropiados para tal fin?	100
7.4.3	11.4.3	Identificación de equipamientos en la red	¿Se cuenta con equipos de identificación automática, que permiten la autenticación a las conexiones desde equipos y direcciones específicas?	100
7.4.4	11.4.4	Diagnóstico Remoto y configuración de protección de puertos	¿Los accesos lógicos y físicos a puertos de diagnóstico están debidamente controlados y protegidos por mecanismos de seguridad?	100
7.4.5	11.4.5	Segregación en la Red	¿Los grupos de usuarios, sistemas y servicios de información, son segregados en la red?	100
			¿La red está segregada con mecanismos de seguridad perimetral como firewalls, para controlar el acceso a los usuarios externos?	100
			¿En la segregación de la red se tienen en cuenta consideraciones para separar las redes Wireless en internas y privadas?	100
7.4.6	11.4.6	Control de Conexiones de Red	¿Transmilenio cuenta con políticas de control de acceso para la verificación de conexiones provenientes de redes compartidas, especialmente aquellas que tienen alcances más allá de los límites de la empresa?	100

Tabla 24. (Continuación).

7.4.7	11.4.7	Control de Ruteo de Red	¿Las políticas de control de acceso establecen controles para los ruteos implementados en la red?	100
			¿Los controles de ruteo, establecen mecanismos de identificación positiva de origen y destino?	100
7.6	**11.6**	**Control de Acceso a las Aplicaciones y a la Información**		
7.6.1	11.6.1	Restricción de Acceso a la Información	¿El acceso a la información y los sistemas de aplicaciones está restringido en concordancia con las políticas de control de acceso definidas?	100
7.6.2	11.6.2	Aislamiento de Sistemas Sensibles	¿Los sistemas que se consideran sensibles en la entidad, están en ambientes aislados, en equipos dedicados con aplicaciones seguras y confiables?	100
Desarrollo. Adquisición y Mantenimiento de Sistemas de Información				
8.1	**12.1**	**Requerimientos de Seguridad de los Sistemas de Información**		
8.1.1	12.1.1	Análisis y Especificaciones de Requerimientos de Seguridad	¿Los requerimientos de seguridad para la implementación de sistemas de información y el fortalecimiento de los existentes, especifican los requerimientos para los controles de seguridad?	90
			¿Los requerimientos y controles identificados reflejan el valor económico de los activos de información envueltos y las consecuencias de un fallo de seguridad?	100
8.2	**12.2**	**Procesamiento Correcto en Aplicaciones**		
8.2.1	12.2.1	Validación de Datos de Entrada	¿Los datos introducidos a los sistemas, se validan para asegurar que son correctos y apropiados?	100

Tabla 24. (Continuación).

			¿Se tienen controles para diferentes errores como mensajes en datos mal ingresados, procedimientos para responder a los errores de validación, definición de responsabilidades para todo el personal envuelto en la carga de datos?	100
8.2.2	12.2.2	Control de Procesamiento Interno	¿Las aplicaciones cuentan con validaciones en los datos de entrada para evitar que puedan ser ingresados datos no válidos por error o deliberadamente?	100
			¿En el diseño e implementación de aplicaciones se tiene en cuenta la minimización del riesgo relacionado con la pérdida de integridad de datos?	90
8.2.3	12.2.3	Integridad de Mensajería	¿Se identifican e implementan los controles necesarios en los requerimientos para el aseguramiento y la protección de la integridad de los mensajes en las aplicaciones?	100
			¿Se realizan evaluaciones de riesgos de seguridad para determinar la integridad de los mensajes, y para determinar el método más apropiado de su aplicación?	80
8.2.4	12.2.4	Validación de Datos de Salida	¿Los sistemas de aplicaciones de salida de datos, son validados para asegurar que el procesamiento de información almacenada sea correcto y apropiado a las circunstancias?	100
8.3	**12.3**	**Controles Criptográficos**		
8.3.1	12.3.1	Políticas de Uso de Controles Criptográficos	¿Transmilenio cuenta con políticas de uso de controles criptográficos para protección de la información?	100

Tabla 24. (Continuación).

			¿La política criptográfica considera el enfoque de gestión hacia el uso de controles criptográficos, los resultados de la evaluación de riesgo para identificar nivel requerido de protección, gestión de claves y métodos de diversas normas para la aplicación efectiva?	95
8.3.2	12.3.2	Manejo de Claves	¿La administración de claves se utiliza efectivamente para apoyar el uso de técnicas criptográficas en la organización?	100
			¿Las claves criptográficas están protegidas correctamente contra modificación, pérdida y/o destrucción?	100
			¿Las claves públicas y privadas están protegidas contra divulgación no autorizada?	100
			¿Los equipos utilizados para generar o almacenar claves, están físicamente protegidos?	100
			¿Los sistemas de administración de claves, están basados en procedimientos estandarizados y seguros?	90
8.4	**12.4**	**Seguridad de los Archivos de Sistemas**		
8.4.1	12.4.1	Control de Software Operativo	Existen procedimientos para controlar la instalación de software en los sistemas operativos (Esto es para minimizar el riesgo de corrupción de los sistemas operativos)	100
8.4.2	12.4.2	Protección de Datos de Prueba de Sistemas	¿Los sistemas de testeo de datos, están debidamente protegidos y controlados?	90
			¿La utilización de información personal o cualquier información sensitiva para propósitos de testeo, está prohibida?	
8.4.3	12.4.3	Control de Acceso a Código Fuente	¿Existen controles estrictos de modo a restringir el acceso al código fuente? (esto es para prevenir posibles cambios no autorizados)	70

Tabla 24. (Continuación).

8.5	12.5	Seguridad en el Desarrollo y Servicios de Soporte		
8.5.1	12.5.1	Procedimientos de Control de Cambios	¿Existen procedimientos de control estricto con respecto a cambios en los sistemas de información? (Esto es para minimizar la posible corrupción de los sistemas de información)	100
			¿Estos procedimientos abordan la necesidad de evaluación de riesgos, análisis de los impactos de los cambios?	100
8.5.2	12.5.2	Revisión Técnica de Aplicaciones luego de Cambios en el Sistema Operativo	¿Existen procesos a seguir o procedimientos para revisión y testeo de las aplicaciones críticas de negocio y seguridad, luego de cambios en el Sistema Operativo? Periódicamente, esto es necesario cada vez que haya que hacer un parcheo o upgrade del sistema operativo.	80
8.5.3	12.5.3	Restricciones en Cambios de Paquetes de Software	¿Las modificaciones a los paquetes de software, son desalentadas o limitadas estrictamente a los cambios mínimos necesarios?	100
			¿Todos los cambios son estrictamente controlados?	100
8.5.4	12.5.4	Fuga de Información	¿Existen controles para prevenir la fuga de información?	85
			¿Controles tales como escaneo de dispositivos de salida, monitoreo regular del personal y actividades permitidas en los sistemas bajo regulaciones locales, monitoreo de recursos, son considerados?	100
8.5.5	12.5.5	Desarrollo de Software Tercerizado	¿El desarrollo de software tercerizado, es supervisado y monitoreado por la organización?	90
			Puntos como: ¿Adquisición de licencias, acuerdos de garantía, requerimientos contractuales de calidad asegurada, testeo antes de su instalación definitiva, revisión de código para prevenir troyanos, son considerados?	100

Tabla 24. (Continuación).

8.6	**12.6**	**Gestión de Vulnerabilidades Técnicas**		
8.6.1	12.6.1	Control de Vulnerabilidades Técnicas	¿Se obtiene información oportuna en tiempo y forma sobre las vulnerabilidades técnicas de los sistemas de información que se utilizan?	100
			¿La organización evalúa e implementa medidas apropiadas de mitigación de riesgos a las vulnerabilidades a las que está expuesta?	90
Gestión de Incidentes de Seguridad de Información				
9.1	**13.1**	**Reportando Eventos de Seguridad y Vulnerabilidades**		
9.1.1	13.1.1	Reportando Eventos de Seguridad de la Información	¿Son desarrollados e implementados procedimientos formales de reporte, respuesta y escalación en incidentes de seguridad?	85
			¿Los eventos de seguridad de información, son reportados a través de los canales correspondientes lo más rápido posible?	100
9.1.2	13.1.2	Reportando Vulnerabilidades de la Seguridad	¿Existen procedimientos que aseguren que todos los empleados deben reportar cualquier vulnerabilidad en la seguridad en los servicios o sistemas de información?	100
9.2	**13.2**	**Gestión de Incidentes de Seguridad de la Información y Proceso de Mejoras**		
9.2.1	13.2.1	Responsabilidades y Procedimientos	¿Es utilizado el monitoreo de sistemas, alertas y vulnerabilidades para detectar incidentes de seguridad?	100
			¿Los objetivos de la gestión de incidentes de seguridad de información, están acordados con las gerencias?	95
			¿Están claramente establecidos los procedimientos y responsabilidades de gestión para asegurar una rápida, efectiva y ordenada respuesta a los incidentes de seguridad de información?	85

Tabla 24. (Continuación).

9.2.2	13.2.2	Aprendiendo de los Incidentes de Seguridad de la Información	¿La información obtenida de la evaluación de incidentes de seguridad que ocurrieron en el pasado, es utilizada para determinar el impacto recurrente de incidencia y corregir errores?	100
			¿Existen mecanismos establecidos para identificar y cuantificar el tipo, volumen y costo de los incidentes de seguridad?	100
9.2.3	13.2.3	Recolección de Evidencia	Si las medidas de seguimiento contra una persona u organización después de un incidente de seguridad de la información implican una acción legal (ya sea civil o penal)	100
			¿Las evidencias relacionadas con incidentes, son recolectadas, retenidas y presentadas conforme las disposiciones legales vigentes en las jurisdicciones pertinentes?	100
			¿Los procedimientos internos son desarrollados y seguidos al pie de la letra cuando se debe recolectar y presentar evidencia para propósitos disciplinarios dentro de la organización?	95
Gestión de la Continuidad del Negocio				
10.1	**14.1**	**Aspectos de Seguridad en la Gestión de la Continuidad del Negocio**		
10.1.1	14.1.1	Incluyendo Seguridad en el Proceso de Gestión de Continuidad del Negocio	¿Se tiene definidos y divulgados los procedimientos para seguir la operación de la organización "procedimiento de recuperación" en un centro de datos alterno?	100
			¿Estos procesos, entienden cuáles son los riesgos que la organización enfrenta, identifican los activos críticos, los impactos de los incidentes, consideran la implementación de controles preventivos adicionales y la documentación de los Planes de Continuidad del Negocio direccionando los requerimientos de seguridad?	100

Tabla 24. (Continuación).

10.1.2	14.1.2	Continuidad del Negocio y Evaluación de Riesgos	¿La empresa tiene definidos los procedimientos a seguir en caso de entrar en un plan de contingencia?	95
10.1.3	14.1.3	Desarrollo e Implementación de Planes de Continuidad incluyendo Seguridad de la Información	¿El personal de la entidad tiene claros sus funciones y tareas en caso de que ocurra un evento que obligue a entrar en contingencia?	100
10.1.4	14.1.4	Business continuity planning framework	¿La entidad realiza periódicamente planes de contingencia controlados en conjunto con todas las áreas de la organización?	100
10.1.5	14.1.5	Prueba, Mantenimiento y Reevaluando Planes de Continuidad del Negocio	¿La organización realiza la réplica de sus datos y configuraciones de forma periódica en el centro de datos alterno?	80
			¿La entidad realiza los cambios necesarios en el centro de datos alterno, cada vez que realice cambios en el centro de datos principal?	100
Cumplimiento				
11.1	**15.1**	**Cumplimiento con Requerimientos Legales**		
11.1.1	15.1.1	Identificación de Legislación Aplicable	¿Todas las leyes relevantes, regulaciones, requerimientos contractuales y organizacionales son tenidas en cuenta de modo a que estén documentados para cada sistema de información en la organización?	100
			¿Los controles específicos y responsabilidades individuales de modo a cumplir con estos requerimientos, son debidamente definidos y documentados?	80
11.1.2	15.1.2	Derechos de Propiedad Intelectual	¿Existen procedimientos para asegurar el cumplimiento de los requerimientos legales, regulatorios y contractuales sobre el uso de materiales y software que estén protegidos por derechos de propiedad intelectual?	75

Tabla 24. (Continuación).

