INFORME: OCI-2019-055

PROCESO / ACTIVIDAD REALIZADA: Seguimiento a la Implementación del Plan Estratégico de Seguridad de la Información.

EQUIPO AUDITOR: Jorge Iván Flórez, contratista.

OBJETIVO: Verificar el grado de avance en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) de TRANSMILENIO S.A., en el marco de los requisitos definidos en la NTC-ISO-IEC 27001:2013

ALCANCE: El alcance de la presente labor de consultoría, comprende la implementación al Sistema de Seguridad de la Información, liderado por la Dirección de TIC para el periodo comprendido entre marzo 31 de 2018 y marzo 31 de 2019, para los 14 dominios de la norma NTC-ISO-IEC 27001:2013.

CRITERIOS:

1. Norma NTC-ISO-IEC 27001**:** 2013
2. Ley 1581 de 2012, Ley de Protección de Datos Personales
3. Manual de Políticas de la Seguridad y Privacidad de la Información de TMSA
4. Formatos, Manuales, Procedimientos, Instructivos, Protocolos del SIG de TMSA

1. DESCRIPCIÓN DEL TRABAJO REALIZADO

Se realizó un análisis permitiendo evaluar el estado de los avances en la implementación del SGSI, enmarcado en la Planeación Estratégica de Seguridad de la Información PESI, de TRANSMILENIO S.A.

Dicho análisis fue realizado, utilizando y aplicando la herramienta “Análisis GAP Norma NTC ISO-IEC 27001:2013, diligenciando el Anexo A, el cual presenta los controles de cada uno de los dominios y subdominios definidos en la norma mencionada. Una vez diligenciado el Anexo, se obtuvieron los resultados en porcentaje de avance del cumplimiento tanto de los subdominios, como

de los dominios, representados en la escala de cumplimiento y en los resultados del nivel de implementación de controles.

Las herramientas utilizadas se presentan a continuación:

a) Escala de cumplimiento Norma ISO 27001:2013. Este cuadro colorimétrico, recoge los resultados generales y se determina el nivel de implementación del Sistema en la Entidad, tal como se muestra a continuación:

Nivel de Implementación	% de Cumplimiento	Descripción
Gestionado	100%	Los procesos han sido llevados al nivel de mejores prácticas, con base en los resultados de la mejora continua.
		Es posible hacer seguimiento y medir el cumplimiento de los procedimientos, así como tomar acciones correctivas o preventivas cuando se detectan fallas y hacer seguimiento dichas acciones.
Medible	80%	Es posible hacer seguimiento y medir el cumplimiento de los procedimientos, aunque no es constante que se tomen acciones correctivas o preventivas.
Definido	60%	Los procesos se encuentran totalmente documentados pero la responsabilidad del cumplimiento recae en cada individuo y es poco probable que se detecten desviaciones a los estándares establecidos.
Repetible	40%	Los procesos se han desarrollado hasta un punto en el cual procedimientos similares son utilizados por personas diferentes para llevar a cabo la misma tarea, aun cuando estos no se encuentran totalmente documentados.
Inicial	20%	Se ha identificado una situación que debe ser tratada y se han implementado acciones aun cuando no hay directivas o procesos documentados relacionados con dichas acciones.
Inexistente	0%	Carencia total de procesos relacionados con el SGSI.
		La organización no ha identificado una situación que debe ser tratada.

1tabla GAP

b) Análisis GAP- Resultados nivel de implementación de controles Norma ISO 27001:2013: Con esta tabla, se califican la totalidad de los controles definidos en la norma y recoge el porcentaje de avance que se registró en el Anexo A, tal y como se muestra a continuación:

Ítem	Controles	NM (%)
A.5..	POLITICA DE SEGURIDAD	100%
A.5.1.	Política de Seguridad de la Información	100%
A.5.1.1	Políticas para la seguridad de la información	100%
A.5.1.2	Revisión de la política de seguridad de la información	100%
A.6..	ORGANIZACION DE LA SEGURIDAD DE LA INFORMACIÓN	82%
A.6.1.	Organización interna	64%
A.6.1.1	Seguridad de la información Roles y responsabilidades	80%
A.6.1.2	Separación de deberes	60%
A.6.1.3	Contacto con las autoridades	80%
A.6.1.4	Contacto con grupos de interés especial	100%
A.6.1.5	Seguridad de la información en gestión de proyectos	0%
A.6.2.	Dispositivos móviles y teletrabajo	100%
A.6.2.1	Política para dispositivos móviles	100%
A.6.2.2	Teletrabajo	100%
A.7..	SEGURIDAD DE LOS RECURSOS HUMANOS	72%
A.7.1.	Antes de asumir el empleo	70%
A.7.1.1	Selección	60%
A.7.1.2	Términos y condiciones del empleo	80%

Ítem	Controles	NM (%)
A.7.2.	Durante la ejecución del empleo	87%
A.7.2.1	Responsabilidades de la dirección	80%
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	100%
A.7.2.3	Proceso disciplinario	80%
A.7.3.	Terminación y cambio de empleo	60%
A.7.3.1	Terminación o cambio de responsabilidades de empleo	60%
A.8..	GESTIÓN DE ACTIVOS	45%
A.8.1.	Responsabilidad por los activos	55%
A.8.1.1	Inventario de activos	80%
A.8.1.2	Propiedad de los activos	80%
A.8.1.3	Uso aceptable de los activos	20%
A.8.1.4	Devolución de activos	40%
A.8.2.	Clasificación de la información	40%
A.8.2.1	Clasificación de la información	40%
A.8.2.2	Etiquetado de la información	40%
A.8.2.3	Manejo de activos	40%
A.8.3.	Manejo de medios de soporte	40%
A.8.3.1	Gestión de medios de soporte removibles	100%

Ítem	Controles	NM (%)
A.8.3.2	Disposición de los medios de soporte	20%
A.8.3.3	Transferencia de medios de soporte físicos	0%
A.9..	CONTROL DE ACCESO	64%
A.9.1.1	Requisitos del negocio para control de acceso	80%
A.9.1.2	Política de control de acceso	80%
A.9.1.3	Acceso a redes y a servicios en red	80%
A.9.2.	Gestión de acceso de usuarios	57%
A.9.2.1	Registro y cancelación del registro de usuarios	60%
A.9.2.2	Suministro de acceso de usuarios	60%
A.9.2.3	Gestión de derechos de acceso privilegiado	60%
A.9.2.4	Gestión de información de autenticación secreta de usuarios	60%
A.9.2.5	Revisión de los derechos de acceso de usuarios	40%
A.9.2.6	Retiro o ajuste de los derechos de acceso	60%
A.9.3.	Responsabilidades de los usuarios	60%
A.9.3.1	Uso de información de autenticación secreta	60%
A.9.4.	Control de acceso a sistemas y aplicaciones	60%
A.9.4.1	Restricción de acceso a información	60%
A.9.4.2	Procedimiento de ingreso seguro	60%

Ítem	Controles	NM (%)
A.9.4.3	Sistema de gestión de contraseñas	80%
A.9.4.4	Uso de programas utilitarios privilegiados	60%
A.9.4.5	Control de acceso a códigos fuente de programas	40%
A.10..	CRIPTOGRAFÍA	40%
A.10.1.	Controles criptográficos	40%
A.10.1.1	Política sobre el uso de controles criptográficos	40%
A.10.1.2	Gestión de claves	40%
A.11..	SEGURIDAD FÍSICA Y DEL ENTORNO	58%
A.11.1.	Áreas Seguras	57%
A.11.1.1	Perímetro de seguridad física	80%
A.11.1.2	Controles de acceso físico	60%
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	60%
A.11.1.4	Protección contra amenazas externas y ambientales	60%
A.11.1.5	Trabajo en áreas seguras	80%
A.11.1.6	Áreas de carga, despacho y acceso público	0%
A.11.2.	Equipos	60%
A.11.2.1	Ubicación y protección de los equipos	60%
A.11.2.2	Servicios públicos de soporte	80%

Ítem	Controles	NM (%)
A.11.2.3	Seguridad del cableado	80%
A.11.2.4	Mantenimiento de los equipos	60%
A.11.2.5	Retiro de activos	40%
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	20%
A.11.2.7	Disposición segura o reutilización de equipos	20%
A.11.2.8	Equipos de usuario desatendido	100%
A.11.2.9	Política de escritorio limpio y pantalla limpia	80%
A.12..	SEGURIDAD DE LAS OPERACIONES	55%
A.12.1.	Procedimientos Operacionales y Responsabilidades	30%
A.12.1.1	Documentación de los procedimientos de operación	40%
A.12.1.2	Gestión del cambios	40%
A.12.1.3	Gestión de la capacidad	20%
A.12.1.4	Separación de las instalaciones de desarrollo, pruebas y operación	20%
A.12.2.	Protección contra códigos maliciosos	100%
A.12.2.1	Controles contra códigos maliciosos.	100%
A.12.3.	Copias de respaldo	60%
A.12.3.1	Copias de respaldo de la información	60%
A.12.4.	Registro y seguimiento	55%

