N° INFORME: OCI-2018-022

PROCESO / ACTIVIDAD REALIZADA: GESTIÓN DE LAS TIC´s

EQUIPO AUDITOR: LUZ MARLENNY CANO ROMERO

OBJETIVO(S):

Efecutar el diagnóstico y seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO27001:2013 en TRASNMILENIO S.A.

ALCANCE:

Determinación del nivel de madurez en el proceso de implementación del SGSI, a cargo de la Dirección de TIC´s de TRANSMILENIO S.A., en cumplimiento del plan anual de actividades 2018 de la Oficina de Control Interno y de acuerdo con lo establecido por la Ley 87 de 1993, artículo 17 del Decreto 648 de 2017y NTD-SIG-001-2011, dicho proceso contempla la validación de los controles para los 14 dominios de la norma ISO/IEC 27001:2013 a fin de evidenciar su aplicabilidad al interior de la Entidad.

La actividad se llevó a cabo en conjunto con los profesionales designados por la Dirección de TIC´s de TRANSMILENIO S.A.

CRITERIOS:

1. Norma NTC-ISO-IEC 27001:2013 Anexo A.
2. Guía Técnica Colombiana GTC-ISO-IEC 270012.
3. Ley 1581 de 2012. Ley de protección de datos personales
4. Ley 1273 “De la Protección de la información y de los datos
5. Decreto 1078 de 2015. “Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”
6. Ley 87 de 1993, artículo 17 del Decreto 648 de 2017
7. Norma Técnica Distrital del Sistema Integrado de Gestión para las Entidades y Organismos Distritales NTD-SIG-001:2011
8. Directiva 011 de 2012
9. La demás normatividad interna y/o externa asociada con el proceso auditado
10. Decreto 2693 de 2012
11. Resolución 305 de 2015
12. Resolución 454 de 2017

DESCRIPCIÓN DEL TRABAJO REALIZADO, CONCLUSIONES Y RECOMENDACIONES

Estado actual con respecto a la ISO/IEC 27001:2013

Se realizó un análisis permitiendo evaluar el estado de contexto de la organización, liderazgo, planificación, soporte, operación, evaluación de desempeño y mejoras, los

cuales se convierten en elementos esenciales en el proceso de mejoramiento continuo, para la Entidad desde la pertinencia del subsistema de gestión de seguridad de la información.

Lo anterior mediante la aplicación de cumplimiento del anexo A de la norma ISO 27001:2013 verificando los Objetivos de Control y controles de referencia, a la Dirección de las TIC's, realizada junto con el PROFESIONAL ESPECIALIZADO GRADO 06 SEGURIDAD DE LA INFORMACIÓN y Contratista de seguridad de la información.

Las respuestas posibles están dadas por: NC, CP, CS, NA. De acuerdo con la información que se presenta en la siguiente tabla:

Sigla	Estadode Evaluación	Descripción
NC	NO CUMPLE	No existe y/o no se está haciendo
CP	CUMPLE PARCIALMENTE	Lo que la norma requiere (ISO/IEC 27001 versión 2013) se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió y aprobó pero no se gestiona
CS	CUMPLE SATISFACTORIAMENTE	Existe, es gestionado, se está cumpliendo con lo que la norma ISO/IEC 27001 versión 2013 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI cumple 100%
NA	NO APLICA	No se aplica en la Entidad

Anexo A "**Encuesta aplicada"**

Dominio y Controles Referencia	Objetivos de Control	CS	CP	NC	NA
NA.5	**POLITICA DE LA SEGUIRDAD DE LA INFORMACION**				
A.5.1	Orientación de la dirección para la gestión de la seguridad de la información				
A.5.1.1	Política para la Seguridad de la Información	✔			
A.5.1.2	Revisión de políticas para la seguridad de la Información		✔		
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**				
A.6.1	**Organización Interna**				
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		✔		