			¿Estos procedimientos, están bien implementados?	80
			Controles tales como: Política de Cumplimiento de Derechos de Propiedad Intelectual, Procedimientos de Adquisición de Software, Política de concientización, Mantenimiento de Prueba de la Propiedad, Cumplimiento con Términos y Condiciones, ¿son consideradas?	100
11.1	**15.1**	**Cumplimiento con Requerimientos Legales**		
11.1.3	15.1.3	Protección de los Registros de la Organización	¿Los registros importantes de la organización están protegidos contra pérdida, destrucción y falsificación en concordancia con los requerimientos legales, regulatorios, contractuales y de negocio?	100
			¿Están previstas las consideraciones con respecto al posible deterioro de medios de almacenamiento utilizados para almacenar registros?	100
			¿Los sistemas de almacenamiento son elegidos de modo a que los datos requeridos puedan ser recuperados en un rango de tiempo aceptable y en el formato necesario, dependiendo de los requerimientos a ser cumplidos?	95
11.1.4	15.1.4	Protección de los Datos y privacidad de los datos personales	¿La protección de los datos y la privacidad, están asegurados por legislaciones relevantes, regulaciones y si son aplicables, por cláusulas contractuales?	85
11.1.5	15.1.5	Prevención del mal uso de las instalaciones de procesamiento	¿El uso de instalaciones de proceso de información para cualquier propósito no autorizado o que no sea del negocio, sin la aprobación pertinente, es tratada como utilización impropia de las instalaciones?	100
			Los mensajes de alerta de ingreso, ¿son desplegados antes de permitir el ingreso a la red o a los sistemas? ¿El usuario tiene conocimiento de las alertas y reacciona apropiadamente al mensaje en pantalla?	70

Tabla 24. (Continuación).

			¿Es realizado un asesoramiento jurídico, antes de aplicar cualquier procedimiento de monitoreo y control?	100
11.1.6	15.1.6	Regulación de Controles Criptográficos	¿Los controles criptográficos son usados en cumplimiento de los acuerdos contractuales establecidos, leyes y regulaciones?	100
11.2	**15.2**	**Cumplimiento con las políticas, estándares y regulaciones técnicas**		
11.2.1	15.2.1	Cumplimiento con Políticas de Seguridad y Estándares	Los Administradores se aseguran que todos los procedimientos dentro de su área de responsabilidad, se llevan a cabo correctamente para lograr el cumplimiento de las normas y políticas de seguridad?	100
			¿Los Administradores, revisan regularmente el cumplimiento de las instalaciones de procesamiento de información dentro del área de su responsabilidad de modo a cumplir con los procedimientos y políticas de seguridad pertinentes?	100
11.2.2	15.2.2	Chequeo de Cumplimiento Técnico	¿Los sistemas de información son regularmente revisados con respecto al cumplimiento de estándares de seguridad?	90
			¿La verificación técnica es llevada a cabo por, o bajo la supervisión de, personal técnico competente y autorizado?	100
11.3	**15.3**	**Consideraciones de Auditoría de Sistemas**		
11.3.1	15.3.1	Controles de Auditoría de los Sistemas de Información	¿Los requerimientos y actividades de auditoría, incluyen verificación de sistemas de información que fueron previamente planeados cuidadosamente de modo a minimizar los riesgos de interrupciones en el proceso de negocio?	100
			¿Los requerimientos de auditoria son alcanzables y de acuerdo con una gestión adecuada?	100

Tabla 24. (Continuación).

11.3.2	15.3.2	Protección de la información contra las herramientas de auditoría	¿La información a la que se accede por medio de las herramientas de auditoría, ya sean software o archivos de datos, están protegidos para prevenir el mal uso o fuga no autorizada?	100
			¿El ambiente de auditoría está separado de los ambientes operacionales y de desarrollo, a penos que haya un nivel apropiado de protección?	90

Fuente: El Autor

11.10 Anexo J: Cumplimiento por Control

De acuerdo a la evaluación de los dominios por medio del checklist de cada uno de los controles, el resultado es el siguiente:

Tabla 25. % Cumplimiento por control

Dominio	Objetivos	Estado (%)
Políticas de Seguridad	Políticas de Seguridad de Información	93%
Organización de la Seguridad de Información	Organización Interna	90%
	Partes Externas	73%
Manejo de Activos	Responsabilidad de Activos	95%
	Clasificación de Información	93%
Seguridad de Recursos Humanos	Previo al Empleo	NA
	Durante al Empleo	NA
	Terminación o Cambio de empleo	NA
Seguridad Física y Ambiental	Áreas Seguras	98%
	Equipamiento de Seguridad	96%
Gestión de Comunicaciones y Operaciones	Procedimientos y Responsabilidades Operativas	91%
	Manejo de Entrega de Servicios Tercerizados	79%
	Planeamiento y Aceptación de Sistemas	100%
	Protección contra Código Malicioso y Móvil	78%
	Copias de Respaldo	100%
	Administración de la Seguridad en la Red	100%
	Manejo de Medios	95%
	Intercambio de Información	91%

Tabla 25. (Continuación).

	Servicios de Comercio Electrónico	98%
	Monitoreo	97%
Control de Acceso	Requerimientos del Negocio para Control de Acceso	90%
	Administración de Accesos de Usuarios	86%
	Responsabilidades de Usuarios	79%
	Control de Acceso a la Red	100%
	Control de Acceso a Sistemas Operativos	NA
	Control de Acceso a las Aplicaciones y a la Información	100%
	Computación Móvil y Teletrabajo	NA
Desarrollo, Adquisición y Mantenimiento de Sistemas de Información	Requerimientos de Seguridad de los Sistemas de Información	95%
	Procesamiento Correcto en las Aplicaciones	96%
	Controles Criptográficos	98%
	Seguridad de los Archivos de Sistemas	87%
	Seguridad en el Desarrollo y Servicios de Soporte	95%
	Gestión de Vulnerabilidades Técnicas	95%
Gestión de Incidentes de Seguridad de Información	Reportando Eventos de Seguridad y Vulnerabilidades	95%
	Gestión de Incidentes de Seguridad de la Información y Proceso de Mejoras	97%
Gestión de la Continuidad del Negocio	Aspectos de Seguridad en la Gestión de la Continuidad del Negocio	96%

Tabla 25. (Continuación).

Cumplimiento	Cumplimiento con Requerimientos Legales	91%
	Cumplimiento con las Políticas, Estándares y Regulaciones Técnicas	98%
	Consideraciones de Auditoría de Sistemas	98%

Fuente: El Autor

11.11 Anexo K: Cumplimiento por Dominio

El siguiente cuadro representa la evaluación por dominio según la ISO 27001 en el cual se puede observar que no se tiene en cuenta el dominio de seguridad en recursos humanos debido a que los evaluados se orientaron a los activos informáticos de la entidad:

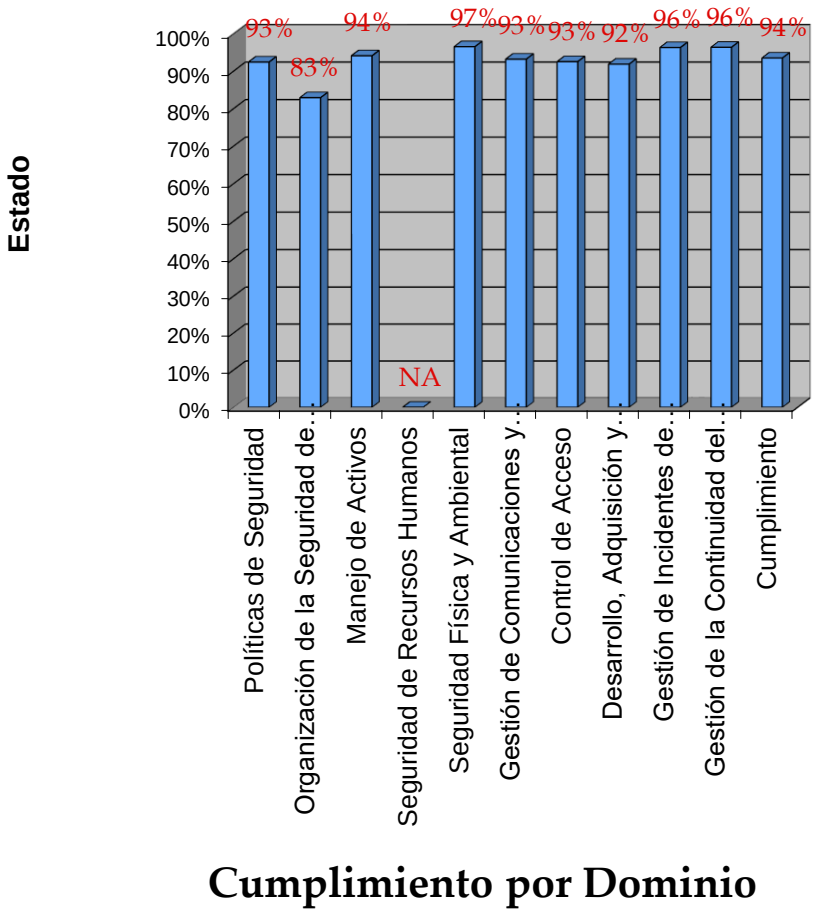
Tabla 26. % Cumplimiento por dominio

Dominio	Estado (%)
Políticas de Seguridad	93%
Organización de la Seguridad de Información	83%
Manejo de Activos	94%
Seguridad de Recursos Humanos	NA
Seguridad Física y Ambiental	97%
Gestión de Comunicaciones y Operaciones	93%
Control de Acceso	93%
Desarrollo, Adquisición y Mantenimiento de Sistemas de Información	92%
Gestión de Incidentes de Seguridad de Información	96%
Gestión de la Continuidad del Negocio	96%
Cumplimiento	94%

Fuente: El Autor

Estos resultados proporcionan una visión general del estado actual de la empresa, con respecto a la política de calidad ISO 27001, la siguiente grafica muestra los resultados de evaluación por dominio:

Fig. 3. Cumplimiento de la empresa por dominio



Cumplimiento por Dominio

Fuente: El Autor

11.12 Anexo L: Declaración de Aplicabilidad SOA

Tabla 27.SOA Políticas de Seguridad

OBJETIVOS DE CONTROL Y CONTROLES DE ACUERDO A ISO27001:2013							
Razones para la selección de controles. **RL:** Requerimientos Legales, **OC:** Obligaciones Contractuales, **RN:** Requerimientos del Negocio, **BP:** Buenas Prácticas, **RER**: Resultados de la Evaluación de Riesgos							
A.5. POLÍTICAS DE SEGURIDAD							
Nº.	**OBJETIVO**	**CONTROL**	**RL**	**OC**	**RN**	**BP**	**RER**
A.5.1	**Política de seguridad de la información**						
A.5.1.1	Documento de política de seguridad de la información.	* Conjunto de políticas para la seguridad de la información, definidas por la entidad. * Las políticas de seguridad están avaladas por la junta directiva. * La entidad socializa y publica las políticas de seguridad para que todo el personal de la empresa tenga pleno conocimiento y las pongan en práctica.	X	X	X	X	X
A.5.1.2	Revisión de la política de seguridad de la información	* Las políticas de seguridad de la información son revisadas y actualizadas por la entidad, cada determinado tiempo, de tal forma que se está a la vanguardia de los avances tecnológicos y las necesidades de seguridad	x	X	X	X	X

Tabla 27. (Continuación).

OBJETIVOS DE CONTROL Y CONTROLES DE ACUERDO ISO27001:2013							
Razones para la selección de controles. **RL:** Requerimientos Legales, **OC:** Obligaciones Contractuales, **RN:** Requerimientos del Negocio, **BP:** Buenas Practicas, **RER**: Resultados de la Evaluación de Riesgos							
A.6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.IÓN							
Nº.	**OBJETIVO**	**CONTROL**	**RL**	**OC**	**RN**	**BP**	**RER**
A.6.1	**Organización interna**						
A.6.1.1	Roles y responsabilidades para la seguridad de la información	* Los cargos de la Dirección de TIC's, definen roles y responsabilidades con respecto a la seguridad de la información.	X	X	X	X	X
A.6.1.2	Separación de deberes	* La Dirección de TIC´s cuenta con un director, y demás cargos especializados, profesionales, tecnólogos y técnicos, de acuerdo a lo requerido por la organización y sus respectivas funciones.	X	X	X	X	X
A.6.1.3	Contacto con las autoridades	* La entidad cuenta con canales de comunicación con las entidades reguladoras de acuerdo a la norma. * Se tiene una serie de formatos establecidos para los diferentes reportes que se requieren, relacionados con la seguridad de la información.	X	X	X	X	X
A.6.1.4	Contacto con grupos de interés especial	* Transmilenio por ser una entidad del estado está vigilada y supervisada por entidades como el MinTIC y Gobierno en línea, por lo tanto, se tiene contacto directo con estas entidades.	X	X	X	X	X
A.6.1.5	Seguridad de la Información en la gestión de proyectos	* La entidad tiene una serie de lineamientos establecidos, con respecto a la seguridad de la información, de acuerdo a cada departamento.		X	X	X	X
A.6.2	**Terceros**						
A.6.2.1	Política para dispositivos móviles	* La política de seguridad de la información de la entidad, abarca dispositivos como celulares y demás, de acuerdo a la norma vigente.	X	X	X	X	X
A.6.2.2	Teletrabajo	* La entidad apoyada por el programa de teletrabajo del Distrito, hace parte del plan piloto que se está implementando en la ciudad, volviéndose este un ítem adicional en la política de la empresa.			X	X	X

Tabla 27. (Continuación).