Ítem	Controles	NM (%)
A.12.4.1	Registro de eventos	40%
A.12.4.2	Protección de la información de registro	40%
A.12.4.3	Registros del administrador y del operador	40%
A.12.4.4	Sincronización de relojes	100%
A.12.5.	Control de software operacional	40%
A.12.5.1	Instalación de software en sistemas operativos	40%
A.12.6.	Gestión de la vulnerabilidad técnica	80%
A.12.6.1	Gestión de las vulnerabilidades técnicas	60%
A.12.6.2	Restricciones sobre la instalación de software.	100%
A.12.7.	Consideraciones sobre auditorías de sistemas de información	20%
A.12.7.1	Controles de auditorías de sistemas de información.	20%
A.13..	SEGURIDAD DE LAS COMUNICACIONES	37%
A.13.1.	Gestión de la seguridad de redes	47%
A.13.1.1	Controles de redes	40%
A.13.1.2	Seguridad de los servicios de red.	40%
A.13.1.3	Separación en las redes	60%
A.13.2.	Transferencia de información	65%
A.13.2.1	Políticas y procedimientos de transferencia de información	60%

Ítem	Controles	NM (%)
A.13.2.2	Acuerdos sobre transferencia de información	60%
A.13.2.3	Mensajes electrónicos	80%
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	60%
A.14..	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	19%
A.14.1.	Requisitos de seguridad de los sistemas de información	20%
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	20%
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	20%
A.14.1.3	Protección de transacciones de servicios de aplicaciones	20%
A.14.2.	Seguridad en los procesos de desarrollo y de soporte	38%
A.14.2.1	Política de desarrollo seguro	80%
A.14.2.2	Procedimientos de control de cambios en sistemas	40%
A.14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	40%
A.14.2.4	Restricciones en los cambios a los paquetes de software	40%
A.14.2.5	Principios de construcción de los sistemas seguros	40%
A.14.2.6	Ambiente de desarrollo seguro	40%
A.14.2.7	Desarrollo contratado externamente	20%
A.14.2.8	Pruebas de seguridad de sistemas	0%
A.14.2.9	Prueba de aceptación de sistemas	40%

Ítem	Controles	NM (%)
A.14.3.	Datos de prueba	0%
A.14.3.1	Protección de datos de prueba	0%
A.15..	RELACIONES CON LOS PROVEEDORES	17%
A.15.1.	Seguridad de la información en las relaciones con los proveedores	33%
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	100%
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	0%
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	0%
A.15.2.	Gestión de la prestación de servicios de proveedores	0%
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	0%
A.15.2.2	Gestión de cambios a los servicios de los proveedores	0%
A.16..	GESTIÓN DE INCIDENTES DE SEGURIDAD	20%
A.16.1.	Gestión de incidentes y mejoras en la seguridad de la información	20%
A.16.1.1	Responsabilidades y procedimientos	40%
A.16.1.2	Reporte de eventos de seguridad de la información	20%
A.16.1.3	Reporte de debilidades de seguridad de la información	40%
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	20%
A.16.1.5	Respuesta a incidentes de seguridad de la información	20%

Ítem	Controles	NM (%)
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	0%
A.16.1.7	Recolección de evidencia	0%
A.17..	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	23%
A.17.1.	Continuidad de seguridad de la información	7%
A.17.1.1	Planificación de la continuidad de la seguridad de la información	20%
A.17.1.2	Implementación de la continuidad de la seguridad de la información	0%
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	0%
A.17.2.	Redundancias	40%
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	40%
A.18..	CUMPLIMIENTO	57%
A.18.1.	Cumplimiento de requisitos legales y contractuales	68%
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	60%
A.18.1.2	Derechos de propiedad intelectual	80%
A.18.1.3	Protección de registros	100%
A.18.1.4	Privacidad y protección de información de datos personales	100%
A.18.1.5	Reglamentación de controles criptográficos	0%
A.18.2.	Revisiones de seguridad de la información	47%

Ítem	Controles	NM (%)
A.18.2.1	Revisión independiente de la seguridad de la información	60%
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	20%
A.18.2.3	Revisión del cumplimiento técnico	60%

Total 49%

c) Tabla de resultados por dominio: Esta tabla, recoge y resume los porcentajes de avance arrojados por la tabla anterior "Resultados Nivel de Implementación de Controles", y muestra el grado de cumplimiento para el total de dominios, tal y como se muestra a continuación:

ANÁLISIS GAP - RESULTADOS POR DOMINIO
NORMA ISO 27001:2013

Item	Dominios	Cumplimiento
5	POLITICA DE SEGURIDAD	100%
6	ORGANIZACION DE LA SEGURIDAD DE LA INFORMACIÓN	82%
7	SEGURIDAD DE LOS RECURSOS HUMANOS	72%
8	GESTIÓN DE ACTIVOS	45%
9	CONTROL DE ACCESO	64%
10	CRIPTOGRAFÍA	40%
11	SEGURIDAD FÍSICA Y DEL ENTORNO	58%
12	SEGURIDAD DE LAS OPERACIONES	55%
13	SEGURIDAD DE LAS COMUNICACIONES	37%
14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	19%
15	RELACIONES CON LOS PROVEEDORES	17%
16	GESTIÓN DE INCIDENTES DE SEGURIDAD	20%
17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	23%
18	CUMPLIMIENTO	57%
TOTAL		49%

Los porcentajes de avance para cada uno de los dominios y subdominios, fueron asignados por la Dirección de TIC y remitidos a ésta oficina mediante correo electrónico del 7 de mayo de 2019, la Oficina de Control Interno, realizo la verificación, registró las observaciones y recomendaciones, de acuerdo con las evidencias enviadas por la Dirección de TIC y por la documentación existente en la intranet de la Entidad en el micrositio MIPG (Manuales, Formatos, Procedimientos, instructivos, protocolos etc.

SITUACIÓN ACTUAL

Por situación actual se entiende el nivel de madurez que posee en este momento TRANSMILENIO S.A. con relación a la Seguridad de la información. El proceso por el cual se lleva a cabo esta estimación del nivel de madurez, se denomina instrumento de diagnóstico del MSPI (Modelo de seguridad y Privacidad de la Información), de MinTic, (Ministerio de las Tecnologías de la información y las Comunicaciones), análisis GAP (análisis de brecha, es un servicio que permite identificar la distancia existente entre la organización actual de la seguridad de la información en la empresa y las buenas prácticas más reconocidas en la industria). Para poder realizar el PESI, es indispensable que se tengan en cuenta los niveles de madurez alcanzados por cada uno de los 14 dominios de la norma NTC-ISO-IEC 27001:2013, con el fin de plantear prioridades sobre su implementación.

El nivel de madurez permite establecer las bases para la mejora continua del proceso de Seguridad de la Información de TRANSMILENIO S.A., e identifica el estado de contexto de la Entidad, liderazgo, planificación, soporte, operación, evaluación de desempeño y mejoras, los cuales se convierten en elementos esenciales en el proceso de mejoramiento continuo y deben estar alineadas a las necesidades que se identificaron en el Plan estratégico de Tecnologías de Información y Comunicaciones y la Estrategia de información PETI.

Se presenta a continuación, el nivel de madurez del modelo de seguridad y privacidad de la información y el porcentaje de cumplimiento de la Entidad frente a los 14 dominios de la Norma ISO IEC 27001:2013 e ISO IEC 27002:2013:

1. RESULTADOS DE LA VERIFICACIÓN

3.1 BRECHA ANEXO A NTC - IEC ISO 27001: 2013

En el Anexo A, Análisis GAP-Norma NTC-ISO-IEC 27001:2013, se cuenta con los resultados de nivel de implementación de controles y las observaciones realizadas por la Oficina de Control Interno, así como las calificaciones respectivas. En dicho anexo, se puede observar el análisis GAP - Escalas de Cumplimiento, que resume el porcentaje de nivel de implementación de acuerdo con los resultados generales obtenidos y permite ubicar a la Entidad en el respectivo nivel, tal y como se presenta a continuación:

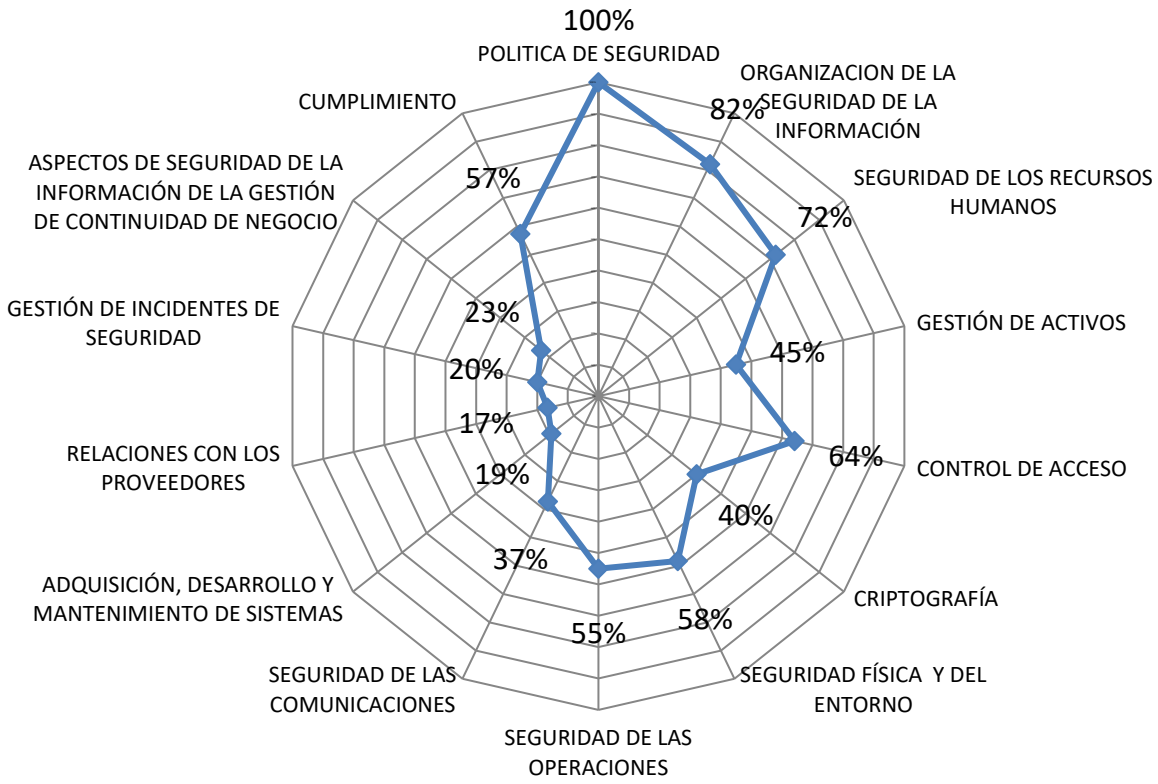
Nivel De Implementación	% Cumplimiento	Descripción
Gestionado	**100%**	Los procesos han sido llevados al nivel de mejores prácticas, con base en los resultados de la mejora continua. Es posible hacer seguimiento y medir el cumplimiento de los procedimientos, así como tomar acciones correctivas o preventivas cuando se detectan fallas y hacer seguimiento dichas acciones.
Medible	**80%**	Es posible hacer seguimiento y medir el cumplimiento de los procedimientos, aunque no es constante que se tomen acciones correctivas o preventivas.
Definido	**60%**	Los procesos se encuentran totalmente documentados pero la responsabilidad del cumplimiento recae en cada individuo y es poco probable que se detecten desviaciones a los estándares establecidos.
Repetible	**40%**	Los procesos se han desarrollado hasta un punto en el cual procedimientos similares son utilizados por personas diferentes para llevar a cabo la misma tarea, aun cuando estos no se encuentran totalmente documentados.
Inicial	**20%**	Se ha identificado una situación que debe ser tratada y se han implementado acciones aun cuando no hay directivas o procesos documentados relacionados con dichas acciones.
Inexistente	**0%**	Carencia total de procesos relacionados con el SGSI. La organización no ha identificado una situación que debe ser tratada.

Fuente: Tabla Escala de Valoración de Controles NTC – ISO- IEC 27001:2013 del Anexo A diligenciada por la Oficina de Control Interno

Adicional, el Anexo A cuenta con la lista de chequeo que permite observar los resultados del nivel de implementación de controles, los resultados por domino, resultados por subdominio y revisión del Anexo.

Con lo anterior, la Oficina de Control Interno, realizó un análisis general encontrando lo siguiente:

ANÁLISIS POR DOMINIOS



Analizando el grafico, se puede observar que los dominios con mayor nivel de madurez son Política de Seguridad de la Información (100%), Organización de la Seguridad de la información (82%) y Seguridad de los recursos Humanos (72%), lo cual, es el resultado del respaldo de la Alta dirección

de TRANSMILENIO S.A., para la implementación del Sistema de Gestión de la Seguridad de la Información de la Entidad, así como la realización del "Manual de las Políticas de la Seguridad y la Privacidad de la Información" y la "Organización de la Seguridad de la Información al interior de la Entidad".

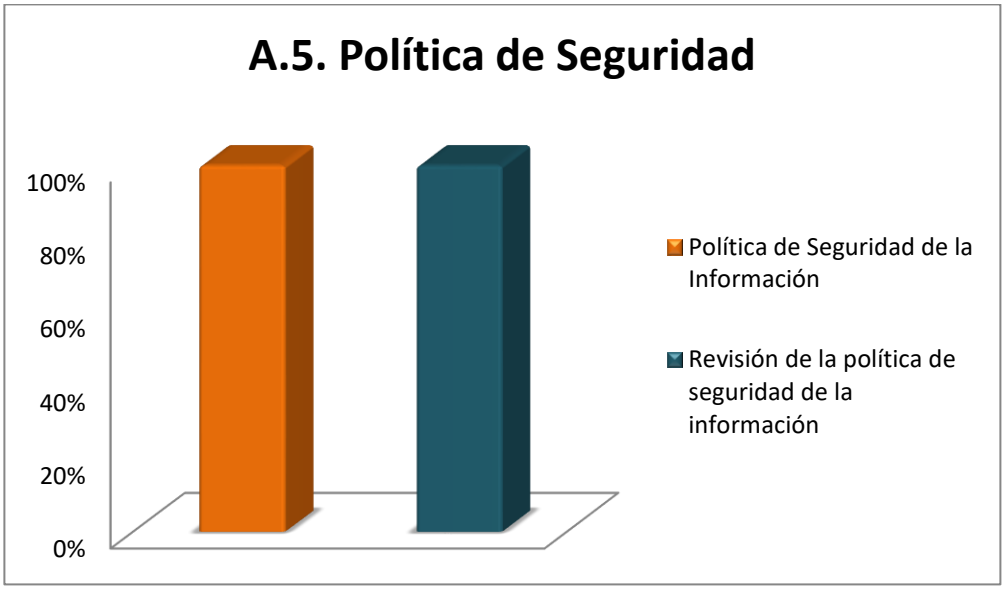
Sin embargo y aunque se muestra un avance significativo con respecto a lo alcanzado en la vigencia 2018, el resultado obtenido del grado de cumplimiento en la implementación del Sistema de Seguridad de la Información y/o nivel de madurez a mayo 31 de 2019 fue del 49%, que significa de acuerdo a la escala de cumplimiento definida en el análisis GAP, que la Entidad está levemente por encima del nivel "Repetible" (40%) es decir, que los procesos se han desarrollado hasta un punto en el cual procedimientos similares son utilizados por personas diferentes para llevar a cabo la misma tarea, aun cuando estos no se encuentran totalmente documentados.

Dichos avances no se han desarrollado en similares porcentajes en todos los frentes, prueba de ello son los relativos bajos, avances en lo que tiene que ver con la "Adquisición, Desarrollo y Mantenimiento de Sistemas" (19%), "Relaciones con los Proveedores" (17%), "Gestión de Incidentes de Seguridad" (20%) y "Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio" (23%), los cuales muestran muy bajos avances comparados con los otros dominios de la Norma. No obstante se considera importante precisar que dado que la Entidad no cuenta con un plan de continuidad del negocio, se incrementan los riesgos de interrupciones no planificadas en TI y telecomunicaciones, ciberataques, brechas de datos, interrupciones del suministro de red, incidentes de seguridad. Riesgos que no fueron identificados, analizados, valorados en el mapa de riesgos del proceso Gestión de TIC publicado en la intranet al corte de la presente evaluación.

A continuación, se presenta un gráfico, donde se muestra la evaluación por cada uno de los 14 dominios:

2. ANÁLISIS DE LOS 14 DOMINIOS DEFINIDOS EN EL ANEXO A

A5. POLÍTICA DE SEGURIDAD: Cumplimiento 100%.



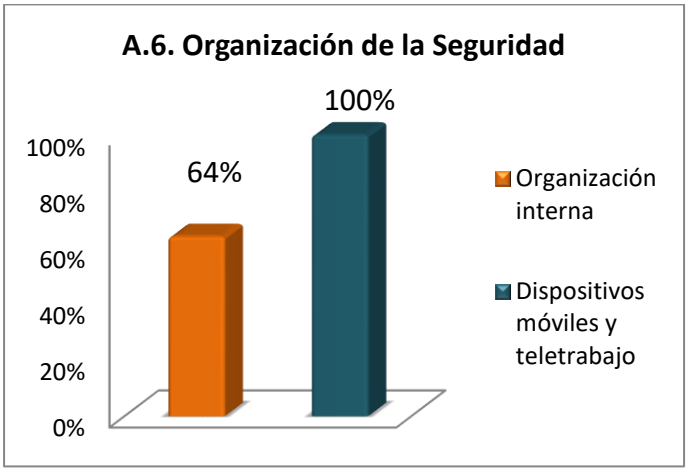
El objetivo en este punto, es brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes, para lo cual se constataron dos (2) subdominios:

1. Política de Seguridad de la Información: La entidad cuenta con el Manual, M-DT-001: de las Políticas de la Seguridad y la Privacidad de la Información, de última versión de fecha 3 de Abril de 2019, debidamente publicado en la intranet.

Para su divulgación, se evidencio la realización por parte de la Dirección de TIC, el "Plan de Cultura y Sensibilización del Sistema de Gestión de Seguridad de la Información – SGSI": T-DT-007, de Agosto de 2018 y su realización los pasados meses de: Septiembre a Diciembre del año 2018.

2. Revisión de la Política de Seguridad de la Información: El documento de las Políticas de la Seguridad y Confidencialidad de la Información de la Entidad, se revisa a intervalos planificados o cuando se producen cambios significativos. Evidencia de la última revisión es la fecha de versión 3 que corresponde a abril de 2019.