Dominio y Controles Referencia	Objetivos de Control	CS	CP	NC	NA
A.6.1.4	Contacto con los grupos de Interés especial		✔		
A.6.1.5	Seguridad de la información en la gestión de proyectos			✔	
A.6.2	**Dispositivos móviles y de teletrabajo**				
A.6.2.1	Políticas para dispositivos móviles		✔		
A.6.2.2	Teletrabajo	✔			
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**				
A.7.1	**Antes de asumir el empleo**				
A.7.1.1	Selección		✔		
A.7.1.2	Términos y condiciones del empleo		✔		
A.7.2	**Durante la ejecución del empleo**				
A.7.2.1	Responsabilidades de la dirección			✔	
A.7.2.2	Toma de conciencia educación y formación de la seguridad de la información		✔		
A.7.2.3	Proceso disciplinario			✔	
A.7.3	Terminación y cambio de empleo				
A.7.3.1	Terminación o cambio de responsabilidades de empleo		✔		
A.8	**GESTION DE ACTIVOS**				
A.8.1	**Responsabilidades de los activos**				
A.8.1.1	Inventario de Activos		✔		
A.8.1.2	Propiedad de los Activos		✔		
A.8.1.3	Uso aceptable de los activos		✔		
A.8.1.4	Devolución de Activos		✔		
A.8.2	**Clasificación de la información**				
A.8.2.1	Clasificación de la información			✔	
A.8.2.2	Etiquetado de la información			✔	
A.8.2.3	Manejo de activos		✔		
A.8.3	**Manejo de medios**				
A.8.3.1	Gestión de medios removibles		✔		
A.8.3.2	Disposición de los medios		✔		
A.8.3.3	Transferencia de medios físicos	✔			
A.9	**CONTROL DE ACCESO**				
A.9.1	**Requisitos del negocio para el control de acceso**				
A.9.1.1	Política de control de acceso	✔			
A.9.1.2	Acceso a redes y a servicios en red	✔			
A.9.2	**Gestión de acceso a Usuarios**				
A.9.2.1	Registro y cancelación del registro de usuarios		✔		
A.9.2.2	Suministro de acceso de usuarios	✔			
A.9.2.3	Gestión de derechos de acceso privilegiado		✔		
A.9.2.4	Gestión de información de autenticación secreta de usuarios	✔			

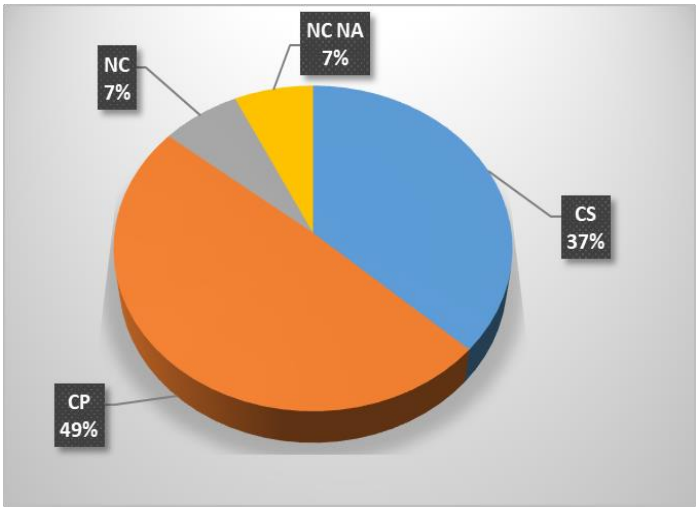
Dominio y Controles Referencia	Objetivos de Control	CS	CP	NC	NA
A.9.2.5	Revisión de los derechos de acceso de usuarios	✔			
A.9.2.6	Retiro a ajuste de los derechos de acceso		✔		
A.9.3	**Responsabilidades de los usuarios**				
A.9.3.1	Uso de Información de autenticación secreta	✔			
A.9.4	**Control de Acceso a sistemas y aplicaciones**				
A.9.4.1	Restricción de acceso a la información	✔			
A.9.4.2	Procedimiento de Ingreso seguro	✔			
A.9.4.3	Sistema de gestión de contraseñas	✔			
A.9.4.4	Uso de programas utilitarios privilegiados		✔		
A.9.4.5	Control de acceso a códigos fuentes de programas	✔			
A.10	**CRIPTOGRAFIA**				
A.10.1	**Controles Criptográficos**				
A.10.1.1	Política sobre el uso de los controles criptográficos	✔			
A.10.1.2	Gestión de llaves		✔		
A.11	**SEGURIDAD FISICA Y DEL ENTORNO**				
A.11.1	Áreas seguras				
A.11.1.1	Perímetro de seguridad física	✔			
A.11.1.2	Controles de acceso físicos	✔			
A.11.1.3	Seguridad de oficinas recintos e instalaciones	✔			
A.11.1.4	Protección contra amenazas externas y ambientales	✔			
A.11.1.5	Trabajo en las áreas seguras	✔			
A.11.1.6	Áreas de despacho y carga				✔
A.11.2	**Equipos**				
A.11.2.1	Ubicación y protección de equipos	✔			
A.11.2.2	Servicios de suministro	✔			
A.11.2.3	Seguridad del cableado		✔		
A.11.2.4	Mantenimiento de equipos	✔			
A.11.2.5	Retiro de activos		✔		
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones			✔	
A.11.2.7	Disposición seguro reutilización de equipos		✔		
A.11.2.8	Equipos de usuario desatentado		✔		
A.11.2.9	Política de escritorio limpio y pantalla limpia		✔		
A.12	**SEGURIDAD DE LAS OPERACIONES**				
A.12.1	Procedimientos operaciones y responsabilidades				
A.12.1.1	Procedimientos de operación documentados		✔		
A.12.1.2	Gestión de cambios			✔	
A.12.1.3	Gestión de la capacidad		✔		
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación		✔		

