**N° INFORME:** OCI-2022-044

**PROCESO/SUBPROCESO/ACTIVIDAD:** Gestión de TIC - Seguridad de la información

**EQUIPO AUDITOR:** Diana Elizabeth Patiño Sabogal – Contratista Oficina de Control Interno

**LÍDER DEL PROCESO:** Dirección de TIC

**INFORME DISTRIBUIDO A:** Gerente General e integrantes del Comité Institucional de Coordinación de Control Interno de TRANSMILENIO S. A.

**FECHA REUNIÓN DE APERTURA:** 15 de julio de 2022

**FECHA REUNIÓN DE CIERRE:** 27 de julio de 2022

## OBJETIVO

Evaluar la implementación al sistema de gestión de seguridad de la información (SGSI), considerando las políticas y procedimientos aplicables al proceso.

## ALCANCE

Evaluar la efectividad de los controles establecidos en la ISO 27001:2013 A.5 políticas de seguridad de la información, A.6 Instrumento de identificación de la línea base de seguridad administrativa y técnica y A.7 Seguridad de los recursos humanos para el periodo del 01 de enero de 2021 al 30 de junio de 2022

## LIMITACIONES AL ALCANCE

Para el trabajo desarrollado no se presentaron limitaciones

## DECLARACIÓN

Esta auditoría fue realizada con base en el análisis de diferentes muestras aleatorias seleccionadas por los auditores a cargo del trabajo, una consecuencia de esto es la presencia del riesgo de muestreo, es decir, el riesgo de que la conclusión basada en la muestra analizada

no coincida con la conclusión a que se habría llegado en caso de haber examinado todos los elementos que componen la población.

## CRITERIOS

- Norma técnica NTC-ISO 27001:2013.
- Norma técnica NTC-ISO 27002.
- T-DT-006 Plan estratégico de SI – PESI versión 1.
- M-DT-001 Manual Política De Seguridad y Privacidad De La Información versión 5.
- M-DT-004 Manual del Sistema de Gestión de Seguridad de la Información (SGSI) versión 0.
- Caracterización Proceso Gestión de TIC.
- P-DA-010 Procedimiento para realizar teletrabajo y trabajo en casa en TRANSMILENIO S. A. versión 5.
- P-DT-020 Procedimiento para la Gestión de Incidentes de Seguridad de la Información versión 0.

## RIESGO CUBIERTO

El Plan Estratégico de Seguridad de la Información (PESI) no se pueda implementar de acuerdo a la hoja de ruta establecida.

## FORTALEZA

Se contó con la disposición del personal de planta y contratistas del proceso para atender al equipo auditor en operaciones específicas que contribuyeron a dar claridad en las pruebas efectuadas por la Oficina de Control Interno.

## ESTADO DEL PLAN DE MEJORAMIENTO VIGENTE AL INICIO DE LA AUDITORIA:

Con corte a 30 de junio de 2022 se realizó seguimiento a los Planes de Mejoramiento Interno del Proceso y su estado es: se tenían 14 acciones propuestas de las cuales quedan 11 en ejecución, 3 incumplidas que corresponden a:

1. Revisar y ajustar con asesoría de la Oficina Asesora de Planeación, los controles del mapa de riesgos de Gestión de TIC, teniendo como referente las recomendaciones de la Oficina de Control Interno.

   Fecha de vencimiento: 31 de marzo de 2022

2. Solicitar apoyo de la alta Dirección y o de las Dependencias para motivar la participación del personal en los procesos de sensibilización que adelante la Dirección de TIC.

   Fecha de vencimiento: 31 de marzo de 2022

3. Articular el componente del plan de recuperación de desastres (DRP) y sus actividades asociadas, con la Fase 1 de gestión y definición del Plan de Continuidad del negocio que adelante la Entidad.