A.6. ORGANIZACIÓN DE LA SEGURIDAD: Cumplimiento 82%.



El Objetivo en este punto es que la Entidad tenga un Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización y garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles. En este punto, se tienen 2 subdominios a evaluar:

1. Organización Interna: Se indica que se debe establecer una estructura de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la Entidad en cuanto a:

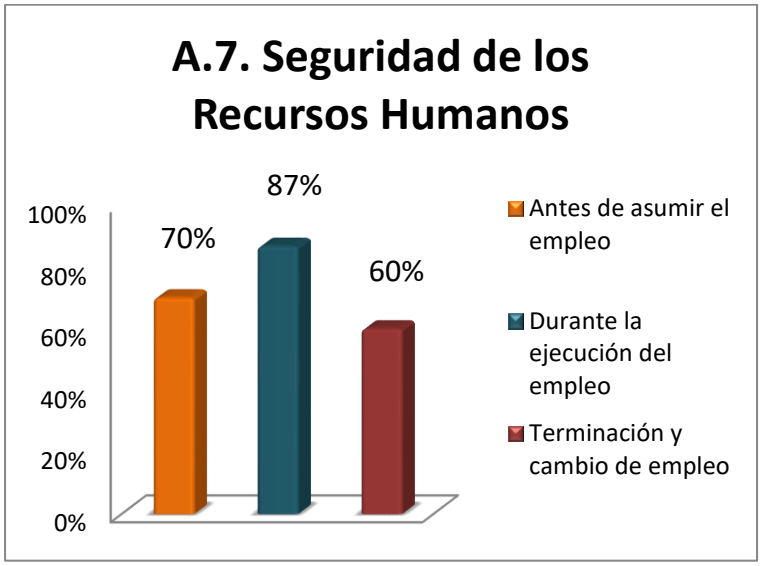
- Asignación de responsabilidades para la seguridad de la información: Las responsabilidades de las actividades específicas de la seguridad de la información están definidas, según el numeral 7: “Autoridades y Roles de Seguridad de la Información”, del “Manual de las Políticas de la Seguridad y la Privacidad de la Información”, donde se definen las autoridades y roles establecidos en el modelo de seguridad de la información, adoptado por la Entidad. Dichas autoridades y roles son: el “Comité de Coordinación del Sistema Integrado de Gestión”, el “Profesión al Especializado de Seguridad de la Información”, el “Profesional Especializados Procesos Corporativos”, el “Operador de Seguridad de la Información”, los “Propietarios de Activos de Información” y todos los “Usuarios de la Información”. Adicional a lo anterior se cuenta

con las funciones definidas para la Dirección de TIC en el Acuerdo 007 de 2017. Para los cargos de profesionales adscritos a la Dirección de TIC se cuenta con el Manual de funciones de los cargos.

- Distribución de Funciones: Están establecidas separaciones entre las funciones y las áreas de responsabilidad para reducir las oportunidades de la modificación no autorizada o uso inadecuado de los activos de información, con el directorio activo se dividen las tareas de acuerdo con el tipo de perfil, el cargo y los accesos a las aplicaciones de la entidad. Sin embargo, no se evidenció matriz de usuarios y perfiles de los sistemas de información con que cuenta la Entidad.
- Contacto con las Autoridades: Existen acuerdos o contactos con las autoridades, personal externo y/o organizaciones que manejen el tema de la seguridad de la información, de modo tal que se asegure que se puedan tomar acciones apropiadas oportunamente.
- Contactos con grupos de interés especiales: La Entidad mantiene contacto con grupos de interés, foros de especialistas en seguridad o en asociaciones profesionales, se tiene establecido en el Manual de Políticas de Seguridad y Privacidad de la Información: M-DT-001, versión 3 de Abril de 2019 y se cuenta con acceso al reporte de: Kaspersky, TRAPS: PaloAlto, Microsoft, y Fortinet, no obstante no se cuenta con contactos que pueden servir de apoyo tales como entidades de orden Nacional, Distrital, y del sector privado.
- Seguridad de la información en gestión de proyectos: En materia de gestión de proyectos, se evidenció que la Entidad no ha integrado la seguridad de la información en el ciclo de vida de los mismos, con el fin de asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto.
- Dispositivos Móviles y Teletrabajo: La Entidad cuenta con una política definida asociada al manejo y control de dispositivos móviles, mediante el manual de políticas de seguridad de la información, adicionalmente se evidenció que se realizan actividades de monitoreo tanto a dispositivos móviles propios de la Entidad, como a los personales conectados a la red corporativa, con el objeto de adoptar mecanismos de protección de la Información y aplicar las medidas correctivas.

La Dirección de TIC, establece además configuraciones definidas pare el manejo de los dispositivos móviles, siguiendo reglas para el uso aceptable de los Activos de la Información.

Respecto al Teletrabajo, se han desarrollado políticas y procedimientos para controlar los riesgos inherentes a actividades de trabajo remoto, no obstante no se evidenció aplicación de las políticas diseñadas para el periodo objeto de la presente consultoría.



A7. SEGURIDAD DE LOS RECURSOS HUMANOS, Cumplimiento: 72,2%

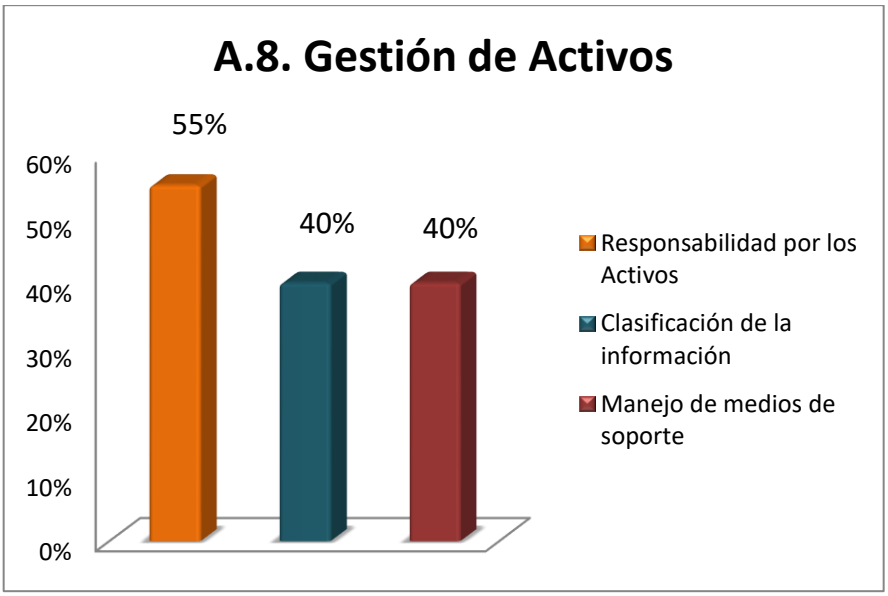
El objetivo en este punto es asegurar que el personal y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que son considerados, además que tomen consciencia de sus responsabilidades sobre la seguridad de la información y las cumplan, así como proteger los intereses de la Entidad para los casos de desvinculación.

En este punto, se verificaron 3 subdominios a saber:

1. Antes de Asumir el Empleo, durante la ejecución del empleo y terminación o cambio de la relación laboral: La Entidad cuenta con lineamientos definidos en el numeral 8.8 “Política del Recurso Humano”, del “Manual de la Seguridad y la Privacidad de la Información”, de los tres ítems evaluados, en materia de seguridad de la información. No obstante, no se evidenció que en el Plan

de Formación y Capacitación de TRANSMILENIO S.A., se tenga programación en temas de la Seguridad de la Información, para este año.

A.8. **GESTIÓN DE ACTIVOS**. Porcentaje de cumplimiento: 45%.



El Objetivo en este punto es: Lograr y mantener la protección adecuada de los activos de la organización. Todos los activos se deben incluir y deben tener un dueño designado.

En este aspecto, la Entidad cuenta con Políticas definidas, sobre: Responsabilidad por los Activos, Clasificación de la Información y Manejo de Medios de Soporte, en el en el Manual: M-DT-001: "Manual de Políticas de la Seguridad y Privacidad de la Información". Se cuenta además, con el Instructivo: I-DT-001: “Instructivo para la identificación, Valoración y Calificación de los Activos de la Información", de Abril de 2019. Se tiene el formato: R-DT-010: "Formato de Inventario de Activos de Información", donde se registran todos los Activos de la Información, los cuales pueden ser: Información, Hardware, Software, Servicios, Conocimiento. Se tiene el Protocolo a Seguir para Gestionar el Uso de los Medios Removibles: T-DT-003. No se evidenció la lista de activos de la

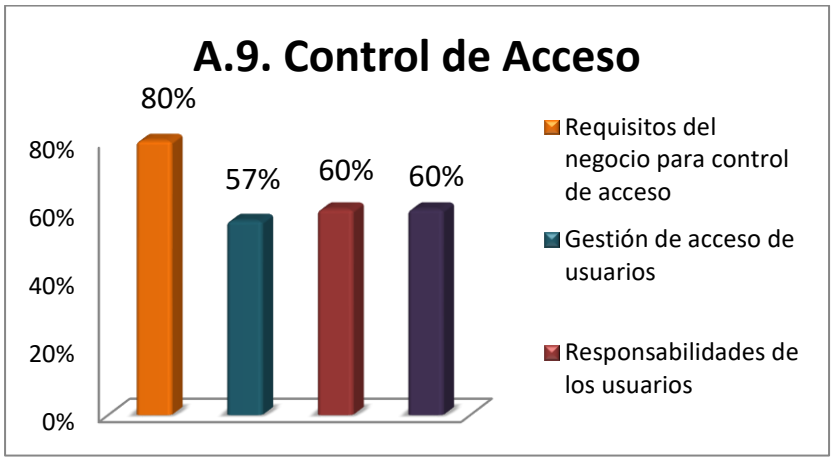
información de TRANSMILENIO S.A. Si bien se encuentra en construcción, al corte del presente documento, no ha sido formalizada.