OBJETIVOS DE CONTROL Y CONTROLES DE ACUERDO ISO27001:2013							
Razones para la selección de controles. **RL:** Requerimientos Legales, **OC:** Obligaciones Contractuales, **RN:** Requerimientos del Negocio, **BP:** Buenas Practicas, **RER**: Resultados de la Evaluación de Riesgos							
A.7. GESTION DE ACTIVOS							
Nº.	**OBJETIVO**	**CONTROL**	**RL**	**OC**	**RN**	**BP**	**RER**
A.7.1	**Responsabilidad por los activos**						
A.7.1.1	Inventario de activos	* Inventario y clasificación de activos por procesos de Transmilenio.	X		X	X	X
A.7.1.2	Propiedad de los activos	* Política de gestión de activos de información. * Matriz de propietarios de información, aplicaciones y base de datos.	X		X	X	X
A.7.1.3	Uso aceptable de los activos	* Política de gestión de activos de información. * Matriz de propietarios de información, aplicaciones y base de datos.			X	X	X
A.7.2	**Clasificación de la información**						
A.7.2.1	Directrices de Clasificación.	* Política de gestión de activos de información. * Matriz de activos de información.			X	X	
A.7.2.2	Etiquetado y manejo de información.	* Política de gestión de activos de información.			X	X	
A.7.2.3	Devolución de activos	* Política de devolución de activos de cada empleado de la entidad, así como los equipos del Data Center que pertenezcan a Transmilenio.		X	X	X	X

Tabla 27. (Continuación).

OBJETIVOS DE CONTROL Y CONTROLES DE ACUERDO ISO27001:2013							
Razones para la selección de controles. **RL:** Requerimientos Legales, **OC:** Obligaciones Contractuales, **RN:** Requerimientos del Negocio, **BP:** Buenas Practicas, **RER**: Resultados de la Evaluación de Riesgos							
A.9. SEGURIDAD FÍSICA Y DEL ENTORNO							
Nº.	**OBJETIVO**	**CONTROL**	**RL**	**OC**	**RN**	**BP**	**RER**
A.9.1	**Áreas seguras.**						
A.9.1.1	Perímetro de Seguridad física	* Definir perímetro, recepción, puertas, alarmas, separación física.	X		X	X	X
A.9.1.2	Controles de acceso físico	* Registro de acceso, identificación, autorizar o revocar permisos.		X	X	X	X
A.9.1.3	Seguridad de oficinas, recintos e instalaciones	* Normas de seguridad y salud, no acceso de instalaciones, claves, estrategias y señales.			X		X
A.9.1.4	Protección contra amenazas externas y ambientales	* Protecciones físicas para desastres naturales o artificiales, ubicar equipo contra incendio adecuadamente.	X	X	X	X	X
A.9.1.5	Trabajo en áreas seguras	*Controles para empleados, contratistas, usuarios.	X		X		X
A.9.1.6	Áreas de carga, despacho y acceso público	*Habilitar el área de Almacén. Separar envíos entrantes/salientes.	X		X	X	X

Tabla 27. (Continuación).

OBJETIVOS DE CONTROL Y CONTROLES DE ACUERDO ISO27001:2013							
Razones para la selección de controles. **RL:** Requerimientos Legales, **OC:** Obligaciones Contractuales, **RN:** Requerimientos del Negocio, **BP:**Buenas Practicas, **RER**:Resultados de la Evaluación de Riesgos							
A.10. GESTION DE COMUNICACIONES Y OPERACIONES							
Nº	**OBJETIVO**	**CONTROL**	**RL**	**OC**	**RN**	**BP**	**RER**
A 10.1	**Procedimientos y Responsabilidades Operativas**						
A.10.1.1	Documentación de Procedimientos Operativos	* Documentación de los procesos operativos y disponibilidad para usarlos.	X	X		X	X
A.10.1.2	Manejo de Cambios	* Tratamiento de documentos de Transmilenio. * Control de cambios.		X	X	X	X
A.10.1.3	Segregación de Tareas	* Separación de tareas y funciones del analista de Transmilenio.	X			X	X
A.10.1.4	Separación de desarrollo, test e instalaciones operativas	*Separación de equipos de desarrollo y pruebas. * Separación de equipos operacionales.	X			X	X
A 10.2.	**Manejo de Entrega de Servicios Tercerizados**						
A.10.2.1	Entrega de Servicios	* Medidas de aseguramiento de los controles de seguridad, niveles de servicio y entrega de Transmilenio. * Verificación de los contratos de servicios con terceros.	X	X	X	X	X
A.10.2.2	Monitoreo y revisión de servicios tercerizados	* Revisión de los servicios, reportes y registros proveídos por terceros. * Controles de auditoría que son realizados a intervalos regulares sobre los servicios, reportes y registros suministrados por terceros.		X	X	X	
A.10.2.3	Manejo de Cambios de servicios tercerizados	* Gestión de los cambios en la provisión de servicios, incluyendo mantenimiento y la mejora en las políticas de seguridad de información existentes, procedimientos y controles. * Sistemas de negocio críticos, procesos involucrados y re-evaluación de riesgos.		X	X	X	X

Tabla 27. (Continuación).

A.10. GESTION DE COMUNICACIONES Y OPERACIONES							
Nº.	**OBJETIVO**	**CONTROL**	**RL**	**OC**	**RN**	**BP**	**RER**
A 10.3	**Planeamiento y Aceptación de Sistemas**						
A.10.3.1	Gestión de la Capacidad	* Monitorización de la capacidad de procesamiento de los sistemas de Transmilenio. * Disponibilidad y aseguramiento de la capacidad de proceso y almacenamiento.		X	X		X
A.10.3.2	Aceptación de Sistemas	* Establecimiento de criterios de aceptación para nuevos sistemas de información, actualizaciones y nuevas versiones.		X	X	X	X
A 10.4	**Protección contra código malicioso y móvil**						
A.10.4.1	Controles contra código malicioso	* Controles para detección, prevención y recuperado contra código malicioso. * Procedimientos apropiados de advertencia a los usuarios de Transmilenio (Alarmas).	X	X	X		X
A.10.4.2	Controles contra código móvil	* Políticas de configuración de código móvil. * Autorización de realización de código móvil.	X	X	X	X	
A 10.5	**Copias de Respaldo**						
A.10.5.1	Respaldo de la Información	* Copias de respaldo de la información y software. * Pruebas de testing para software con políticas de backup. * Recuperación la información y el software esencial en caso de ocurrencia de un desastre o fallo de medios.	X	X	X	X	X
A 10.6	**Administración de la Seguridad de la Red**						

Tabla 27. (Continuación).

A.10.6.1	Controles de Red	* Acuerdos de servicio de la seguridad, niveles de servicio y requerimientos de administración de todos los servicios de red identificados en Transmilenio.		X	X		X
A.10.6.2	Seguridad en los Servicios de Red	* Capacidad del proveedor de servicios de red de proporcionar los servicios de forma segura.	X	X		X	X
A 10.7	**Manejo de Medios**						
A.10.7.1	Manejo de medios removibles	* Política de procedimiento para el manejo de medios removibles como cintas, diskettes, tarjetas de memoria, lectores de CD, pendrives, entre otros. *Política de procedimientos y niveles de autorización están claramente definidos y documentados.	X	X	X	X	X
A.10.7.2	Disposición de los medios	* Política de eliminación de medios de forma segura bajo procedimientos formalmente establecidos.		X	X	X	X
A.10.7.3	Procedimientos de manejo de la información	* Cumplimiento de los procedimientos para el manejo del almacenamiento de la información.	X			X	X
A.10.7.4	Seguridad en la Documentación de los Sistemas	* Política de protección de los sistemas contra acceso no autorizado.	X			X	X
A 10.8	**Intercambio de Información**						
A.10.8.1	Políticas y Procedimientos de intercambio de información	* Política formal, procedimientos y/o controles aplicados para asegurar la protección a la información.		X	X		X
A.10.8.2	Acuerdos de Intercambio	* Acuerdos de intercambio de información y software entre Transmilenio y partes externas.	X	X	X	X	X
A.10.8.3	Medios físicos en tránsito	* Políticas de protección contra acceso no autorizado de los medios físicos o corrupción de la información.	X		X	X	X
A.10.8.4	Mensajería Electrónica	* Política de protección de mensajería electrónica	X			X	X

Tabla 27. (Continuación).

A.10.8.5	Sistema de información empresarial	* Fortalecimiento de las políticas de la protección de la información.	X	x			X

A.10. GESTION DE COMUNICACIONES Y OPERACIONES							
Nº.	**OBJETIVO**	**CONTROL**	**RL**	**OC**	**RN**	**BP**	**RER**
A 10.9	**Servicios de Comercio Electrónico**						
A.10.9.1	Comercio Electrónico	* Acuerdos de comercio electrónico entre los socios comerciales de Transmilenio en cuestiones de seguridad de la información. * Aplicación de controles Criptográficos		X	X		X
A.10.9.2	Transacciones On-line	* Protección de transacciones en línea protegida contra transmisiones incompletas, mal ruteo, alteración de mensajería, divulgación no autorizada, duplicación no autorizada o replicación.	X	X		X	X
A.10.9.3	Información disponible públicamente	* Integridad de la información disponible públicamente contra modificaciones no autorizadas.	X		X		
A 10.10	**Monitoreo**						
A.10.10.1	Registros de Auditoría	* Periodo de información guardada sobre los usuarios, excepciones, eventos de seguridad de información que ocurren, con el fin de realizar registros de auditoria. * Aplicación de controles Criptográficos.		X	X		X
A.10.10.2	Uso de Sistemas de Monitoreo	* Desarrollo de procedimientos de monitoreo de equipos de procesamiento de datos. *Niveles de monitoreo requeridos por los equipos de procesamiento de información son determinados por un análisis de riesgos.	X	X	X	X	X
A.10.10.3	Protección de los Logs	* Protección de los registros de auditoria contra posibles manipulaciones y acceso no autorizado.	X		X	X	

Tabla 27. (Continuación).

A.10.10.4	Log de actividades de Administradores y Operadores	* Registro de las actividades de los administradores y operadores de Transmilenio.	X	X	X		X
A.10.10.5	Registro de Fallas	* Niveles de registros en logs requeridos para cada sistema individual.	X	X		X	X
A.10.10.6	Sincronización de relojes	* Sincronización de relojes de todos los sistemas de información.	X		X	X	X

OBJETIVOS DE CONTROL Y CONTROLES DE ACUERDO ISO27001:2013							
Razones para la selección de controles. **RL:** Requerimientos Legales, **OC:** Obligaciones Contractuales, **RN:** Requerimientos del Negocio, **BP:**Buenas Practicas, **RER**:Resultados de la Evaluación de Riesgos							
A.11. CONTROL DE ACCESO							
Nº.	**OBJETIVO**	**CONTROL**	**RL**	**OC**	**RN**	**BP**	**RER**
A.11.1	**Requisitos de negocio para el control de acceso.**						
A.11.1.1	Políticas de control de acceso	* Establecer, doc y revisar reglas y derechos de cada usuario int/ext en servicios y sistemas. Requisitos de seg de sw.			X	X	X
A.11.2	**Gestión de acceso de usuario.**						
A.11.2.1	Registro de usuarios	* Procedimiento de registro/cancelación de usuarios para sistemas y servicios, autorización, verificación, dar a usuario declaración escrita de sus derechos.		X	X	X	X
A.11.2.2	Gestión de privilegios	* Identificar usuarios, privilegios por producto como S.O., SGB.D, aplicaciones.	X	X	X	X	X
A.11.2.3	Gestión de contraseñas para usuarios	* Declaración firmada de confidencial de contraseñas, procedimientos de verificación de ID Plan de recuperación de desastres.	X		X		X
A.11.2.4	Revisión de los derechos de acceso de los usuarios	* Procedimiento de revisión/reasignación de contraseña-cambio contrato laboral.		X	X	X	X
A.11.3	**Responsabilidades de los usuarios.**						
A.11.3.1	Uso de contraseñas	* Buenas practicas-uso de contraseñas.			X	X	

Tabla 27. (Continuación).