   Fecha de vencimiento: 10 de junio de 2022

## RESUMEN EJECUTIVO DE LA AUDITORÍA

A continuación, se relaciona un resumen de los hallazgos/ no conformidades (incumplimiento a requisitos) y observaciones (mejores prácticas) de la auditoría realizada:

## HALLAZGOS

| **Hallazgo** | **Nivel de Severidad** | **Probabilidad** | **Impacto** |
|---|---|---|---|
| Mecanismos de manejos de desviaciones y excepciones sin documentar. | **Bajo** | **1** | **2** |

## DESARROLLO DE LA AUDITORÍA

Durante la auditoría realizada al proceso de Gestión de TIC, teniendo en cuenta el objetivo y alcance, se desarrollaron los siguientes pasos:

a) **Entendimiento del proceso**: Se realizaron consultas basadas en la documentación existente del proceso (manuales, guías, procedimientos, instructivos, mapas de riesgos), así como la búsqueda de distintos controles que apliquen las áreas para la gestión de riesgos.

b) **Revisión de la normativa vigente aplicable**: Se verificó la normativa aplicable para constatar su cumplimiento.

c) **Identificación de riesgos y controles**: Fueron identificados los riesgos claves que pudieran afectar el proceso, así como la existencia de controles que mitiguen su materialización.

d) **Elaboración y ejecución del plan de trabajo**: Con base en el entendimiento adquirido del proceso el cual, durante su desarrollo permitió determinar la existencia, funcionalidad y aplicación de controles y requisitos identificados.

e) **Identificación de hallazgos/no conformidades y observaciones:** Como resultado de comparación entre el criterio (el estado correcto del requisito) y la condición (es decir es estado actual), durante el ejercicio auditor se encontraron diferencias entre ambos lo cual, se convirtió en insumo para la elaboración del informe.

**Breve descripción de las pruebas de auditoría realizadas:**

Teniendo en cuenta el alcance establecido para el desarrollo de esta auditoría se definieron 3 pruebas asociadas a los dominios: políticas de seguridad de la información; responsabilidades y organización de la seguridad de la información y, seguridad de los recursos humanos.

De acuerdo con lo anterior, cada actividad fue desarrollada de la siguiente manera:

- **Políticas de seguridad de la información.**

Inicialmente, se realizó una verificación documental de los manuales y procedimientos establecidos por el proceso gestión de TIC y se identificó que este cuenta con el Manual de

Seguridad de la Información, Manual del SGSI y el Plan Estratégico PESI, los cuales fueron adoptados mediante la Resolución 335 del 22 de junio de 2022 y se encuentran publicados en el MIPG para ser consultados y validados por todos los funcionarios públicos, contratistas y terceras partes. Dando cumplimiento a lo establecido en la Norma técnica NTC-ISO 27001:2013

A pesar de que, las desviaciones y excepciones permitidas al interior de la entidad se encuentran documentadas en diferentes procedimientos, estas no están consolidadas en un solo índice que permita identificarlas y conocer el proceso que se debe adelantar para su solicitud. Lo que genera posibles incumplimientos por parte de los funcionarios a las políticas de seguridad de la información establecidas por la entidad.

De acuerdo con lo anterior, se presenta el hallazgo 1.

- **Responsabilidades y organización de la seguridad de la información**

Para la realización de esta prueba se validó dentro de la documentación registrada por el proceso de gestión de TIC la definición de los roles y responsabilidades de los profesionales encargados de la planeación, implementación y seguimiento al Manual del Sistema de Gestión de Seguridad de la Información (SGSI), así como, la definición de las responsabilidades que tienen los propietarios de los activos de información.

Por otra parte, se tienen implementados los procedimientos para la gestión de incidentes de seguridad de la información, teletrabajo y trabajo en casa. El Manual de Política y Privacidad de la información de Transmilenio S.A. permite revisar y valorar el cumplimiento de lo allí establecido.

- **Seguridad de los Recursos Humanos de la Seguridad de la Información**

En el desarrollo de esta prueba se identificó que la Dirección de TIC cuenta con el apoyo de un funcionario de planta y tres contratistas para la implementación de la política de seguridad de la información. Los contratistas son profesionales, con título de formación profesional en ingeniería de sistemas, ingeniería electrónica e ingeniería de telecomunicaciones. Sin embargo, al validar el Plan Institucional de Formación y Capacitación 2022, no se observaron capacitaciones asociadas a la seguridad de la información.