No se evidenciaron registros sobre la aplicación de las políticas definidas por la entidad en materia de gestión de Activos.

No se evidenciaron registros sobre la aplicación de las políticas definidas por la entidad en materia de gestión de Activos.

No se evidenciaron procedimientos formalizados respecto a cumplir dichos lineamientos en materia de eliminación de activos de información cuando ya no se requieran.

A.9. CONTROL DE ACCESO, Cumplimiento: 64,2%



El Objetivo en este punto es: limitar el acceso a la información y a instalaciones de procesamiento de información, asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios, hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación y evitar el acceso no autorizado a sistemas y aplicaciones.

En este aspecto en la Entidad, se cuenta con el “Manual de Políticas de la Seguridad y la Privacidad de la Información”: M-DT-001, “Procedimiento Administración de Usuarios”: P-DT-007 y el “Procedimiento Otorgar Acceso a los Medios de Procesamiento de Información”: P-DT-011, donde se definen lineamientos claros respecto a los siguientes puntos:

- Requisitos del negocio para el control de acceso: La Entidad ha establecido una política de control de acceso con base en los requisitos del negocio en cuanto a seguridad y de este modo poder asegurar que los usuarios sólo tienen acceso a los servicios para los cuales están específicamente autorizados.

- Gestión de Acceso de Usuarios: La Entidad cuenta con el procedimiento: P-DT-007 Administración de Usuarios, versión 3 de Enero de 2019. Además, cuenta con el procedimiento: P-DT-011: Procedimiento para Otorgar Acceso a los Medios de Procesamiento de Información, con los cuales se realiza el registro, cancelación, suministro de usuarios y de retiro del acceso a los sistemas de procesamiento de información a empleados, contratistas o terceras partes al finalizar la relación laboral, contrato o acuerdo.

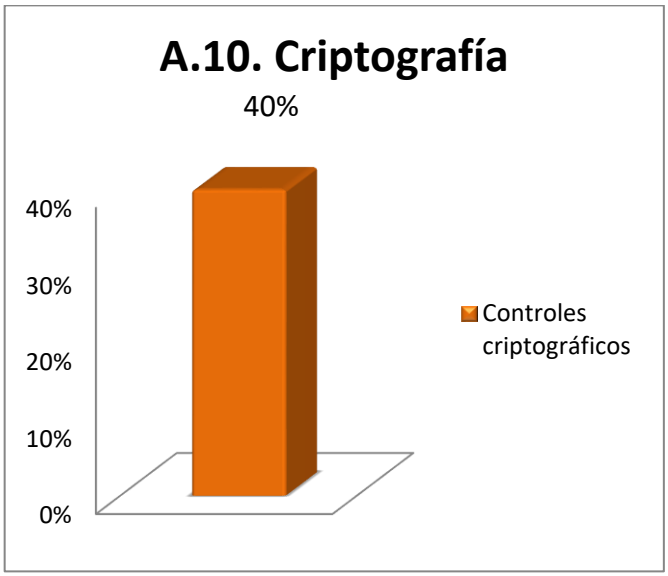
Sin embargo, la Entidad no cuenta con un proceso formal para la asignación y uso de privilegios a los usuarios de los Sistemas de Información (privilegios asignados con base a requerimientos necesarios para su desempeño), tampoco tiene un procedimiento formal para la revisión periódica de los derechos de acceso a usuarios.

- Responsabilidad de los Usuarios: Se realizaron campañas de sensibilización en la Entidad dirigida a los usuarios a través de los medios de comunicación interna, sobre buenas prácticas de la seguridad en la selección y el uso de contraseñas, además se exige a los usuarios el cumplimiento de estas buenas prácticas, en el momento de cambiar las contraseñas respectivas.

- Control de Acceso a Sistemas y Aplicaciones: El acceso a los datos y a las funciones de los sistemas de aplicaciones se restringe de acuerdo con las políticas de acceso definidas, existe un procedimiento de registro de inicio seguro para acceso a los sistemas operativos, se tiene un sistema de gestión de contraseñas, que se emplea para autenticar a usuarios, además se garantiza la calidad de las contraseñas, se restringen los programas utilitarios de sistemas que se podrían

utilizar para pasar los controles de los sistemas y aplicaciones, sin embargo no se tiene un procedimiento formal llevar a cabo esta acción. Además para reducir el potencial para la corrupción de los programas de los sistemas, el acceso al código fuente es controlado, pero tampoco se tiene un procedimiento formal para esto.

A.10. **CRIPTOGRAFÍA**, Cumplimiento 40%

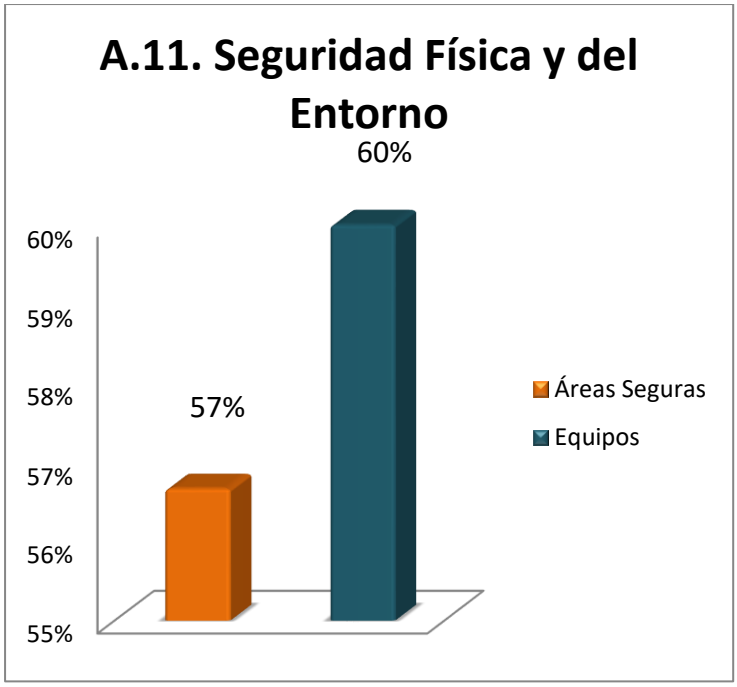


El Objetivo en este punto es establecer si la Entidad ha desarrollado una política sobre el uso de controles criptográficos y si existe un sistema de administración implementado para soportar el uso en la organización de llaves públicas y privadas.

Se cuenta con el “Manual de Políticas de la Seguridad y la Privacidad de la Información”: M-DT-001, numeral: 9.3: “Política sobre el Uso de Controles Criptográficos”, donde se define la Política y lineamientos claros respecto al uso de los controles criptográficos y la gestión de claves en la Entidad. Sin embargo, no se evidenció la existencia de un sistema o procedimiento de administración formalizado e implementado para soportar el uso en la organización de llaves públicas y privadas.

A.11. SEGURIDAD FÍSICA Y DEL ENTORNO, Cumplimiento: 58.3%.

El objetivo en este punto es prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización. Además prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.



En este aspecto, se verifican dos puntos a saber:

1. Áreas Seguras: Se tiene definida la Política de Áreas Seguras, en el Manual de las Políticas de la Seguridad y la Privacidad de la Información, en cuanto a los aspectos de: Perímetro de seguridad física, controles de acceso físico, seguridad de oficinas, recintos e instalaciones, protección contra amenazas externas y ambientales, trabajo en áreas seguras, áreas de carga, despacho y acceso público. Respecto al Subdominio Áreas de carga, despacho y acceso público, la Entidad no cuenta con este tipo de áreas, por lo que se registró un avance de 0%.

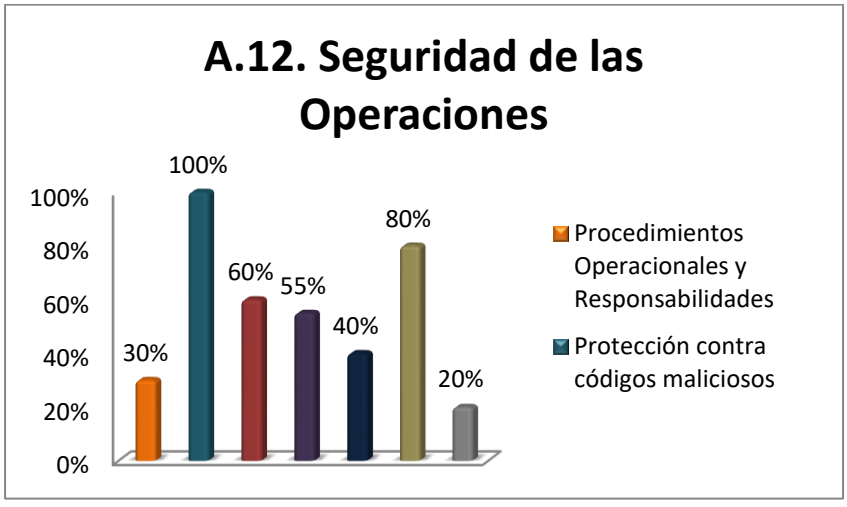
2. Equipos: su objetivo es evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización. Se tiene definida la Política de Seguridad delos Equipos, en el Manual de las Políticas de la Seguridad y la Privacidad de la Información y en cuanto a: ubicación y protección de los equipos, servicios públicos de soporte, seguridad del cableado, mantenimiento de los equipos.