A.11.3.2	Equipo de usuario desatendido	* Protección como protector de pantalla, logout, apagar, bloqueo-contraseña.	X	X	X	X	X
A.11.3.3	Política de escritorio despejado y de pantalla despejada	* Políticas: guardar gabinetes, cerrar sesión, correo, uso no autorizado de fotocopiadora-scanner, cámaras, entre otras.	X		X	X	

A.11. CONTROL DE ACCESO							
Nº.	**OBJETIVO**	**CONTROL**	**RL**	**OC**	**RN**	**BP**	**RER**
A.11.4	**Control de acceso a las redes.**						
A.11.4.1	Política de uso de los servicios en red	* Procedimiento para autorización uso de redes y servicios.	X	X	X	X	X
A.11.4.2	autenticación de usuarios para conexiones externas	* Métodos de autenticación para controlar accesos remotos.	X	X	X	X	X
A.11.4.3	Identificación de los equipos en las redes	* autenticar en ubicaciones específicas.	X		X		X
A.11.4.4	Protección de los puertos de configuración y diagnostico remoto	*Control de acceso a puertos, inhabilitar o retirar si no se requiere.	X	X	X		X
A.11.4.5	Separación en las redes	* Grupos de servicios de información, usuarios, sistemas de información. División de dominios lógicos – firewall, conmutación IP, red privada. Red Wifi.	X		X	X	X
A.11.4.6	Control de conexión a las redes	* Política de control, mensajería, transferencia de archivos, acceso interactivo, acceso a aplicaciones. Redes compartidas.	X	X	X	X	X
A.11.4.7	Control de enrutamiento en la red	* Mecanismos de verificación direcciones fuente/destino: validos.	X			X	X
A.11.5	**Control de acceso al sistema operativo.**						

Tabla 27. (Continuación).

A.11.5.1	Procedimientos de registro de inicio seguro	* Acceso a S.O, intentos (3), registro.	X		X		X
A.11.5.2	Identificación y autenticación de usuarios	* Identificador único, token, criptografía, medios biométricos.	X	X	X	X	X
A.11.5.3	Sistema de gestión de contraseñas	* Sistemas Interactivos y contraseñas de calidad.	X	X	X		X
A.11.5.4	Uso de las utilidades del sistema	* Control de acceso a puertos, inhabilitar o retirar si no se requiere.	X		X	X	
A.11.5.5	Tiempo de inactividad de la sesión	* Utilidad para suspender sesión.	X	X	X	X	X
A.11.5.6	Limitación del tiempo de conexión	* Controles de T para aplicaciones sensibles, horario, repetición de autenticación.	X	X	X		X

OBJETIVOS DE CONTROL Y CONTROLES DE ACUERDO ISO27001:2013							
Razones para la selección de controles. **RL:** Requerimientos Legales, **OC:**Obligaciones Contractuales,**RN:** Requerimientos del Negocio, **BP**:Buenas Practicas, **RER**:Resultados de la Evaluación de Riesgos							
A.12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN							
Nº.	**OBJETIVO**	**CONTROL**	**RL**	**OC**	**RN**	**BP**	**RER**
A.12.1	**Requisitos de seguridad de los sistemas de información.**						
A.12.1.1	Análisis y especificaciones de los Requisitos de seguridad	* Incluir Requisitos de seguridad. *Proceso formal de adquisición y prueba. * Requisitos en la etapa de diseño.			X	X	X
A.12.2	**Procesamiento correcto en las aplicaciones.**						
A.12.2.1	Validación de los datos de entrada	* Procedimiento de prueba y validación de datos, errores, responsabilidades en la entrada.		X	X	X	X
A.12.2.2	Control de procesamiento interno	* Procedimiento para verificar procesos del sw.	X	X	X	X	X
A.12.2.3	Integridad del mensaje	* Identificar requisitos para autenticidad-integridad.	X		X		X

Tabla 27. (Continuación).

A.12.2.4	Validación de los datos de salida	* Procedimiento de pruebas, responsabilidades, registro de esta validación.		X	X	X	X
A.12.3	**Controles criptográficos.**						
A.12.3.1	Política sobre el uso de controles criptográficos	* Políticas de encript en medios móviles, claves, recuperación, responsabilidades.			X	X	
A.12.3.2	Gestión de claves	* Proteger las claves criptográficas por modificación, pérdida, destrucción. * Registro y auditoria de claves.	X	X	X	X	X

A.12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN							
Nº.	**OBJETIVO**	**CONTROL**	**RL**	**OC**	**RN**	**BP**	**RER**
A.12.4	**Seguridad de los archivos del sistema.**						
A.12.4.1	Control del software operativo	* Procedimientos instalación en SO con autorización. Sistema de Control de Configuración, política de restaurar estado anterior, registro de auditoria de actualizaciones, monitorear proveedor.	X	X	X	X	X
A.12.4.2	Protección de los datos de prueba del sistema	* Autorizar la copia de prueba, borrar, rastro de auditoria.	X	X	X	X	X
A.12.4.3	Control de acceso al código fuente de los programas	* Control, procedimiento de control de cambio.	X		X		X
A.12.5	**Seguridad en los procesos de desarrollo y soporte.**						
A.12.5.1	Procedimientos de control de cambios.	* Documentar procedimientos S.I. aprobación.	X		X		X
A.12.5.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo	* Procedimiento de integridad y control de aplicación, plan de revisión,	X	X	X	X	X

Tabla 27. (Continuación).

A.12.5.3	Restricciones en los cambios a los paquetes de software	* Programa estándar de actualizaciones.	X	X	X		X
A.12.5.4	Fuga de información	* Explorar medios de salida, uso de alto nivel de sistemas y sw. Monitoreo personal-sistemas.	X		X	X	
A.12.5.5	Desarrollo de software contratado externamente	* Acuerdos, convenios, derechos P.I.	X	X	X	X	X
A.12.6	**Seguridad en los procesos de desarrollo y soporte.**						
A.12.6.1	Control de las vulnerabilidades técnicas	* Proceso= identificar vulnerabilidades de sistemas en uso, instalar parches.	X		X		X
OBJETIVOS DE CONTROL Y CONTROLES DE ACUERDO ISO27001:2013							
Razones para la selección de controles. **RL:** Requerimientos Legales, **OC:** Obligaciones Contractuales, **RN:** Requerimientos del Negocio, **BP:** Buenas Practicas, **RER**: Resultados de la Evaluación de Riesgos							
A.13. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION							
Nº.	**OBJETIVO**	**CONTROL**	**RL**	**OC**	**RN**	**BP**	**RER**
A.13.1	**Reportando Eventos de Seguridad y Vulnerabilidades**						
A.13.1.1	Reportando Eventos de Seguridad de la Información	* Documentación de los reportes e implementación de procedimientos de Transmilenio. * Reporte de eventos de seguridad sobre canales correspondientes.	X	X		X	X
A.13.1.2	Reportando Vulnerabilidades de la Seguridad	* Procedimientos que aseguren que todos los empleados deben reportar cualquier vulnerabilidad en la seguridad en los servicios o sistemas de información.		X	X	X	X
A.13.2	**Gestión de Incidentes de Seguridad de la Información y Proceso de Mejoras**						

Tabla 27. (Continuación).

A.13.2.1	Responsabilidades y Procedimientos	* Monitoreo de sistemas, alertas y vulnerabilidades para detectar incidentes de seguridad.	X	X	X	X	X
A.13.2.2	Aprendiendo de los Incidentes de Seguridad de la Información	* Revisión de los servicios, reportes y registros proveídos por terceros. * Objetivos de la gestión de incidentes de seguridad de información, están acordados con las gerencias.	X	X	X	X	
A.13.2.3	Recolección de Evidencia	* Los procedimientos internos desarrollados y seguidos al pie de la letra cuando se debe recolectar y presentar evidencia para propósitos disciplinarios dentro de la organización.	X	X	X		X
OBJETIVOS DE CONTROL Y CONTROLES DE ACUERDO ISO27001:2013							
Razones para la selección de controles. **RL:** Requerimientos Legales, **OC:** Obligaciones Contractuales, **RN:** Requerimientos del Negocio, **BP:** Buenas Practicas, **RER**: Resultados de la Evaluación de Riesgos							
A.14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO							
Nº.	**OBJETIVO**	**CONTROL**	**RL**	**OC**	**RN**	**BP**	**RER**
A.14.1	**Aspectos de Seguridad de la Información, de la Gestión de la Continuidad del Negocio**						

Tabla 27. (Continuación).

A.14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	* Manual del Plan de Continuidad del Negocio (PCN). * Instructivo para el registro de eventos de riesgo. * Formato de eventos generales de riesgo. *Formato procedimiento en contingencia. * Plan de respuesta ante sismo, incendio o amenaza de bomba. * Plan de contingencia atención al ciudadano. * Instructivo preparación y respuesta ante emergencias. * Se tienen esquemas de Alta disponibilidad en el Data Center principal, procedimientos de contingencia y Data Center Alterno.			X	X	X
A.14.1.2	Continuidad del negocio y evaluación de riesgos.	* Manual gestión de riesgos. * Se tienen esquemas de Alta disponibilidad en el Data Center principal, procedimientos de contingencia y Data Center Alterno. * Diseño del BCP, Diseño del plan DRP con estrategias alternativas. Plan de recuperación de desastres. * Planeamiento de continuidad del negocio y administración de crisis.	X		X	X	X
A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información.	* Plan de recuperación de desastres. Se realizaron pruebas integradas de DRP y cinco (5) pruebas de escritorio. * Diseño del BCP, Diseño del plan DRP con estrategias alternativas. Plan de recuperación de desastres * Planeamiento de continuidad del negocio y administración de crisis.	X		X	X	X
A.14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO							
Nº.	**OBJETIVO**	**CONTROL**	**RL**	**OC**	**RN**	**BP**	**RER**
A.14.1.4	Estructura para la planificación de la continuidad del negocio.	* Diseño del BCP, Diseño del plan DRP con estrategias alternativas. Plan de recuperación de desastres.	X		X	X	X
A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio.	* Se realizan pruebas periódicas de los planes de continuidad del negocio y DRP para garantizar su efectividad.			X	X	X

Tabla 27. (Continuación).

A.15 CUMPLIMIENTO							
Nº.	**OBJETIVO**	**CONTROL**	**RL**	**OC**	**RN**	**BP**	**RER**
A.15.1	**Cumplimiento de los requisitos legales**						
A.15.1.1	Identificación de la legislación aplicable	* Hacer resumen de normatividad y actualizarlo.			X	X	X
A.15.1.2	Derechos de propiedad intelectual (DPI)	* Procedimiento para cumplir DPI.	X		X	X	X
A.15.1.3	Protección de los registros de la organización	* Controles para salvaguardar registros.	X		X	X	X
A.15.1.4	Protección de los datos y privacidad de la información personal	* Cláusulas -controles a la recolección, procesamiento y transmisión de datos personales.	X		X	X	X
A.15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información	* Procesamiento de información solo para proceso de negocio-procedimiento de monitoreo.			X	X	X
A.15.1.6	Reglamentación de los controles criptográficos	* Controles criptográficos deben cumplir la ley.			X	X	X
A.15.2	**Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.**						
A.15.2.1	Cumplimiento con las políticas y las normas de seguridad	* Procedimiento, formato para registrar el cumplimiento.			X	X	X
A.15.2.2	verificación del cumplimiento técnico	* Verificar para que cumplan con la norma.	X		X	X	X
A.15.3	**Consideraciones de la auditoría de los sistemas de información.**						
A.15.3.1	Controles de auditoría de los sistemas de información	* Proteger el sistema operativo, documentar procedimiento.			X	X	X
A.15.3.2	Protección de las herramientas de auditoría de los sistemas de información	* Proteger estas herramientas.	X		X	X	X

Fuente: El Autor

11.13 Anexo M: Plan de Tratamiento de Riesgos PTR

Tabla 28.PTR Plan de Tratamiento de Riesgos

ID	CONTROL	ACTIVO DE INFORMACIÓN	ACTIVIDAD / DESCRIPCIÓN	PRI	ESTADO	RESPONSABLE
POLÍTICAS DE SEGURIDAD						
A.5.1.1	Documento de política de seguridad de la información.	Política de seguridad de la información	El documento de la política de seguridad de la información, debe ser aprobado por los directivos, publicado y comunicado a todos los empleados y partes externas.	A	Culminado	Seguridad Informática
A.5.1.2	Revisión de la política de seguridad de la información	Política de seguridad de la información	La política de seguridad de la información debe ser revisada a intervalos planeados, o si se presentan cambios significativos, para garantizar la continuidad, sostenibilidad y efectividad.	A	Culminado	Seguridad Informática
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN						
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Máquinas físicas que soportan los aplicativos, bases de datos y almacenamiento	La Dirección debe apoyar activamente la seguridad dentro de la entidad con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información.	A	Culminado	Administración TI
A.6.1.2	Separación de deberes	Recurso humano	Las actividades de seguridad de la información deben ser coordinadas por los representantes de todas las áreas de la entidad con roles y funciones laborales pertinentes, según lo definido en la estructura institucional.	A	Culminado	Administración TI

Tabla 28. (Continuación).