Dominio y Controles Referencia	Objetivos de Control	CS	CP	NC	NA
A.12.2	**Protección contra código maliciosos**				
A.12.2.1	controles contra códigos maliciosos		✔		
A.12.3	**copias de Respaldo**				
A.12.3.1	Respaldo de información	✔			
A.12.4	**Registro y seguimiento**				
A.12.4.1	Registro de eventos		✔		
A.12.4.2	Protección de la información de registro		✔		
A.12.4.3	Registros del administrador y del operador	✔			
A.12.4.4	Sincronización de relojes	✔			
A.12.5	**Control de software operacional**				
A.12.5.1	Instalación de software en sistemas operativos	✔			
A.12.6	**Gestión de la vulnerabilidad técnica**				
A.12.6.1	Gestión de las vulnerabilidades técnicas	✔			
A.12.6.2	Restricciones sobre la Instalación de software		✔		
A.12.7	**Consideraciones sobre auditorias de sistemas de información**				
A.12.7.1	controles de auditorías de sistemas de información	✔			
A.13	**SEGURIDAD DE LAS COMUNICACIONES**				
A.13.1	**Gestión de la seguridad de las redes**				
A.13.1.1	Controles de redes	✔			
A.13.1.2	Seguridad de los servicios de red	✔			
A.13.1.3	Separación en las redes	✔			
A.13.2	**Transferencia de la información**				
A.13.2.1	Políticas y procedimientos de transferencia de información	✔			
A.13.2.2	Acuerdos sobre transferencia de información		✔		
A.13.2.3	Mensajería electrónica	✔			
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	✔			
A.14	**Adquisición, desarrollo y mantenimiento de sistemas**				
A.14.1	**Requisitos de seguridad de los sistemas de información**				
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	✔			
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	✔			
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	✔			
A.14.2	**Seguridad en los procesos de desarrollo y soporte**				
A.14.2.1	Política de desarrollo seguro				✔
A.14.2.2	Procedimiento de control de cambio de Sistemas		✔		

Dominio y Controles Referencia	Objetivos de Control	CS	CP	NC	NA
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de la operación		✔		
A.14.2.4	Restricciones en los cambios a los paquetes de software	✔			
A.14.2.5	principios de construcción de los sistemas seguros				✔
A.14.2.6	Ambiente de desarrollo seguro				✔
A.14.2.7	Desarrollo contratado externamente		✔		
A.14.2.8	Pruebas de seguridad de sistemas				✔
A.14.2.9	Pruebas de aceptación de sistemas				✔
A.14.3	Datos de Prueba				
A.14.3.1	Protección de datos de prueba				✔
A.15	**RELACIONES CON LOS PROVEEDORES**				
A.15.1	**Seguridad de la información en las relaciones con los proveedores**				
A.15.1.1	Políticas de seguridad de la información para las relaciones con los proveedores		✔		
A.15.1.2	Tratamiento dela seguridad dentro de los acuerdos con proveedores		✔		
A.15.1.3	Cadena de suministro de tecnología de información y comunicación		✔		
A.15.2	**Gestión de la prestación de servicios de proveedores**				
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores		✔		
A.15.2.2	Gestión de cambios en los servicios de los proveedores		✔		
A.16	**Gestión de Incidentes**				
A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**				
A.16.1.1	Responsabilidades y procedimientos		✔		
A.16.1.2	Reporte de eventos de seguridad de la información		✔		
A.16.1.3	Reporte de debilidades de seguridad de la información		✔		
A.16.1.4	Evaluación de los eventos de seguridad de la información y decisiones sobre ellos		✔		
A.16.1.5	Respuesta a incidentes de seguridad de la información		✔		
A.16.1.6	Aprendizaje obtenido de los incidentes de SI		✔		
A.16.1.7	Recolección de evidencia		✔		
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DEL NEGOCIO**				