No se evidencio un procedimiento definido para retiro de equipos, información o software que requiera previa autorización.

No se evidencio un procedimiento, para la seguridad de los equipos que se encuentran fuera de las instalaciones, teniendo en cuenta los diferentes riesgos que esto conlleva.

No se evidencio un procedimiento para la disposición segura o reutilización de equipos.

A.12. SEGURIDAD DE LAS OPERACIONES, Cumplimiento: 55%



El Objetivo en este punto es: asegurar la operación correcta y segura de los servicios de procesamiento de información.

En este caso, se analizan 7 subdominios a saber:

En este aspecto, la Entidad, tiene definida la Política de Seguridad en la Operaciones, en el Manual de la Seguridad de las Políticas de Seguridad y Privacidad de la Información, donde se dan lineamientos claros sobre: Procedimientos Operacionales y Responsabilidades, protección contra códigos maliciosos, copias de respaldo de la información, registro y seguimiento, control de software operacional, gestión de la vulnerabilidad técnica y consideraciones sobre Auditorías de Sistemas de Información.

Sin embargo, no se evidencian procedimientos de operación requeridos para la mejora continua del sistema de gestión de seguridad de la información.

Se tienen procedimientos de Gestión de Cambios y se evidenciaron avances en la formalización del Comité de Gestión de Cambios de la Entidad.

No se evidenció el documento de gestión de la capacidad, para asegurar el desempeño requerido del sistema.

No se evidencia una clara separación en los ambientes de desarrollo, prueba y producción, para reducir los riesgos de acceso o cambios no autorizados al ambiente de producción.

Se cuenta con procedimientos de copias de respaldo y se evidenció que se realizan, sin embargo, no se cuenta con procedimientos para la restauración de dichos respaldos, de modo que se pueda probar la efectividad de los mismos y de esta manera, tener la seguridad de usarlos en un momento de requerirlos.

Registro y seguimiento: Se tienen lineamientos claros, en el Manual de la Seguridad y la Privacidad de la Información, sin embargo no se evidencia un procedimiento encaminado a revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información, tampoco se evidencia un procedimiento para revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

No se evidencia un procedimiento para controlar la instalación de software en sistemas operativos, aplicaciones y programas por parte de los administradores

En la Entidad, todos los sistemas (servidores, equipos activos de red y máquinas de usuarios) cuentan con sincronización de reloj a nivel de sistema operativo, teniendo como referencia la Hora Legal Colombiana y no está permitida la desactivación del sistema de sincronización o la manipulación manual de la hora.

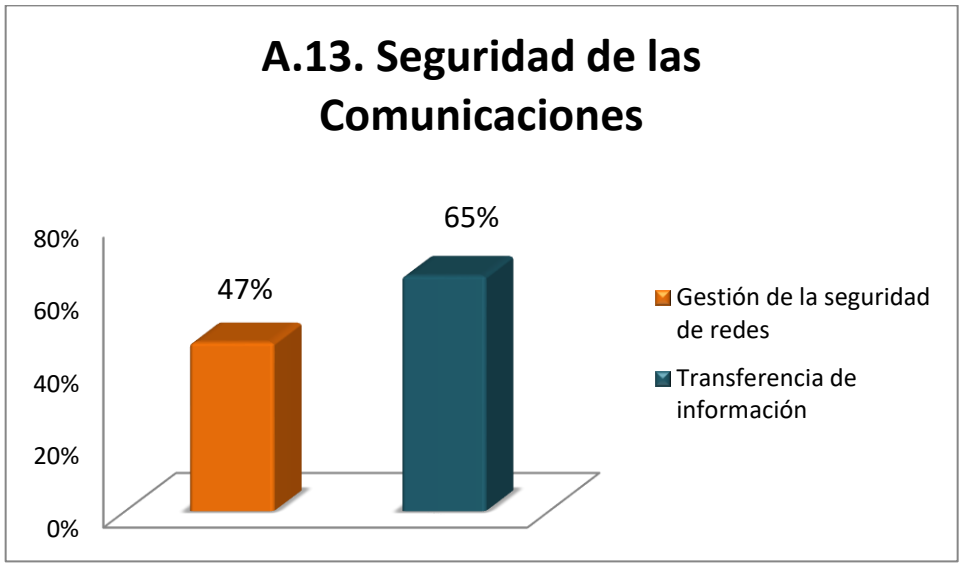
Control de Software Operacional: No se evidencio la existencia de procedimientos para controlar la instalación e implementación de software en los sistemas operativos.

Gestión de la vulnerabilidad técnica, se obtiene información sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, sin embargo no se evidenciaron procedimientos formales establecidos, donde se evalúe la exposición de la organización a dichas vulnerabilidades.

Se han implementado procedimientos e infraestructura, respecto a la prohibición de la instalación de Software, por parte de los usuarios en la Entidad.

Consideraciones sobre auditorías de sistemas de información: No se evidencian procedimientos formalizados e implementados, para cuando el desarrollo de Software es subcontratado en la Entidad, donde se definan los detalles para proteger, supervisar y monitorear el desarrollo éste.

A.13 SEGURIDAD DE LAS COMUNICACIONES, Cumplimiento: 55,8%



El Objetivo en este punto es: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte. Además mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

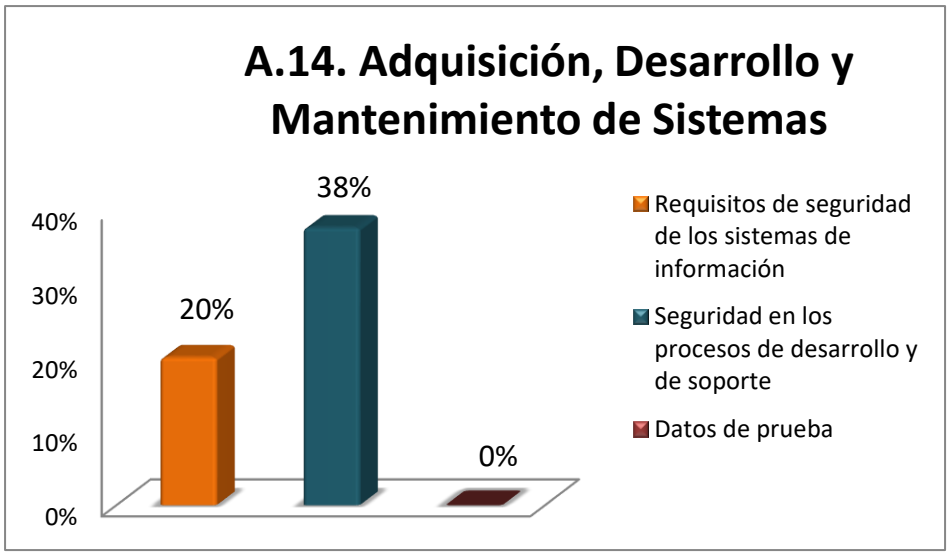
En este aspecto, se evalúan dos puntos a saber:

1. Gestión de la seguridad de redes: La Entidad tiene lineamientos claros respecto a la Seguridad en las comunicaciones, según el Manual de las Políticas de la Seguridad y la Privacidad de la Información. Sin embargo, no se evidencian tener procedimientos documentados e implementados respecto a los Controles en las Redes y la Seguridad de los Servicios de Red.

En cuanto a la Segmentación de las redes, también se cuentan con lineamientos claros y estos se vienen implementando en la Entidad, en función de los grupos de servicios, usuarios y sistemas de información.

2. Transferencia de información: La Entidad cuenta con la Política de la Seguridad en la Transferencia de la Información, según el Manual de las Políticas y la Seguridad y la Privacidad de la Información. Se cuenta además, con el procedimiento: P-DT-012: "Procedimiento para el intercambio seguro de información electrónica", de abril de 2019, el cual se viene implementando en la Entidad respecto a las Políticas y procedimientos de transferencia de información.