A.6.1.3	Contacto con las autoridades	Recurso Humano	Transmilenio debe mantener contactos apropiados con las autoridades pertinentes.	A	Avanzado	Planeación y Riesgo
A.6.1.4	Contacto con grupos de interés especial	Recurso Humano	Contactos adecuados con grupos especiales de interés u otros foros especializados de seguridad o asociaciones profesionales deben ser implementados.	M	En Progreso	Planeación y Riesgo
A.6.1.5	Seguridad de la Información en la gestión de proyectos	Máquinas físicas que soportan los aplicativos, bases de datos, almacenamiento y recurso humano	Todos los requerimientos de seguridad deben ser atendidos en cada proyecto, de tal forma que se restrinja el acceso a los clientes según se requiera para garantizar la seguridad de la información.	A	Avanzado	Seguridad Informática
A.6.2.1	Política para dispositivos móviles	Dispositivos móviles computación y comunicaciones	Se debe establecer una política formal y se debe adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.	A	Avanzado	Seguridad Informática
A.6.2.2	Teletrabajo	Recurso humano	Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo.	A	Avanzado	Seguridad Informática
GESTIÓN DE ACTIVOS						
A.7.1.1	Inventario de activos.	Política de inventarios de activos	Transmilenio debe controlar todos los activos para que cada uno esté claramente identificado, confeccionando y manteniendo un inventario con los más importantes de Transmilenio.	A	Culminado	Planeación y Riesgo

Tabla 28. (Continuación).

A.7.1.2	Propiedad de los activos.	Base de datos de la configuración	Transmilenio debe tener toda la información y activos asociados a los recursos para el tratamiento de la información designada a una parte de la Organización.	A	Culminado	Seguridad Informática
A.7.1.3	Uso aceptable de los activos.	Política de uso correcto de cada uno de los activos en función con sus objetivos	Transmilenio debe identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.	A	Avanzado	Seguridad Informática
A.7.2.1	Directrices de clasificación.	Política de gestión de la información.	Transmilenio debe clasificar la información en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.	A	Avanzado	Planeación y Riesgo
A.7.2.2	Etiquetado y manipulado de la información.	Política de tratamiento de información.	Transmilenio debe desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la Organización.	A	Avanzado	Planeación y Riesgo
GESTIÓN DE COMUNICACIONES Y OPERACIONES						
A.10.2.1	Entrega de Servicios	Equipos terminales de usuarios funcionales	Se debe identificar los servicios que van tercerizados ya que deben tener un control de seguridad según la políticas internas de Transmilenio. Se debe generar un acta de entrega de los equipos a monitorear por terceros.	A	Avanzado	administración TI

Tabla 28. (Continuación).

A.10.2.2	Monitoreo y revisión de servicios tercerizados	Servidor de archivos que soportan la plataforma y aplicaciones	Revisión constante de los servicios que soportan los terceros, así como los reportes que semanalmente deben realizar confirmando la estabilidad de la red y las anomalías que se han encontrado. Para esto, se debe generar un registro de peticiones al tercero con el fin de llevar el control realizado.	A	Culminado	Seguridad Informática
A.10.2.3	Manejo de Cambios de servicios tercerizados	Máquinas físicas que soportan los aplicativos, bases de datos y almacenamiento	Transmilenio debe solicitar al tercero, el mejoramiento del servicio contratado, esto aplica para las políticas internas de la empresa que exigen el mejoramiento de la red, por lo tanto se debe crear un formato de mejoramiento.	M	En Progreso	Seguridad Informática
A.10.3.1	Gestión de la Capacidad	Seguridad de trafico de información SIAF (SP-ERP) Motor gestor de bases de datos principal TOAD CAT	Para Transmilenio la seguridad de la información es de vital importancia, por lo que las actividades de monitorización de su herramienta y servidores, deben soportar la capacidad que esto requiere, por lo que debe garantizar de forma óptima este ítem, además de garantizar la integridad del sistema, disponibilidad e integración de todas las herramientas.	A	Avanzado	administración TI

Tabla 28. (Continuación).

A.10.3.2	Aceptación de Sistemas	Equipos y dispositivos de red activos	Transmilenio establece una política de estudio para la integración de un nuevo software, ya que antes de integrarla a las demás herramientas, se deben crear los respectivos manuales de uso y capacitación de la misma, para optimizar el conocimiento y experiencia de los usuarios finales.	A	Avanzado	seguridad Informática
A.10.4.1	Controles contra código malicioso	SIAF (SP-ERP) Motor gestor de bases de datos principal TOAD CAT	Las políticas de seguridad de Transmilenio, deben establecer métodos de controles con el código malicioso, por ende el administrador de la red debe implementar configuración de seguridad y cortafuegos para prevenir cualquier ataque de código malicioso que perjudique la integridad de la información, además se debe realizar la instalación de un PKI, y un IDS para la detección de intrusos.	A	Avanzado	seguridad Informática
A.10.4.2	Controles contra código móvil	Seguridad de trafico de información SIAF (SP-ERP) Motor gestor de bases de datos principal TOAD CAT	Transmilenio debe establecer un gobierno de control de privilegios para uso de código móvil, ya que este tipo de privilegios establece un tipo de formato de solicitud de autorización de privilegios para el código móvil, debido a que cualquier cambio puede alterar la funcionalidad de las aplicaciones ya preinstaladas.	A	Avanzado	seguridad Informática

Tabla 28. (Continuación).

GESTIÓN DE COMUNICACIONES Y OPERACIONES						
A.10.5.1	Respaldo de la Información	Máquinas físicas que soportan los aplicativos, bases de datos y almacenamiento	Transmilenio debe establecer el procedimiento para realizar el respaldo o backup de la información, utilizando el método Abuelo-Padre-Hijo, el cual consiste en realizar backup de la información diaria, Semanal y mensual, ya que es de vital importancia tener la información más vulnerable resguardada.	A	Avanzado	seguridad Informática
A.10.6.1	Controles de Red	Equipos y dispositivos de red activos	Transmilenio debe implementar la acción e implementación de controles por listas de acceso para los enrutadores del trafico TCP, además de levantamiento del protocolo EIGRP para la interconexión de sedes.	A	Avanzado	seguridad Informática
A.10.6.2	Seguridad en los Servicios de Red	Equipos y dispositivos de red activos	Se debe implementar el uso de dispositivos robustos de red para salvaguardar el tráfico y toda la información que pase por los canales internos de Transmilenio.	A	Avanzado	seguridad Informática
A.10.7.1	Manejo de medios removibles	Máquinas físicas que soportan los aplicativos, bases de datos y almacenamiento	Transmilenio debe realizar el proceso de bloqueo de los puertos, bandeja de medios ópticos entre otros, para evitar la integración de malware en la red LAN de la empresa, además de proteger la información sensible.	A	Avanzado	administración TI
A.10.7.2	Disposición de los medios	Equipos y dispositivos de red activos	Establecer un procedimiento para la eliminación de los riesgos de forma controlada, llevando un formato de registro.	A	En Progreso	planeación y Riesgo

Tabla 28. (Continuación).

A.10.7.3	Procedimientos de manejo de la información	Máquinas físicas que soportan los aplicativos, bases de datos y almacenamiento	Transmilenio debe establecer el procedimiento para el manejo adecuado de la información interna, esto se realiza mediante capacitación al personal interno ya que se realiza una educación al usuario.	A	Avanzado	seguridad Informática
A.10.7.4	Seguridad en la Documentación de los Sistemas	Seguridad en la Documentación de los Sistemas	Se debe implementar el uso de protocolos y herramientas de monitoreo de la información entrante y saliente, además de resguardar la documentación de los procesos internos, en donde solo los usuario de Transmilenio tendrían acceso.	A	Avanzado	seguridad Informática
A.10.8.1	Políticas y Procedimientos de intercambio de información	Seguridad de trafico de información	Transmilenio debe realizar la política de intercambio de información por medio de registro de intercambio ya que debe quedar registrado todo intercambio y modificaciones que se hayan realizado, esto con el fin de resguardar la información, esto establece la política de seguridad.	A	Culminado	planeación y Riesgo
		SIAF (SP-ERP)				
		Motor gestor de bases de datos principal				
		TOAD				
		CAT				
A.10.8.2	Acuerdos de Intercambio	Políticas de intercambio	Se establece una política para el acceso de intercambio de la información, para acceder a la información privilegiada, se debe solicitar acceso por medio de un formato de solicitud de acceso.	A	Culminado	planeación y Riesgo

Tabla 28. (Continuación).

A.10.8.3	Medios físicos en transito	Seguridad de trafico de información	Por medio de la implementación de protocolos de cifrado, Transmilenio debe establecer una infraestructura de clave pública.	A	Culminado	administración TI
A.10.8.4	Mensajería Electrónica	Seguridad de trafico de información	Transmilenio debe realizar una zona desmilitarizada para salvaguardar la información de la red pública.	A	Avanzado	seguridad Informática
A.10.8.5	Sistema de información empresarial	Políticas de intercambio	Transmilenio debe garantizar el fortalecimiento de las políticas de seguridad empresarial, para el mejoramiento de dichas políticas se establecerá una encuesta periódica para el mejoramiento.	A	Avanzado	planeación y Riesgo
A.10.9.1	Comercio Electrónico	Seguridad de trafico de información	Se debe exigir a los usuarios internos no realizar transacciones personales, cualquier anomalía que se presente en el sistema deben abrir una incidencia con el cliente interno para realizar la trazabilidad de las transacciones fallidas.	A	Avanzado	seguridad Informática
A.10.9.2	Transacciones On-line	Seguridad de trafico de información	Se deben garantizar las transacciones en línea del portal, para lo cual la conectividad nunca se debe interrumpir para dar la fiabilidad a los datos.	A	Avanzado	seguridad Informática
A.10.9.3	Información disponible públicamente	Seguridad en la Documentación de los Sistemas	Se debe garantizar la disponibilidad e integridad de la información de acceso a los usuarios, por lo tanto se debe hacer uso de intranet para realizar el vínculo con el usuario final.	A	Culminado	seguridad Informática
A.10.10.1	Registros de Auditoría	Seguridad en la Documentación de los Sistemas	Cada vez que se realiza una auditoria a los sistemas de la información de Transmilenio, siempre debe quedar registro de la auditoria, ya que se debe dejar un historial de reconocimiento de las vulnerabilidades.	A	Avanzado	planeación y Riesgo
A.10.10.2	Uso de Sistemas de Monitoreo	Seguridad de trafico de información	Se debe establecer un sistema de monitoreo permanente, para encontrar trafico irregular, ya que esto resguarda la seguridad de la información	A	Culminado	administración TI

Tabla 28. (Continuación).

A.10.10.3	Protección de los Logs	Seguridad de trafico de información SIAF (SP-ERP) Motor gestor de bases de datos principal TOAD CAT	Los dispositivos de red, generan una serie de log's de eventos en donde se recopila toda la información de qué pasa en la red, y allí se pueden observar alarmas de todo tipo. El listado de log's debe ser resguardado y cifrado para evitar ser alterado por intrusos.	A	Avanzado	administración TI
A.10.10.4	Log de actividades de Administradores y Operadores	Seguridad de tráfico de información	Deben ser guardados los lgo de los administradores con mayores privilegios como política de seguridad de la información.	A	Avanzado	administración TI
A.10.10.5	Registro de Fallas	Equipos y dispositivos de red activos	Los usuarios finales deben reportar a la línea de cliente interno, cualquier anomalía o fallas en aplicaciones o en la red, el cual le proveerá el número de un consecutivo o incidente para dar una solución desde la mesa de servicios.	A	Avanzado	administración TI
A.10.10.6	Sincronización de relojes	Equipos y dispositivos de red activos	El administrador de la red debe configurar un servidor de sincronización de relojes de todas las máquinas que soportan una aplicación y da conectividad a una red de oficinas.	A	Avanzado	planeación y Riesgo
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN						
A.13.1.1	Reportando Eventos de Seguridad de la Información	Seguridad de tráfico de información SIAF (SP-ERP)	Los usuarios deben reportar a la mesa de ayuda de las aplicaciones las fallas en los servidores y eventos que comprometan la seguridad de la información, esto se realiza con un consecutivo de incidencia para dar solución a la falla reportada.	A	Culminado	Seguridad Informática

Tabla 28. (Continuación).