Dominio y Controles Referencia	Objetivos de Control	CS	CP	NC	NA
A.17.1	continuidad de seguridad de la información				
A.17.1.1	Planificación de la continuidad de la SI		✔		
A.17.1.2	Implementación de la continuidad de la SI		✔		
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la SI			✔	
A.17.2	Redundancias	✔			
A.17.2.1	Disponibilidad de las Instalaciones de procesamiento de la información	✔			
A.18	**CUMPLIMIENTO**				
A.18.1	Cumplimiento de los requisitos legales y contractuales				
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	✔			
A.18.1.2	Derechos de propiedad intelectual		✔		
A.18.1.3	Protección de registros		✔		
A.18.1.4	Privacidad y protección de información de datos personales	✔			
A.18.1.5	Reglamentación de controles criptográficos				✔
A.18.2	Revisiones de seguridad de la información				
A.18.2.1	Revisiones independientes de la seguridad de la información		✔		
A.18.2.2	cumplimiento de las políticas y normas de seguridad		✔		
A.18.2.3	Revisión del cumplimento técnico		✔		

Tras el análisis se obtienen los siguientes resultados:



ID	Dominio	CS	CP	NC	NA
A5	Política de seguridad	1	1		
A6	Organización de la SI	3	3	1	
A7	Seguridad de los RRHH		4	2	
A8	Gestión de activos	1	7	2	
A9	Control de accesos	10	4		
A10	Criptografía	1	1		
A11	Seguridad física y del entorno	8	5	1	1
A12	Seguridad en las operaciones	6	7	1	
A13	Seguridad en las comunicaciones	6	1		
A14	Adquisición de sistemas, desarrollo y mantenimiento	4	3		6
A15	Relación con proveedores		5		
A16	Gestión de los incidentes de seguridad		7		
A17	Continuidad del negocio	2	4	1	1
A18	Cumplimiento con requerimientos legales y contractuales		3		
	Suma total	**42**	**56**	**8**	**8**

Como resultado de la encuesta realizada al anexo A de la norma ISO 27001:2013 a los 14 dominios y 114 controles, se describe dominio a dominio el estado de madurez obtenido por medio de las evidencias presentadas en el momento de la verificación con el PROFESIONAL ESPECIALIZADO GRADO 06 SEGURIDAD DE INFORMACIÓN

A.5 Política de Seguridad

Se evidencia la definición de un conjunto de políticas de seguridad de la información plasmadas en el Manual de políticas de seguridad de la Información M-DT-001 versión 1 Julio 2017, no obstante no se evidencian procesos continuos de sensibilización y apropiación de las mismas al interior de la Entidad. De igual manera no se evidencian planes de acción efectivos que apoyen desde la Alta Dirección el Sistema de Gestión de Seguridad de la Información -SGSI en lo referente a la difusión de las políticas, soportados en los resultados de las revisiones por la dirección.

A.6 Organización de la seguridad de la información.

La entidad cuenta con políticas para teletrabajo reglamentada a través de la resolución 420 de 2016 al interior de la Entidad, con medidas aplicadas en cuanto a seguridad física, autorización del jefe o encargado del área que postula al candidato de teletrabajo, protocolo de soporte y mantenimiento de hardware y software, mecanismos de seguridad en

comunicaciones, para el acceso remoto a los sistemas de TRANSMILENIO S.A., protección antivirus y requerimientos de firewall., Conexiones vía VPN a los sistemas de información de TRANSMILENIO S.A así mismo con el procedimiento P-DA-010-TMSA

Se observa que la entidad ha avanzado en la tarea de asignación de responsabilidades de seguridad de la información, como es el caso, en la definición del cargo del profesional especializado grado 06 de Sistema de Información de la Dirección de TIC's.

Sin embargo no se evidencia la identificación de responsabilidades para la protección de activos individuales y realización de procesos de seguridad de la información específica, algunas responsabilidades de Sistema de Información se plasman de manera muy básica en los perfiles específicos de funcionarios contenidos en el manual de funciones de la entidad.

A.7 Seguridad de los RRHH.

Debido a que existe una definición parcial de responsabilidades y roles de seguridad, como se mencionó en el anterior dominio, la aplicación de la seguridad de la información de acuerdo a las políticas establecidas por la Entidad, también se lleva a cabo de forma parcial sobre empleados y contratistas. Se evidencia la inexistencia de requisitos exigibles de seguridad de la información en contratos laborales de fecha 2018 y escenarios de ingreso de nuevos funcionarios.