A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS, Cumplimiento: 29%



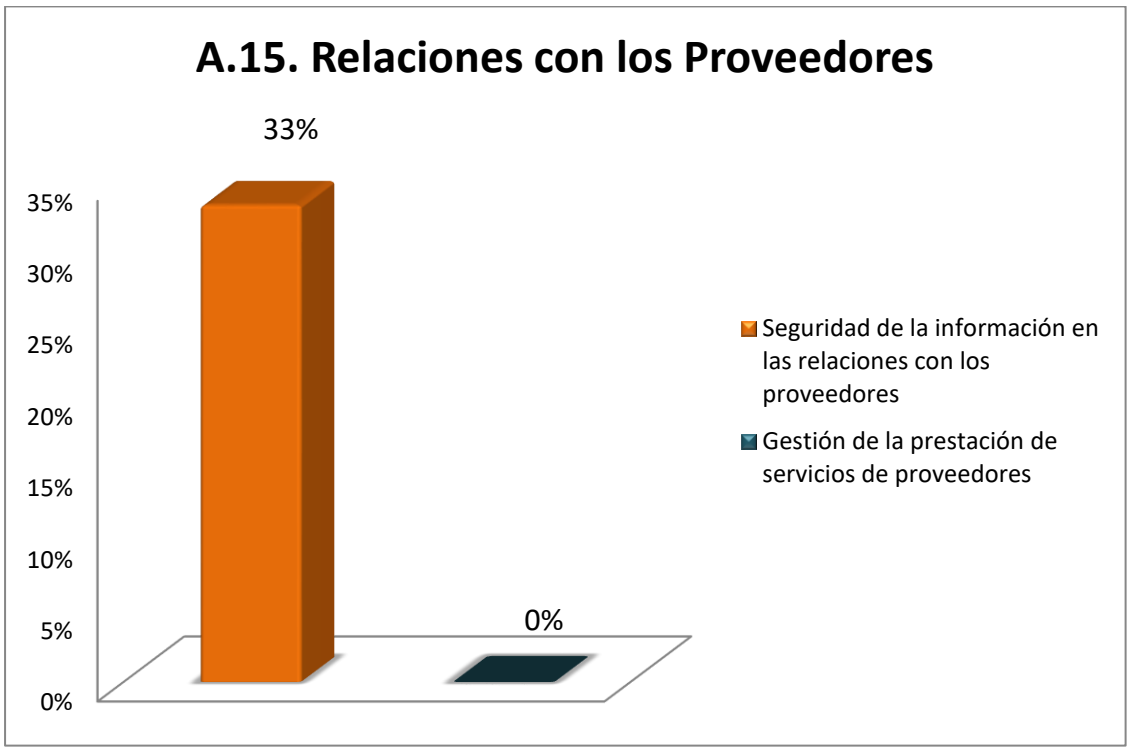
El Objetivo en este punto es asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Además asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información y asegurar la protección de los datos usados para pruebas.

En este aspecto la Entidad tiene la “Política de Desarrollo Seguro”, en el numeral 9.4, del “Manual de las Políticas de la Seguridad y la Privacidad de la Información”: M-DT-001. Se tiene el formato: “Especificación de Requerimientos de Software – ERS”: R-DT-004. Se cuenta además con el procedimiento: “Gestión del Ambiente de Pruebas de Software”: P-DT-004. Se cuenta con el Procedimiento: “Compra y Actualización de Software”: P-DT-005. Se tiene el procedimiento: “Construcción de Sistemas de Información”: P-DT-013. Se cuenta con el protocolo: “Protocolo Estándares para el Desarrollo de Software en Transmilenio S.A.”: T-DT-002, donde se dan lineamiento claros en cuanto a lo que tiene que ver con la adquisición o el desarrollo de Software para la Entidad.

Sin embargo no se evidencian la definición de los requisitos relacionados con seguridad de la información, ni directrices de control de cambios en los sistemas de información, ni en revisión técnica de las aplicaciones después de cambios en la plataforma de operación, ni directrices de restricciones en los cambios a los paquetes de software, ni directrices para ambiente desarrollo seguro.

Tampoco se evidencian procedimientos para la realización de pruebas de seguridad de la información para que los desarrollos nuevos o modificaciones a los Sistemas ya existentes puedan pasar al estado: “Paso a Producción”.

A.15. RELACIÓN CON LOS PROVEEDORES, Cumplimiento 17%.



El Objetivo en este punto es: que la Entidad Asegure la protección de los activos que sean accesibles para los proveedores y mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores

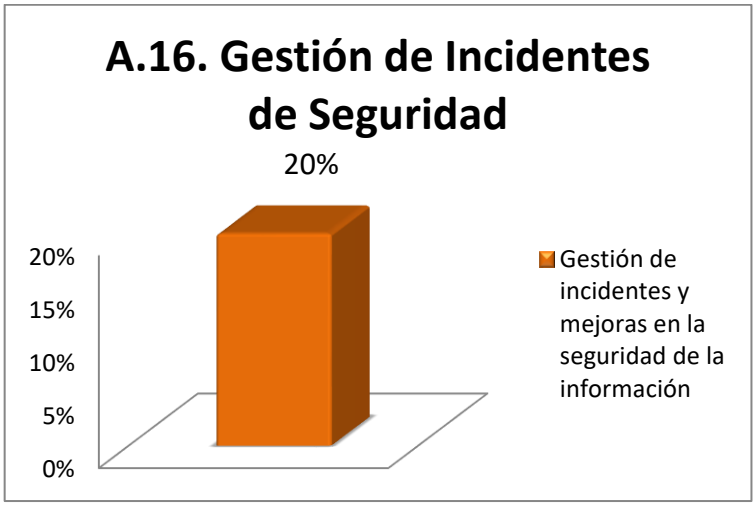
En este aspecto, la Entidad tiene definida la Política de la Seguridad de la Información para las relaciones con los proveedores, en el Manual de las Políticas de la Seguridad y la Privacidad de la Información.

Sin embargo, no se evidenció el establecimiento de los requisitos de Seguridad de la Información pertinentes con cada proveedor para que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la Entidad.

Tampoco se evidenció tener acuerdos con los proveedores que incluyan requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

Tampoco se tienen definidos procedimientos de gestión de cambios en la prestación de servicios con terceras partes que incluya mantenimiento, mejoras de políticas existentes de seguridad, procedimientos, sistemas, etc.

A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD, Cumplimiento 20%.



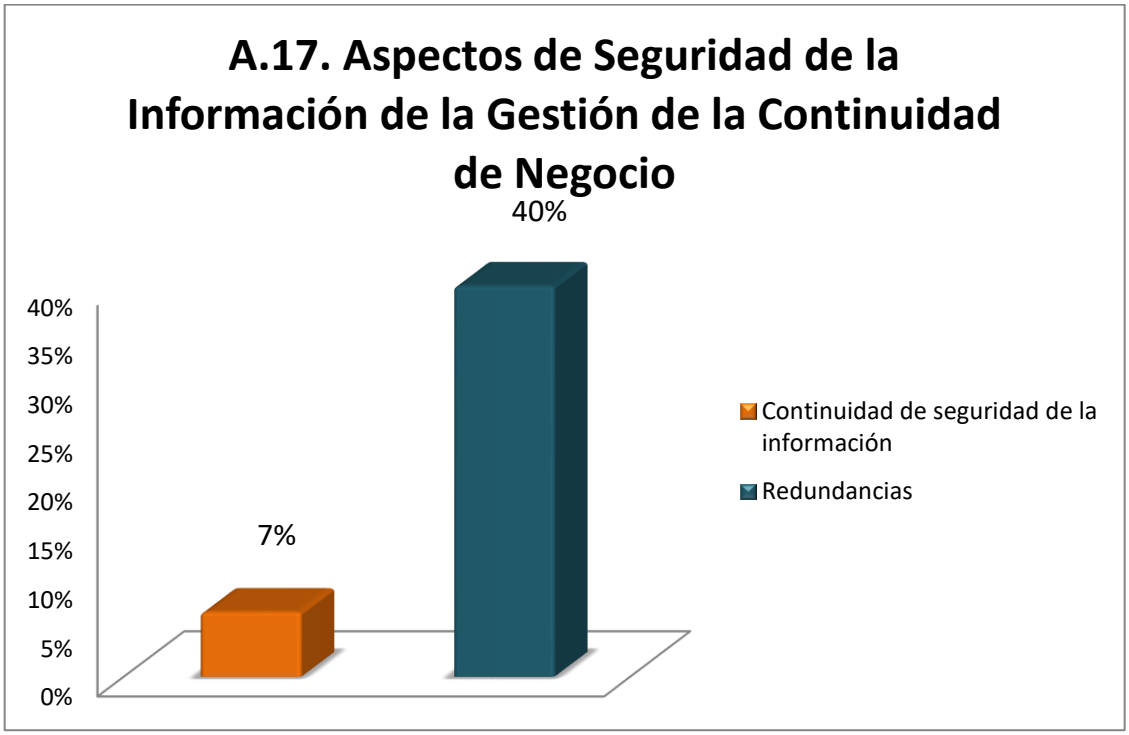
El objetivo es asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

En este punto, la Entidad tiene definida en el numeral 10.0 la “Política de Gestión de Incidentes de la información”, en el “Manual de las Políticas de la Seguridad y la Privacidad de la Información”.

Sin embargo, la Entidad no ha diseñado, formalizado e implementado procedimientos, para reportar los eventos de la Seguridad de la Información, donde los usuarios puedan reportarlos y tampoco se cuenta con procedimiento para reportes de eventos de debilidades de los sistemas, servicios y redes.

No se evidenciaron mecanismos para cuantificar y monitorear los tipos, los volúmenes y los costos de los incidentes de la Seguridad de la Información.

A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO, Cumplimiento: 23%.



El objetivo en este punto, es que la Entidad esté debidamente preparada ante la presentación de un siniestro y se pueda recuperar eficientemente.