		Motor gestor de bases de datos principal TOAD CAT				
A.13.1.2	Reportando Vulnerabilidades de la Seguridad	Seguridad de tráfico de información	Los usuarios deben reportar a la mesa de ayuda de las aplicaciones las fallas en los servidores y eventos que comprometan la seguridad de la información, esto se realiza con un consecutivo de incidencia para dar solución a la falla reportada.	A	Culminado	Planeación y Riesgo
A.13.2.1	Responsabilidades y Procedimientos	Máquinas físicas que soportan los aplicativos, bases de datos y almacenamiento	Se rige de la imposición de los procedimientos a seguir para el cumplimiento de las responsabilidades del cliente interno con el fin de realizar el reporte correspondiente a la mesa de ayuda.	A	Culminado	Seguridad Informática
A.13.2.2	Aprendiendo de los Incidentes de Seguridad de la Información	Políticas de intercambio	Mediante el registro de las incidencias reportadas por los usuarios, se corrigen vulnerabilidades encontradas, el cual además se apoya en la documentación para tener un histórico de los eventos expuestos para la solución.	A	Culminado	Seguridad Informática
A.13.2.3	Recolección de Evidencia	Política de seguridad de la información	Se debe recolectar evidencia mediante la documentación de las incidencias, por medio de pruebas, monitoreo, solicitudes, imágenes de las fallas expuestas para solución y todos los reportes de las eventualidades que realizan los usuarios.	A	Culminado	Seguridad Informática

Tabla 28. (Continuación).

GESTIÓN DE LA CONTINUIDAD						
A.14.1.1	Proceso de la gestión de continuidad del negocio	Política de gestión de la continuidad del negocio	Transmilenio debe desarrollar y mantener un proceso de gestión de la continuidad del negocio en la organización que trate los requerimientos de seguridad de la información necesarios para la continuidad del negocio.	A	Culminado	Seguridad Informática
A.14.1.2	Continuidad del negocio y análisis de impactos	Vulnerabilidades y riesgos de los activos informáticos	Transmilenio debe identificar los eventos que puedan causar interrupciones a los procesos de negocio junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información.	A	Culminado	Planeación y Riesgo
A.14.1.3	Redacción e implantación de planes de continuidad	Plan de recuperación de desastres	Transmilenio debe desarrollar e implantar planes de mantenimiento o recuperación de las operaciones del negocio para asegurar la disponibilidad de la información en el grado y en las escalas de tiempo requeridas, tras la interrupción o fallo de los procesos críticos de negocio.	A	Culminado	Seguridad Informática
A.14.1.4	Marco de planificación para la continuidad del negocio	Tratamiento y afinación del plan de continuidad del negocio	Transmilenio debe mantener un esquema único de planes de continuidad del negocio para garantizar que sean consistentes, para tratar los requisitos de seguridad y para identificar las prioridades de prueba y mantenimiento.	A	Culminado	Seguridad Informática
A.14.1.5	Prueba, mantenimiento y reevaluación de planes de continuidad	Pruebas controladas con toda la organización en la continuidad del negocio.	Transmilenio debe probar regularmente los planes de continuidad del negocio para garantizar su actualización y eficacia.	A	Culminado	Seguridad Informática

Fuente: El Autor

11.14 Anexo N: Resumen Analítico RAE

Tabla 29.Resumen Analítico RAE

Tipo de documento	Trabajo de grado
Título	Estudio del modelo de seguridad de la información para la empresa Transmilenio S.A., acorde a la norma ISO/IEC 27001 versión 2013
Autor	QUINTERO, Nicolás
Año	2018
Palabras Claves	Transmilenio, Seguridad Informática, SGSI, Riesgo, Magerit, Amenazas. ISO27001, Activo
Descripción	El proyecto pretende contribuir a la empresa Transmilenio S.A., en la construcción de un modelo de seguridad informática, que se ajuste a los requerimientos de la Estrategia de Gobierno en Línea, la cual exige mediante decreto regulatorio a las entidades públicas, acogerse a dicha iniciativa. El modelo está basado en la norma ISO/IEC 27001 VERSIÓN 2013 y abarca todos los dominios y controles que contribuyen a alcanzar altos niveles en seguridad informática.

Tabla 29. (Continuación).

Fuentes Bibliográficas	9. fuentes bibliográficas relacionadas con los Sistemas de Gestión de la Seguridad Informática – SGSI, las metodologías, normas y lineamientos de la estrategia de Gobierno en línea, que contribuyen al desarrollo del modelo: ISO2700.es. ¿Qué es un SGSI? [en línea]. <http://www.iso27000.es/sgsi.html> [citado en 15 de Octubre de 2016] ISO27000.es. Sistema de Gestión de la Seguridad de la Información. [en línea]. <http://www.iso27000.es/doc_sgsi_all.htm> [citado en 15 de Octubre de 2016] ISO 27001: La Seguridad de la Información en la Gestión de la Continuidad de Negocio. [en línea]. <http://www.pmg-ssi.com/2014/11/iso-27001-la-seguridad-de-la-informacion-en-la-gestion-de-la-continuidad-de-negocio/> [citado en 15 de Octubre de 2016] JIMÉNEZ, L. Guía de desarrollo de un plan de continuidad de negocio. [en línea]. <http://www.criptored.upm.es/guiateoria/gt_m001r.htm> [citado en 30 de Octubre de 2016] LERMA, Héctor Daniel. Metodología de la investigación. Bogotá: Ecoe Ediciones, 2004. MENDEZ, C. Metodología, Diseño y Desarrollo del proceso de Investigación. Tercera Edición, McGraw Hill, Colombia, 2001. MITIC. Fortalecimiento de la Gestión TI en el Estado. Modelo de Seguridad. [En línea]. http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos NTC-ISO/IEC 27005, Tecnología de la información. Código de práctica para la gestión de la seguridad de la información.

Tabla 29. (Continuación).

Contenido	Introducción, Planteamiento del problema, Objetivos, Situación actual de la empresa, Justificación, Alcance y Delimitación del proyecto, Marco referencial, Marco metodológico, Producto resultado a entregar, Conclusiones y Recomendaciones, Bibliografía, Anexos
Objetivo General	Realizar un estudio de seguridad de la información para la empresa Transmilenio S.A. de acuerdo a la norma ISO/IEC 27001 versión 2013, según los lineamientos de la Estrategia de Gobierno en Línea.
Objetivos específicos	Realizar el levantamiento de la información a través metodologías de análisis y gestión de riesgos, normatividad, técnicas de pentesting, del estado actual de la seguridad de la empresa Transmilenio. Determinar y aplicar las metodologías de análisis y gestión de riesgos en la empresa Transmilenio S.A. Elaborar la propuesta de solución de seguridad para la empresa Transmilenio S.A., con base a la norma ISO/IEC 27001 versión 2013, de acuerdo a lo requerido por la Estrategia de Gobierno en Línea.
Metodología	**Tipo de investigación:** Proyecto aplicado **Población:** 420 funcionarios de la empresa Transmilenio S.A., a los cuales se les realizó levantamiento de información de activos informáticos para el análisis e identificación del estado de la empresa. **Fase 1:** Selección fuentes bibliográficas **Fase 2:** Reconocimiento de la empresa mediante observación, entrevistas y encuestas de seguridad informática **Fase 3:** Levantamiento de información de activos informáticos

Tabla 29. (Continuación).

	Fase 4: Sistematización y análisis de resultados **Fase 5:** Elaboración entregables
Conclusiones	El proyecto resalta las ventajas de trabajar con la metodología Magerit, en el tratamiento de los activos informáticos y la efectividad que logra la empresa en la solución de riesgos y amenazas sobre la seguridad informática. De igual forma se evidencia la importancia de la aplicabilidad de los dominios y controles del estándar ISO/IEC 27001, empleando listas de chequeo que permitan identificar el estado y las acciones que requiere la empresa para alcanzar los niveles de seguridad requeridos. Finalmente se alcanza un cumplimiento por encima del 90% de la mayoría de los dominios y se dan recomendaciones para aquellos que están por debajo de esta referencia, con el fin de alcanzar niveles de cumplimiento de todos los dominios cercanos al 100%.
Recomendaciones	Teniendo en cuenta los resultados obtenidos en la elaboración del proyecto, en cuanto al estado actual de la empresa, se hace necesario actualizar las políticas de seguridad y hacer un seguimiento minucioso, designando tareas o responsabilidades especificas a determinados funcionarios, las cuales deberían estar consignadas dentro de sus funciones, lo cual garantizará a la entidad que siempre se esté al frente y se mantengan actualizadas las políticas y procedimientos de seguridad informática en la entidad.

Fuente: El Autor

10.15 Anexo M: Propuesta de Seguridad para Transmilenio S.A.

Después de hacer el reconocimiento de la empresa, conocer los activos informáticos, hacer el análisis de riesgos y demás procesos, se procedió a hacer un trabajo conjunto con la entidad, para establecer el estado frente al cumplimiento de la estrategia de Gobierno en línea (GEL), con respecto a la seguridad de la información de Transmilenio S.A.

La realización de este trabajo inicia explicando todos los componentes del GEL, la normatividad y los avances que la entidad ha alcanzado frente a los plazos impartidos por el MINTIC.

Componentes Gobierno En Línea (GEL)

Esta nueva Estrategia que se plasma en el Decreto 1078 de 2015, comprende cuatro grandes propósitos[54]:

- ✓ Lograr que los ciudadanos cuenten con servicios en línea de muy alta calidad.
- ✓ Impulsar el empoderamiento y la colaboración de los ciudadanos con el Gobierno.
- ✓ Encontrar diferentes formas para que la gestión en las entidades públicas sea óptima gracias al uso estratégico de la tecnología.
- ✓ Garantizar la seguridad y la privacidad de la información.

Normatividad

La estrategia GEL está soportada bajo un gran paquete normativo, lo que la hace de estricto cumplimiento para las entidades que aplica este programa del MINTIC. A continuación se listan las normas que rigen la estrategia GEL[55]:

[54] Alta Consejería Distrital de TIC. Estrategia GEL Distrito Capital. Disponible en: http://ticbogota.gov.co/estrategia-gel-bogota

LEY 1341 DE 2009

“Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones - TIC”.

LEY 1712 de 2014

“Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional”

LEY 962 de 2005
“Racionalización de trámites y procedimientos administrativos”

DECRETO 1078 de 2015
“Decreto Único Reglamentario del Sector TIC”

DECRETO 235 de 2010
“se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas”

Decreto 1081 de 2015

Resolución 3564 de 2015

Ley estatutaria 1618 de 2013

Ley 1266 de 2008

NTC 5854 de 2012

Decreto 1166 de 2016

Acuerdo 003 de 2015 del AGN

Ley estatutaria 1581 de 2012

---

[55] Alta Consejería Distrital de TIC. Estrategia GEL Distrito Capital. Disponible en: http://ticbogota.gov.co/estrategia-gel-bogota