Dichas exigencias se deben plasmar en los términos y condiciones del empleado durante y a la terminación de su relación laboral con la Entidad en concordancia con lo establecido en la ISO/IEC 27001:2013.

A.8 Gestión de activos.

El objetivo propuesto dentro del manual de Políticas de Seguridad establecido en la Entidad es Lograr y mantener la protección adecuada de los activos de información mediante la asignación de éstos a los usuarios finales, que deban administrarlos de acuerdo a sus roles y funciones

Sin embargo se evidenció que en la Entidad se cuenta con un inventario de activos de información desactualizado inconsistente y no alineado con los otros inventarios, razón por la cual existe incumplimiento frente al Manual de políticas de Seguridad de la información, establecida en la Entidad

No se evidencia procedimiento o proceso alguno tendiente a la clasificación y etiquetado de los activos de información.

Al existir, como ya se mencionó, una definición parcial de responsabilidades en cuanto a seguridad de la información, se presentan falencias en la concepción del término y la función de propiedad de los activos en lo que a los usuarios se refiere, razón por la cual algunos de los controles implementados no son efectivos, tal es el caso de la devolución de activos. (Formato de devolución de activos vigente en la entidad no contempla la revisión del área de tecnología)

A.9 Control de accesos.

Es de gran importancia limitar el acceso a información y a instalaciones de procesamiento de información, asegurando el acceso de los usuarios autorizados y evitando el acceso no autorizado a sistemas y servicios. Se observa que en la Entidad se hace uso de contraseñas como medida para restringir el acceso a sus sistemas y se tiene conocimiento de la necesidad de desarrollar políticas de control de accesos, gestión de contraseñas y gestionar correctamente escenarios como el teletrabajo, por lo cual han tomado medidas basadas en las buenas prácticas. Sin embargo, existe documentación parcial y se encuentran en construcción nuevos documentos, relacionados con los controles de acceso. Hay políticas de control de acceso para el ingreso al centro de cómputo, sin embargo durante la visita realizada no se evidenció la aplicación de los controles de entrada como lo especifica el Manual de políticas de seguridad de la información de la Entidad, Numeral 8.9.1

Es necesario aclarar que la responsabilidad en la gestión de accesos es compartida entre la dirección de TIC´s y la Dirección Corporativa, ya que esta última tiene a su cargo la gestión y monitoreo de los dispositivos de acceso físico, política que no se pudo evidenciar.

A.10 Criptografía

Con la criptografía se busca asegurar el uso apropiado y eficaz de ésta, para proteger entre otras la confidencialidad, integridad y no repudiación de la información. Se evidencia la mención de forma general a las políticas de controles criptográficos en el Manual de políticas de Seguridad de la Información, pero no existen procedimientos escritos sobre el uso protección y tiempo de vida de las llaves criptográficas.

Se evidencia el uso de controles criptográficos por ejemplo en el uso de conexiones VPN a través de los firewalls de la Entidad, sin embargo, como ya se mencionó no se han determinado de forma oficial criterios para establecer tiempos de vida o políticas de gestión de las llaves criptográficas.

A.11 Seguridad física y del entorno.

Se observa que la entidad ha tomado medidas para controlar el acceso físico no autorizado, el daño y la interferencia a la información. (Control de incendios, control ambiental, UPS, plantas eléctricas…)

Se hace énfasis en que la responsabilidad de gestión del acceso físico a recintos e instalaciones se encuentra compartida entre la dirección de TIC´s y la Dirección Corporativa, razón por la cual no se evidencia la implementación de un procedimiento general conjunto, puesto que a pesar de que existe, no incluye todos los aspectos de la operación.

A.12 Seguridad en las operaciones.

Con la seguridad en las operaciones se busca obtener operaciones correctas y seguras de las instalaciones de procesamiento de información. Aquí, se incluyen controles contra

códigos maliciosos, respaldo de la información, separación de los ambientes de desarrollo, pruebas y operación, registro de eventos.

Se evidencia que la Entidad ha gestionado a través de la implementación de controles efectivos la seguridad en las operaciones. Se hace necesario sin embargo continuar con el proceso de documentar y actualizar los procedimientos que permitan evidenciar al proceso de mejoramiento continuo con énfasis en los siguientes aspectos:

- Implementación para la detección y seguimiento a fallos.
- Control parcial de cambios en los sistemas de procesamiento de información.