En cuanto al procedimiento disciplinario que se debe implementar una vez se identifique una violación a la seguridad de la información, la Dirección de TIC mediante el procedimiento P-DT-020 «Procedimiento para la Gestión de Incidentes de Seguridad de la Información» V.0 en el numeral 7.10 «Medidas disciplinarias» informa a la oficina de Control Disciplinario las regularidades que llegase a presentar. Dando cumplimiento a lo establecido en la Norma técnica NTC-ISO 27001:2013.

**HALLAZGO No. 1**

Mecanismos de manejos de desviaciones y excepciones sin documentar.

**Descripción del hallazgo o situación encontrada:**

Al verificar la documentación registrada por la Dirección de TIC, se observó que, a pesar de tener documentado en algunos procesos las actividades que se deben desarrollar en caso de presentarse alguna desviación o excepción, no se tiene definido un mecanismo que permita reportar los incidentes de seguridad de la información, el profesional al que debe ser dirigido y si es necesario incluir un formato de autorización para el respectivo monitoreo y seguimiento continuo.

Lo anterior permite identificar un incumplimiento a lo establecido en la norma ISO 27011:2013 control: A.12.1.2 «Procedimientos de operación documentados», generando posibles investigaciones por el uso indebido de los sistemas de información.

**Posibles causas identificadas por la Oficina de Control Interno:**

Desconocimiento de la normativa en la implementación de los controles establecidos.

**Descripción del riesgo:**

Que el Plan Estratégico de Seguridad de la Información (PESI) no se pueda implementar de acuerdo a la hoja de ruta establecida.

Impacto: Menor

Probabilidad: Muy baja

Nivel de severidad: De acuerdo con la calificación de la probabilidad y el impacto, el nivel de severidad es bajo.

Recomendaciones:

1. Implementar un mecanismo donde se documenten las deviaciones que son presentadas al interior de la entidad.
2. Establecer un seguimiento a las desviaciones identificadas e implementar planes de acción por autocontrol en caso de ser necesarios.

**Posible causa identificada por el responsable del proceso auditado:**

La Dirección de TIC se encuentra realizando la formulación del respectivo plan de mejoramiento, en el cual se incluye un análisis de las posibles causas que originaron el hallazgo.

**CONCLUSIONES Y RECOMENDACIONES GENERALES**

1. Implementar proceso o procedimiento donde se documenten las deviaciones que son presentadas al interior de la entidad.
2. Solicitar la publicación del documento al MIPG
3. Socializar el procedimiento al interior de la entidad.
4. Reforzar los riesgos asociados a temas que podrían afectar la integridad, confidencialidad y disponibilidades de la información como:
    a. Los privilegios de acceso excesivo o inutilizado.
    b. Manejo ilegal de los datos realizados por personal no autorizado o sin conocimiento.
    c. La falta o desactualización del software de ciberseguridad, así como también vulnerabilidades en los aplicativos web.
5. Solicitar a la alta dirección incluir dentro del Plan Institucional de Formación y Capacitación temas relacionados con la seguridad de la información, esto con el fin de afianzar los conocimientos de los funcionarios cuyas obligaciones están enfocadas en el cumplimiento y las mejoras de dicha política.

6. Reforzar el plan de sensibilización a todos los servidores públicos, contratistas, proveedores y terceras partes, de acuerdo con las necesidades identificadas por la Dirección de TIC respecto a la seguridad de la información.

Bogotá D. C., 27 de julio de 2022

**Sandra Jeannette Camargo Acosta**

Jefe Oficina de Control Interno

Elaboró: Diana Elizabeth Patiño Sabogal, Contratista - Oficina de Control Interno.

Revisó: Luz Nelly Castañeda, Contratista - Oficina de Control Interno.