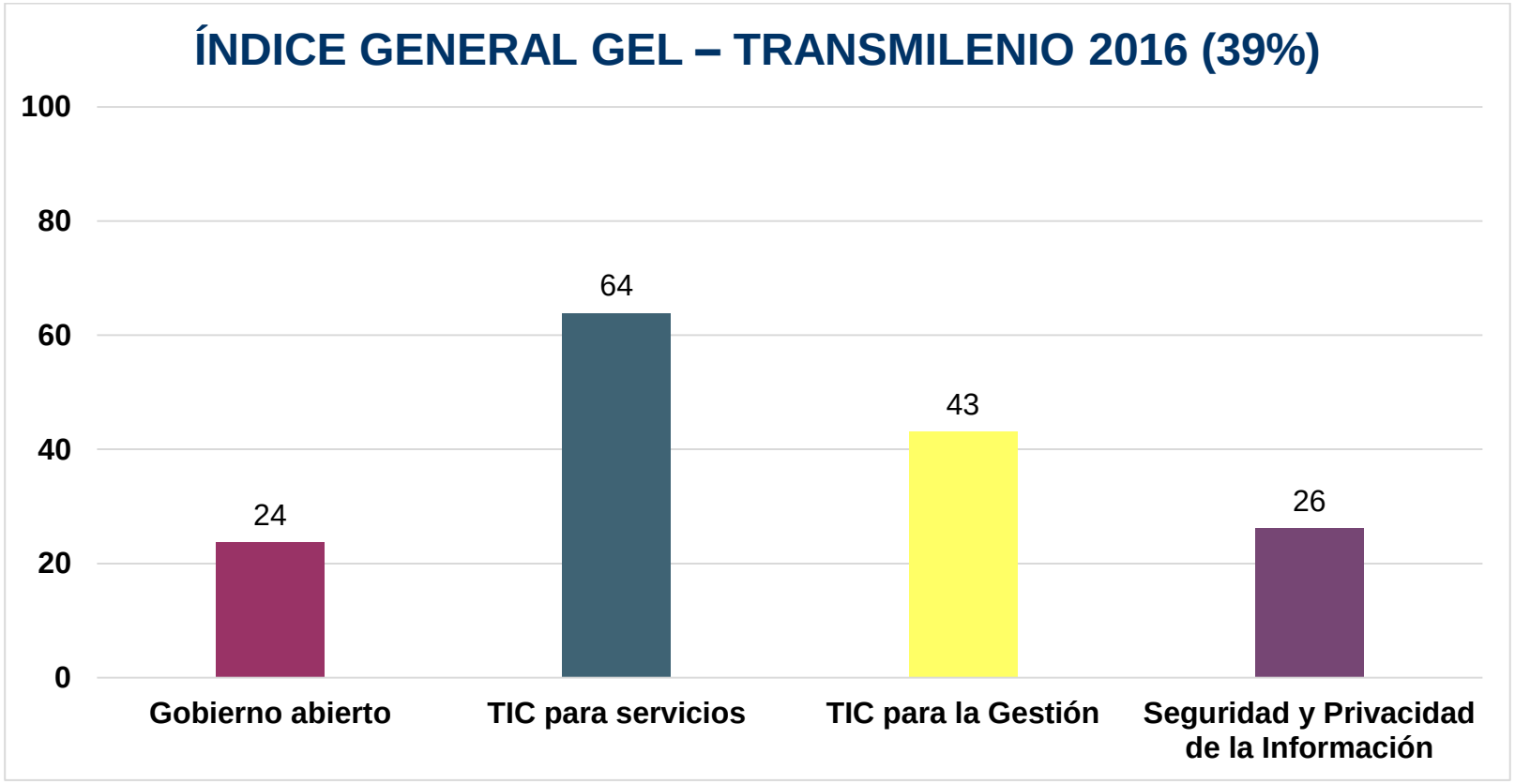
Decreto 1074 de 2015

Manual GEL

Modelo de seguridad y privacidad de la información

Avances de la entidad frente a los plazos impartidos por el MINTIC

Fig. 4. % de cumplimiento Transmilenio a Dic 2016

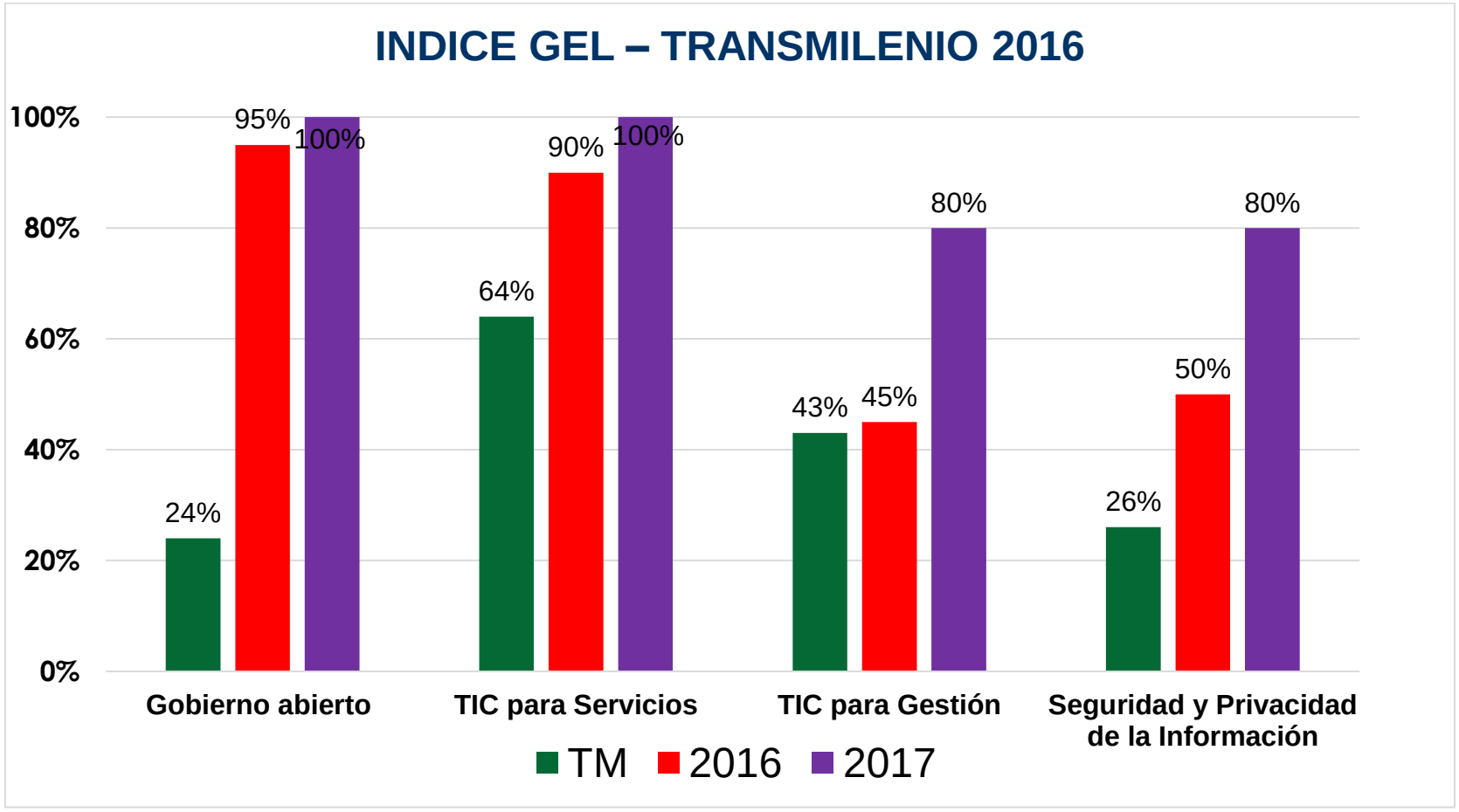


Fuente: Alta Consejería del Distrito TIC. Información año 2016. http://ticbogota.gov.co/estrategia-gel-bogota/

De acuerdo al gráfico anterior, Transmilenio S.A. para el año 2016 obtuvo un avance promedio en la implementación GEL del 39%.

A continuación se comparan los avances alcanzados por Transmilenio para el año 2016 en la estrategia GEL, con respecto a los plazos establecidos por el MINTIC para los años 2016 y 2017:

Fig. 5. Porcentaje de cumplimiento Transmilenio vs lo requerido a Dic 2016

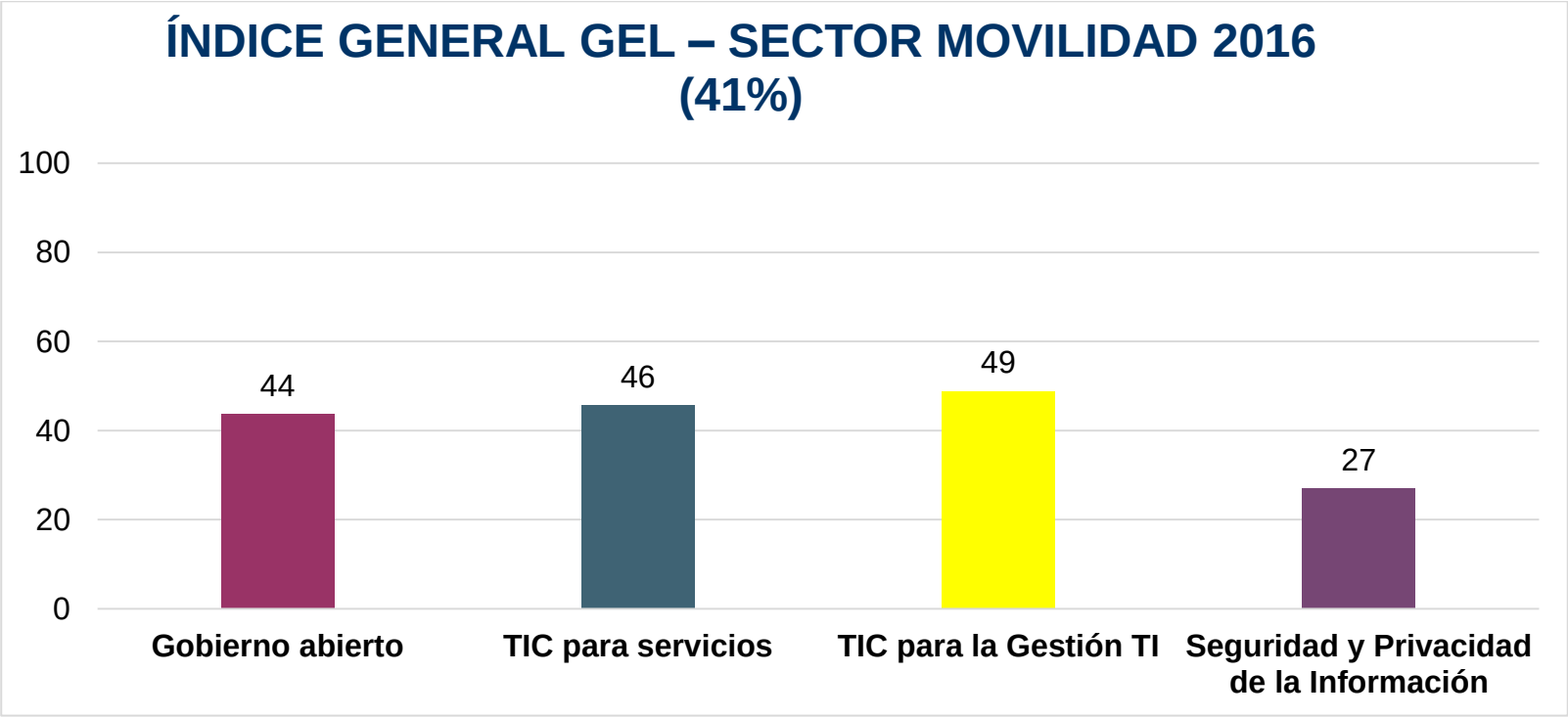


Fuente: Alta Consejería del Distrito TIC. Información año 2016. http://ticbogota.gov.co/estrategia-gel-bogota/

Con base en el gráfico anterior, Transmilenio S.A., presenta un incumplimiento considerable y se hace necesario proceder de inmediato para avanzar en el tema y evitar medidas sancionatorias en la Entidad.

Para tener una visión más clara, se presentan los avances del sector movilidad para el 2016 con respecto a la estrategia GEL.

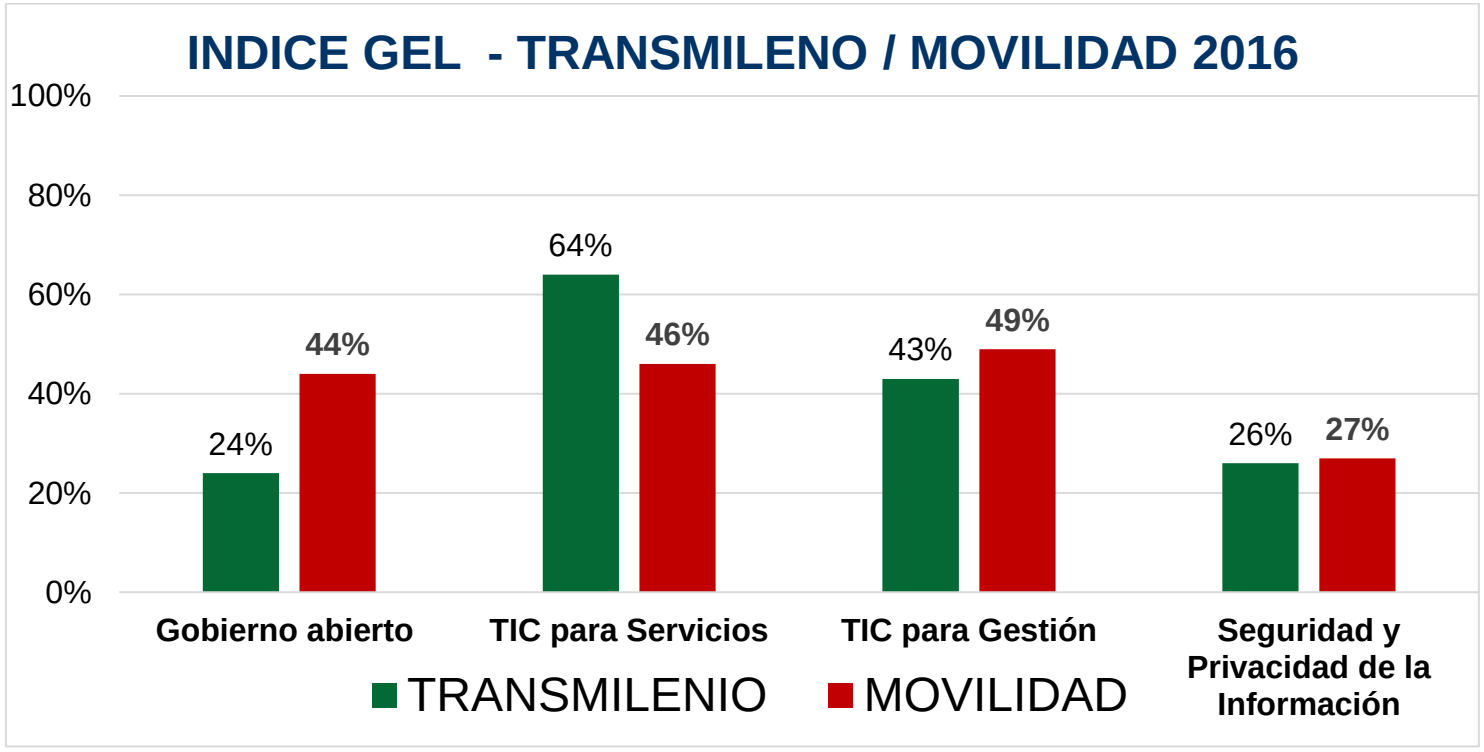
Fig. 6. % de cumplimiento sector Movilidad a Dic 2016