La entidad, mediante la herramienta TIVOLI que realiza los Backus de la información, estas copias se almacenan en la cintoteca de la Entidad, sin embargo no se evidencia que se envíen a custodio externo como se menciona en el manual de Seguridad de la Información numeral en lo referente a almacenamiento de Backup.

A.13 Seguridad en las Comunicaciones.

El objetivo de la Entidad de asegurar la protección de la información en las redes y la transferencia de información, se ha enfocado en la implementación de controles para proteger la confidencialidad, integridad y disponibilidad de la información publicada y transferida en los escenarios LAN y WAN de la Entidad. Se hace necesario ajustar y actualizar los procedimientos publicados con respecto a los acuerdos sobre transferencia segura de información para asegurar criterios de trazabilidad y no repudio.

A.14 Adquisición de sistemas, desarrollo y mantenimiento.

La entidad tiene desarrollos tercerizados con el proveedor *BISA CORPOTAION S.A.S* con el objeto de Bodega de Datos para los indicadores de recaudo, un ingeniero de soporte para el software ERP y una contratación masiva de siete (7) ingenieros desarrolladores en la Dirección de TIC´s para el inicio de un proyecto cuyo producto es el desarrollo de sistemas de información.

Existen procedimientos que establecen directrices sobre actividades relacionadas con la adquisición de sistemas, desarrollo y mantenimiento basados en las mejores prácticas para el caso específico de TRANSMILENIO S.A., el estándar ISO/IEC 27001:2013. Sin embargo se evidenció durante el proceso de entrevistas que no hay un criterio de riesgo en la implementación de controles para los proyectos (desarrollo de Software) y por ende en las labores de seguimiento al mencionado proyecto, puesto que no existen procedimientos documentados ni la información pertinente disponible que permitan el adecuado seguimiento en el contexto del sistema integrado de seguridad de la Información.

Durante la ejecución de la entrevista se evidenció, que se desconoce si se llevan técnicas de programación segura tanto para los nuevos desarrollos, como para escenarios de reúso de códigos

A.15 Relación con proveedores.

En la Entidad la relación con los proveedores se establece contractualmente. Dichos contratos incluyen acuerdos de confidencialidad.

Sin embargo dichos acuerdos contemplan requisitos muy básicos de seguridad de la información, como acuerdos de confidencialidad y la no autorización de divulgación confidencial, situación que genera un criterio de riesgo en el establecimiento de las relaciones con proveedores que puedan tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI y que se pudiesen materializar en escenarios de incumplimiento ante la inexistencia de controles efectivos.

A.16 Gestión de los incidentes de seguridad.

La Gestión de Incidentes propende por asegurar un enfoque coherente y eficaz para el manejo de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

Se evidencia que al interior de TRANSMILENIO S.A., existen canales formales de comunicación (mesa de ayuda) para que se informe acerca de eventos e incidentes de seguridad al grupo de trabajo (soporte) con el fin de generar los correspondientes planes de acción.

Existen sin embargo debilidades en cuanto a la apropiación por parte de los usuarios finales de la cultura de reportar incidentes de seguridad, lo que a su vez determina que la base de conocimiento no crezca en el espectro de casos que permita disminuir tiempos de respuesta y generación de planes de acción efectivos.

A.17 Continuidad del negocio.

TRANSMILENO S.A debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa, situación que se ha evidenciado en el caso de las bases de datos corporativas, cubiertas por el concepto de continuidad del negocio con un proveedor externo (google).

Se evidencia de igual forma que el concepto de continuidad del negocio se aplica parcialmente y no se encuentra documentado el concepto de Recuperación de desastres ni de matriz BIA.

A.18 Cumplimiento con requerimientos legales y contractuales.

La entidad ha referenciado normativas y disposiciones legales vigentes relacionadas con el resguardo de la propiedad intelectual y las demás concordantes de aplicabilidad identificadas en el Nomograma 2017 de TRANSMILENIO S.A.
Sin embargo, en el Nomograma TMSA 2017 ya citado no se hace referencia a documentos que soporten el SGSI como es el caso de la ISO/IEC 27001:2013, gestión de riesgos de seguridad de la información ISO 27005 entre otras.

Generalidades: Los procesos Contractuales 2017 ejecutados asociados al SGSI fueron:

Objeto	Valor estimado	Rubro	No. Contrato
Contratar la prestación de servicios a través de una empresa especializada, para la realización de un test de intrusión (Ética 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.	$66.708.500	Gastos de Computador	CTO 232-17
Contratar la adquisición de una solución de protección de Red especializada que permita fortalecer la seguridad perimetral de la Red de Transmilenio S.A. en una segunda capa	$362.698.450	Operación y Control	CTO 579-17

Los procesos Contractuales 2018 previstos asociados al SGSI.

Objeto	Valor estimado	Rubro
Ética Hacking " Contratar la prestación de servicios a través de una empresa especializada, para la realización de un test de intrusión (Ética 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".	$42.000.000	Gastos de Computador
Mantenimiento y actualización de la Herramienta Modular de Seguridad de la Información.	$30.000.000	Gastos de Computador
Apoyar a la Dirección de Tics en la implementación y fortalecimiento de la estrategia de seguridad de la información de TRANSMILENIO S.A. en el marco de GEL	$80.000.000	Servicios Profesionales

CONCLUSIONES Y RECOMENDACIONES

En concordancia con las evidencias obtenidas se puede concluir sobre la implementación del Subsistema Sistema de Gestión de Seguridad de la Información (**SGSI)** en la Entidad, que de los 114 (100%) Controles exigidos en el anexo A de la NTC-ISO 27001:2013, 42 controles, es decir el 38% se cumplen satisfactoriamente, 56 controles que equivalen al 49% se cumplen parcialmente, y 8 controles que equivalen al 7% no se cumplen.

- Es importante precisar que los 8 controles que TRANSMILENIO S. A. actualmente no aplica, así como la selección de los mismos, dependen de las decisiones de la Entidad basadas en los criterios para la aceptación de los riesgos.

- Adicionalmente, es importante mencionar que la eficacia de los controles serán evaluados una vez revisado el Modelo de Seguridad y Privacidad de la Información o mediante las auditoras específicas.

- Si bien la entidad cuenta con una política de seguridad, no se evidenció que la misma cuente con las reglas necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información en todos los procesos, por lo que resulta necesario que dicha política sea definida, asignada y comunicada a todos los miembros de la Entidad, bajos los requisitos enunciados en la NTC-ISO 27001.

- Aunque actualmente, se cuenta con el comité del Sistema Integrado de Gestión – SIG, se evidenció en los soportes de actas de comité, que no se tratan a profundidad los temas inherentes a la implementación del SGSI tal como lo demanda la NTC-ISO 27001, razón por la cual se recomienda con regularidad se incluya un punto en el Comité en el cual se presente el porcentaje de avance en la implementación del SGSI, así como los inconvenientes presentados.

- Evaluar la conformación de un equipo de trabajo orientado a la implementación del SGSI, dirigido por la Dirección de las TIC bajo los requisitos de la NTC-ISO 27001.

- Durante la realización del diagnóstico se evidenció que en la Entidad no se realizan resúmenes de los análisis de incidentes y vulnerabilidades de seguridad de la información y tampoco son presentados ante la gerencia de la Entidad. Por lo anterior, se observa debilidad en el cumplimiento de la NTC-ISO 27001 y se requiere dar efectivo cumplimiento a lo enunciado.

- Se evidenció que no existe un equipo de trabajo completo para la implementación de la NTC-ISO 27001 en la Entidad, generando así incumplimiento en el numeral 5.1 de la norma enunciada, razón por la cual, esta oficina recomienda la creación de dicho grupo de trabajo.

- No se evidenció adecuada asignación sobre la protección de activos individuales claramente definidos en la Entidad incumpliendo el numeral A12 de la NTC-ISO 27001, lo anterior en razón a que el archivo enviado a esta oficina por parte de la Dirección de las TICs mediante correo electrónico, no se encuentra adoptado ni controlado por el SGSI y la información allí registrada no es concordante con la política de inventario de

activos de información enunciada en el Manual de Políticas de Seguridad de la Información con código M-DT-001 versión 1 en el numeral 8.7.1 Inventarios de activos.

- Se recomienda fortalecer las campañas de sensibilización para asegurar que los empleados y contratistas tomen conciencia y den cumplimiento a sus responsabilidades en materia de seguridad de la información.

- Los contratos de prestación de servicios personales no presentan cláusulas en materia de Seguridad de la información que exija a los contratistas que se encuentren debidamente informados sobre sus roles y responsabilidades de seguridad de la información antes de que se les otorgue el acceso a la información o sistemas de información confidenciales. Por lo anterior se requiere que la Alta Dirección incluya en los "*lineamientos generales del contrato*" para los de PSP, dicha cláusula.