Fuente: Alta Consejería del Distrito TIC. Información año 2016. http://ticbogota.gov.co/estrategia-gel-bogota/

En el siguiente gráfico se hace la comparación de los avances del Transmilenio vs los avances del sector Movilidad en la implementación de la estrategia GEL para el año 2016:

Fig. 7. % de cumplimiento Transmilenio vs sector Movilidad a Dic 2016



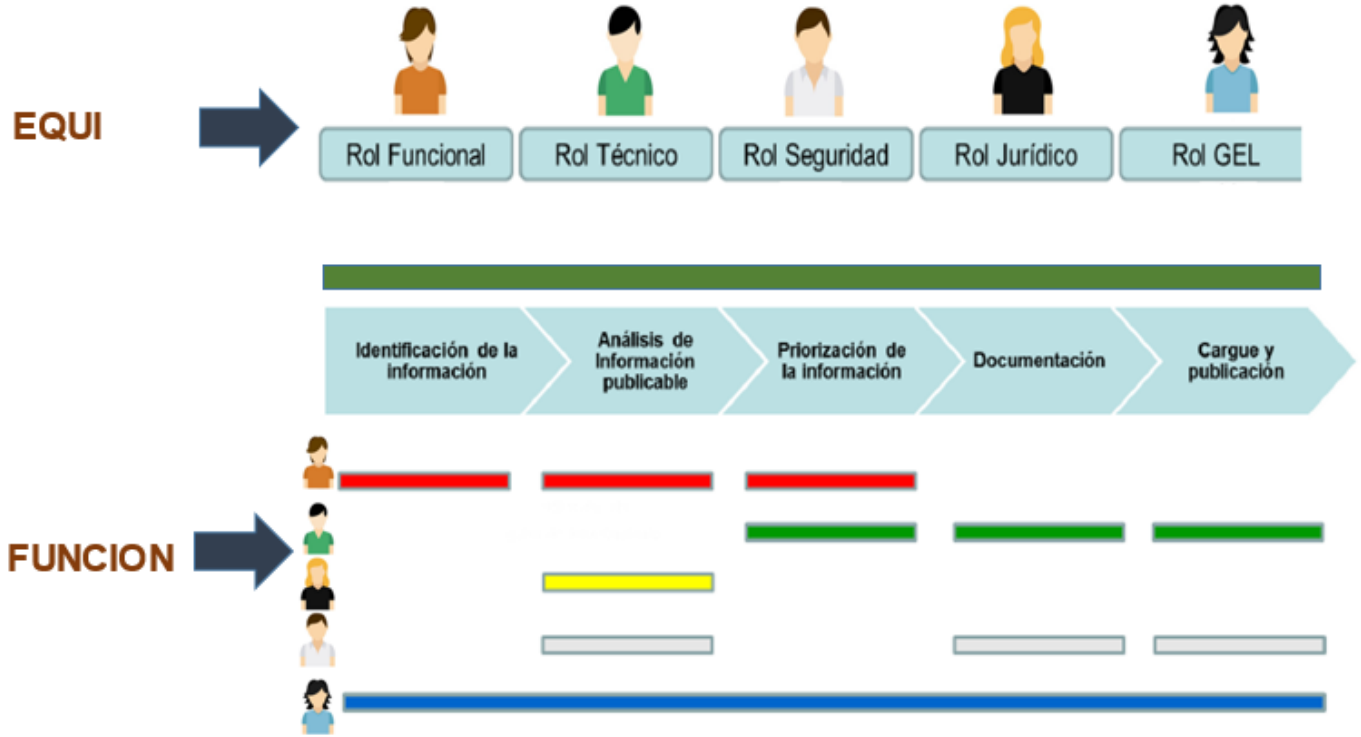
Fuente: Alta Consejería del Distrito TIC. Información año 2016. http://ticbogota.gov.co/estrategia-gel-bogota/

Se evidencia que Transmilenio S.A. para el año 2016 está por debajo del promedio en el cumplimiento del GEL, con respecto al sector Movilidad, esto da una referencia de la importancia de seguir avanzando en la estrategia GEL.

Equipo y plan de trabajo

Para la ejecución del plan GEL en Transmilenio S.A., se requiere involucrar toda la entidad, y cada funcionario debe asumir la responsabilidad que le corresponde desde cada una de las funciones que desempeña.

Fig. 8. Esquema de trabajo TIC para Datos Abiertos



De acuerdo a la estrategia GEL, al sector movilidad le corresponde dar apertura de datos asociados con el parque automotor, seguridad vial, transporte público y malla vial, velocidades promedio, flota geoposicionada, origen – destino, tiempos de desplazamiento, tarifas, estado de la malla vial, licencias, infracciones y accidentalidad, registro de conductores, zonas de parqueo, rutas y horarios de transporte público, sanciones y aseguramiento. El esquema anterior representa las responsabilidades de los funcionarios involucrados para el cumplimiento de este requerimiento.

Dentro del desarrollo de este trabajo se realizó el reconocimiento de la empresa, levantamiento de información de activos informáticos, su identificación, valoración y tratamiento de los mismos, lo cual se tomará como insumo para el cumplimiento del ítem Seguridad y Privacidad de la información. Para lo cual se recomienda tener en cuenta los siguientes informes:

- ✓ Caracterización de las amenazas
- ✓ Valoración del Riesgo
- ✓ Matriz de Riesgos Residuales
- ✓ Evaluación de Dominios
- ✓ Cumplimiento por Control
- ✓ Cumplimiento por Dominio
- ✓ Declaración de Aplicabilidad SOA
- ✓ Plan de Tratamiento de Riesgos PTR

En la tabla 30 se detalla el cronograma de trabajo que debe seguir Transmilenio S.A., con el fin de adelantar los procesos requeridos y ponerse al día frente a lo solicitado por la estrategia GEL, con un plan semanal perfectamente alcanzable por la Entidad, para así cumplir a cabalidad los requisitos del MINTIC.

Tabla 30. Cronograma GEL 2017 – 2018 Transmilenio S.A.

PLAN GENERAL DE TRABAJO PARA LA IMPLEMENTACIÓN DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA EN TRANSMILENIO S.A.																			
ACTIVIDAD	**ENTREGABLE**	**NOV**		**DIC**				**ENE**				**FEB**				**MAR**			
		S3	**S4**	**S1**	**S2**	**S3**	**S3**	**S4**	**S1**	**S2**	**S3**	**S3**	**S4**	**S1**	**S2**	**S3**	**S3**	**S4**	**S1**
1. Generación de herramientas para levantamiento de información y seguimiento de la estrategia GEL																			
2. Revisión de información referente al Plan Estratégico de TI (PETI) actual de Transmilenio S.A.																			
3. Unificación de documentos existentes referentes al PETI para crear la primera versión en la entidad, de acuerdo con el esquema recomendado por el Ministerio de TIC	Primera versión de PETI																		

Tabla 30. (Continuación).

PLAN GENERAL DE TRABAJO PARA LA IMPLEMENTACIÓN DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA																			
ACTIVIDAD	**ENTREGABLE**	**NOV**		**DIC**				**ENE**				**FEB**				**MAR**			
		S3	**S4**	**S1**	**S2**	**S3**	**S3**	**S4**	**S1**	**S2**	**S3**	**S3**	**S4**	**S1**	**S2**	**S3**	**S3**	**S4**	**S1**
4. Identificar el estado en el que se encuentra Transmilenio S.A. en la estrategia de GEL	Matriz de "Metas GEL" con los respectivos soportes																		
5. Identificar y conocer a los respectivos responsables de los temas referentes a la estrategia de GEL en cada una de las áreas de Transmilenio S.A.	Matriz de "Metas GEL" con los respectivos soportes																		
6. Dar a conocer a los directivos de Transmilenio S.A. la importancia de la estrategia de GEL para la organización de la entidad y el beneficio para sus usuarios y grupos de interés.	Lista de asistencia personal de Transmilenio S.A.																		

Tabla 30. (Continuación).

PLAN GENERAL DE TRABAJO PARA LA IMPLEMENTACIÓN DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA																			
ACTIVIDAD	**ENTREGABLE**	**NOV**		**DIC**				**ENE**				**FEB**				**MAR**			
		S3	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**
7. Dar a conocer por medio de presentaciones y/o talleres qué es la estrategia de GEL a todos las áreas de Transmilenio S.A.	Lista de asistencia personal de Transmilenio S.A.																		
8. Identificar las falencias y brechas que hay en Transmilenio S.A. en cuanto a la implementación de la estrategia de GEL.	Matriz de "Metas GEL" con los respectivos soportes																		
9. Presentación y/o taller de datos abiertos a las áreas y terceros que manejan información de Transmilenio S.A.	Lista de asistencia personal de Transmilenio S.A.																		

Tabla 30. (Continuación).

PLAN GENERAL DE TRABAJO PARA LA IMPLEMENTACIÓN DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA																			
ACTIVIDAD	**ENTREGABLE**	**NOV**		**DIC**				**ENE**				**FEB**				**MAR**			
		S3	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**
10. Asignar responsables en cada área de Transmilenio S.A. de los temas respectivos a la estrategia de GEL que les corresponde.	Matriz de "Metas GEL" con responsables de cada tema por área																		
11. Cumplir al 100% con los objetivos de los componentes de TIC para Gobierno abierto y TIC para servicios, de acuerdo con lo estipulado en el Decreto 1078 de 2015 por medio de las herramientas creadas por MINTIC y la ACDTIC, así como lo son formatos, resoluciones y guías.	Matriz de "Metas GEL" con los respectivos soportes																		

Tabla 30. (Continuación).

PLAN GENERAL DE TRABAJO PARA LA IMPLEMENTACIÓN DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA																			
ACTIVIDAD	**ENTREGABLE**	**NOV**		**DIC**				**ENE**				**FEB**				**MAR**			
		S3	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**
12. Avanzar al 60% con los objetivos del componente de Gestión de TI por medio de las guías, lineamientos y recomendaciones publicadas por MINTIC	Matriz de "Metas GEL" con los respectivos soportes																		
13. Identificar el estado y avance del componente de Seguridad y Privacidad de la Información como componente transversal de la estrategia de GEL.	Matriz de "Metas GEL" con los respectivos soportes																		
14. Apoyar al área y/o responsables de Seguridad de la información en el avance del componente de Seguridad y privacidad de la información para lograr llegar al 80% de los objetivos.	Matriz de "Metas GEL" con los respectivos soportes																		

Tabla 30. (Continuación).

PLAN GENERAL DE TRABAJO PARA LA IMPLEMENTACIÓN DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA																			
ACTIVIDAD	**ENTREGABLE**	**NOV**		**DIC**				**ENE**				**FEB**				**MAR**			
		S3	**S4**	**S1**	**S2**	**S3**	**S3**	**S4**	**S1**	**S2**	**S3**	**S3**	**S4**	**S1**	**S2**	**S3**	**S3**	**S4**	**S4**
15. Levantamiento de información para creación de nuevo PETI																			
16. Avanzar al 30% en el PETI 2018	Avance de PETI 2018																		