- No se evidenció adecuada implementación, como lo establece el numeral 7.2.1, de la GTC-ISO/IEC 27002 en cuanto a que la Entidad cuente con un canal de reporte anónimo de incumplimiento de políticas o procedimientos de seguridad de la información ("Denuncias internas"), razón por la cual, se recomienda dar cumplimiento a lo enunciado.

- La Entidad debe fortalecer los controles de los activos pertinentes en el ciclo de vida de la información y documentar su importancia incluyendo su creación, procesamiento, almacenamiento, trasmisión, eliminación y destrucción

- La Entidad debe fortalecer el inventario de activos de información (Hw y Sw) actualizarlo y alinearlo con otros inventarios, así mismo se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de la información adoptado por la Entidad, de otra parte fortalecer los controles para la devolución de activos involucrando a Dirección de las TIC´s.

- Fortalecer e implementar estrategias para el cumplimiento adecuado de la política de puesto de trabajo despejado y bloqueo de pantalla asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades y la cumplan.

- Fortalecer la política sobre el uso de controles criptográficos para la protección de la información, incluyendo los principios generales bajo los cuales se debería proteger la información de la Entidad.

- Fortalecer la política sobre el uso, protección y tiempo de vida de las llaves criptografías durante todo su ciclo de vida con el objetivo de dar cumplimiento al Manual de Seguridad de la Entidad en materia de niveles de seguridad.

- Fortalecer los controles de acceso físico apropiados para asegurar que solo se permite el ingreso a personal autorizado considerando las siguientes directrices: un registro de la fecha y hora de entrada y salida de los visitantes.

- Fortalecer los procedimientos de operación documentándolos y poniéndolos a disposición de todos los usuarios que los necesitan

- Fortalecer las copias de respaldo de información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con las políticas de copias de respaldo acordadas, incluyendo: Requisitos de retención y protección, mejorar la herramienta con que se hace el backup adquiriendo una de mayor capacidad y cumplir con lo establecido en el numeral 8.11.3 Copias de Seguridad de la Información del Manual de Políticas de Seguridad de la Información M-DT-001 que menciona:
  "***Seguridad del almacenamiento de backup***
  … Los controles aplicados a los medios del sitio principal deben ser extendidos al sitio de respaldo externo…" (Subrayado fuera del texto).

- La Entidad debe fortalecer las políticas de desarrollo seguro, controles para establecer y aplicar las reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la Entidad y los cambios de los sistemas dentro del ciclo de vida de desarrollo de software.

- Fortalecer los controles para establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la Entidad, así mismo tratar los riesgos de Seguridad de la Información asociados con la cadena de suministros de productos y servicios de tecnologías de información y comunicación, manteniendo el nivel acordado de Seguridad de la información y de prestación de servicios de los proveedores.

- Documentar los procedimientos y procesos de la operación de las unidades de control de acceso (proceso de seguridad física), para poder establecer acuerdos de nivel de servicio claros y eficientes con los proveedores, acordes con los lineamientos del sistema de gestión de seguridad de la información, en procura siempre del mejoramiento continuo.

- Fortalecer la política para el reporte y tratamiento de incidentes de seguridad mediante controles que permitan asegurar una respuesta rápida eficaz y ordenada a los incidentes de Seguridad de la Información, sensibilizar a los empleados y contratistas para tomar conciencia de su responsabilidad de reportar eventos de seguridad de la información.

- Reforzar los planes de continuidad de negocio, análisis de impacto del negocio (planes de contingencias, sedes alternas) y planes de recuperación desastre, a través de la generación de estrategias diversas tales como sensibilizaciones, capacitaciones, ejercicios de suplencia escalonados, etc., para disminuir el nivel de impacto, en la posibilidad de materializarse un evento que pudiese afectar la operación del negocio. Así mismo verificar a intervalos regulares los controles de continuidad de la Seguridad de la Información establecidos e implementados, con el fin de asegurar que son eficaces durante situaciones adversas.

- Realizar con más frecuencia pruebas controladas sobre dispositivos de seguridad electrónica (controles de acceso), verificando su correcto funcionamiento y el estado de sus componentes, para prevenir posibles fallas en el escenario de poder materializarse un riesgo de seguridad física y a su vez establecer los tiempos de reacción y prestación de servicios de seguridad por terceras partes.

Cualquier información adicional con gusto será suministrada.

Bogotá D.C., 04 de abril del 2018.

LUIS ANTONIO RODRÍGUEZ OROZCO
Jefe Oficina de Control Interno

Elaboró: Luz Marlenny Cano Romero - Contratista.