En este aspecto, se evalúan dos puntos a saber:

1. Continuidad de Seguridad de la Información: Se tiene la Política definida con lineamientos claros en el numeral: 9.9 : “Política de Gestión de Continuidad del Negocio, sin embargo se identificó que actualmente no se tiene implementado un BCP (Plan de Continuidad del Negocio), que permita apoyar las estrategias de todas las dependencias de la Entidad.

Se encontró además que actualmente se cuenta con un DRP (Plan de Restauración ante Desastres), sin embargo no hay evidencias que demuestren que haya sido puesto en prueba.

No se cuenta con un documento BIA (Análisis de Impacto del negocio), de igual forma la descripción de la infraestructura del Centro de computo alterno formalmente documentado, en el cual se determinen proceso que son esenciales para la continuidad de las operaciones de la Entidad.

Dado que no se implementa un BIA, se establece que no se ha definido una Matriz de Riesgos VS. Controles en donde se identifiquen y analicen las posibles amenazas y/o vulnerabilidades de personas, sistemas, infraestructura y procesos que podrían ocasionar riesgo de continuidad para la Entidad.

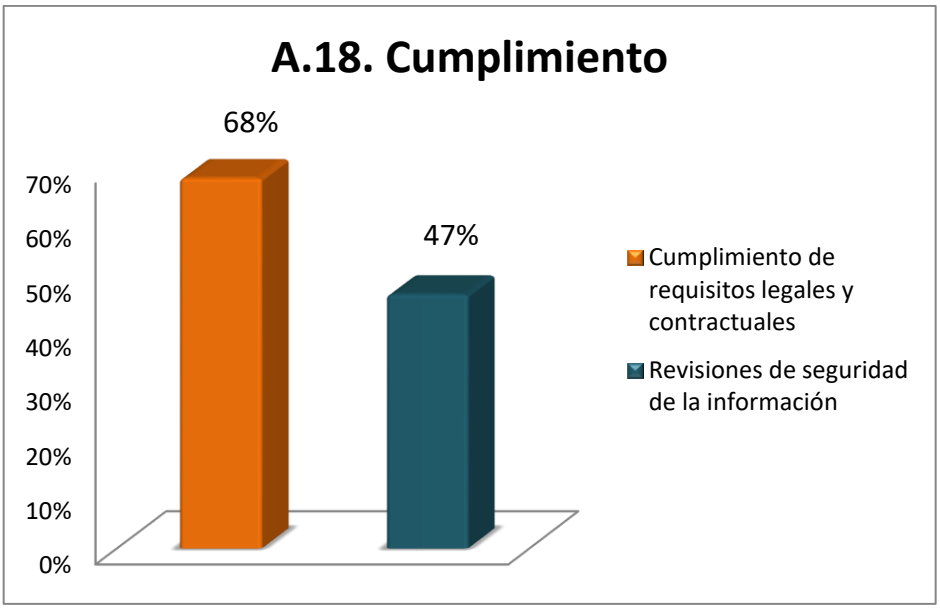
No se cuenta con la matriz donde se registren los riesgos de operación (Matriz SARO: Sistema de Administración de Riesgos Operativos) y los riesgos de TI. Estos servirán para determinar el Plan de Contingencias.

Se evidencio, que no se cuenta con un sitio alterno de operaciones (con cubrimiento tecnológico, operativo y de funciones), que permita tener continuidad de las Operaciones en caso de contingencia.

Dado que la Entidad no tiene documentado el Plan de Continuidad del Negocio, no se puede hablar de la implementación de dicho plan, ni tampoco de la revisión periódica del mismo, por esto la calificación actual en ambos subdominios es 0%.

2. Redundancias, en las instalaciones de procesamiento de información no se han implementado controles con redundancia para cumplir todos los requisitos de disponibilidad, según el Plan de Continuidad del Negocio.

A.18. CUMPLIMIENTO, 57%



El Objetivo en este punto es: evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad. En este punto, se evalúan 2 puntos a saber:

1. Cumplimiento de Requisitos Legales y Contractuales: Se tiene la Política de Cumplimiento en el numeral 10.2: del Manual de las Políticas de la Seguridad y la Privacidad de la Información, donde se define claramente las Políticas y los lineamientos respecto al cumplimiento de requisitos legales y contractuales, incluyendo los derechos a la propiedad intelectual, la Protección de registros, la Privacidad y protección de información de datos personales.

Se evidencio, que la Entidad no está usando los controles criptográficos que cumplan con los acuerdos, leyes y reglamentos dispuestos por TRANSMILENIO S.A.

2. Revisiones de Seguridad de la Información: Se realizan revisiones independientes a la Seguridad de la Información, sin embargo, no se videncia que estas revisiones, se estén realizando a intervalos planificados o cuando ocurran cambios significativos.

CONCLUSIONES Y RECOMENDACIONES

1. La alta Dirección de TRANSMILENIO S.A., como responsable Institucional de la Política de Gobierno Digital y sus ejes articuladores, entre los que se cuenta la seguridad de la información, apoya la implementación del Sistema de Gestión de Seguridad de la Información, dando los lineamientos, respecto a la implementación del Sistema de Gestión de la Seguridad de la Información, y actividades definidas tanto para la Dirección de TIC, como para las demás áreas de la Entidad, incluyendo todos los usuarios de los Sistemas de Información de la Entidad.

Dado el análisis GAP de la Entidad, se denota madurez alcanzado en algunos dominios de la Norma como: “Política de la Seguridad y la Privacidad de la Información”, “Organización de la Seguridad de la Información” y “Seguridad de los Recursos Humanos”, sin embargo también se denota un muy bajo avance en otros dominios, como por ejemplo: “Adquisición, Desarrollo y Mantenimiento de Sistemas”: 19%, “Relaciones con los Proveedores”: 17%, “Gestión de Incidentes de Seguridad”: 20% y “Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio”: 23%

En concordancia con las evidencias obtenidas se puede concluir sobre la implementación del Sistema de Seguridad de la Información SGSI en la Entidad, que de los 114 controles exigidos en el Anexo A de la NTC-ISO 27001: 2013, el nivel de madurez alcanzado por TRANSMILENIO S.A. a 31 mayo de 2019, es del 49%, lo que significa que de acuerdo a la escala de cumplimiento definida en el análisis GAP, la Entidad está levemente por encima del nivel “Repetible” (40%) es decir, que los procesos se han desarrollado hasta un punto en el cual procedimientos similares son utilizados por personas diferentes para llevar a cabo la misma tarea, aun cuando estos no se encuentran totalmente documentados.

Con lo anterior a continuación se presentan recomendaciones encaminadas al logro de la Implementación del SGSI en la Entidad:

2. Elaborar, documentar, y socializar Matriz de Usuarios y Perfiles de los sistemas de información con que cuenta la Entidad.

- Distribución de Funciones: Están establecidas separaciones entre las funciones y las áreas de responsabilidad para reducir las oportunidades de la modificación no autorizada o uso inadecuado de los activos de información, con el directorio activo se dividen las tareas de acuerdo con el tipo de perfil, el cargo y los accesos a las aplicaciones de la entidad. Sin embargo, no se evidenció tener la formalización de los Usuarios y los Perfiles.

3. Incluir contactos con grupos de interés especial, como por ejemplo otras entidades del Distritales, Nacional, Instituto ISO y Alta Consejería Distrital.

- Contactos con grupos de interés especiales: La Entidad mantiene contacto con grupos de interés, foros de especialistas en seguridad o en asociaciones profesionales, se tiene establecido en el Manual de Políticas de Seguridad y Privacidad de la Información: M-DT-001, versión 3 de Abril de 2019 y se cuenta con acceso al reporte de: Kaspersky, TRAPS: PaloAlto, Microsoft, y Fortinet, no obstante no se cuenta con contactos que pueden servir de apoyo tales como entidades de orden Nacional, Distrital, y del sector privado.

4. Integrar la seguridad de la información en el ciclo de vida de los proyectos para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto.

- En materia de gestión de proyectos, se evidenció que la Entidad no ha integrado la seguridad de la información en el ciclo de vida de los mismos, con el fin de asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto.

5. Dar cumplimiento al procedimiento y/o política definidos en materia de Teletrabajo.

- La entidad no ha implementado el procedimiento y/o lineamientos definidos en Teletrabajo.

6. Aagilizar la obtención de la lista de todos los activos de la información de la Entidad, de modo tal que se tengan registrados la totalidad de: Información, Hardware, Software, Servicios de TI, Conocimiento y la ubicación.

- Si bien se encuentra en construcción, al corte del presente documento, no ha sido formalizada.
- No se evidenciaron registros sobre la aplicación de las políticas definidas por la entidad en materia de gestión de Activos.

7. Diseñar, elaborar el implementar un procedimiento que defina lineamentos sobre la eliminación de los activos de información, cuando ya no son requeridos.

- No se evidenciaron procedimientos formalizados respecto a cumplir dichos lineamientos.

8. Diseñar, elaborar el implementar un procedimiento para la asignación y uso de privilegios a los usuarios de los Sistemas de Información, así como para revisión periódica de los derechos de acceso a usuarios.

- La Entidad no cuenta con un documento formal para la asignación y uso de privilegios a los usuarios de los Sistemas de Información (privilegios asignados con base a requerimientos necesarios para su desempeño), tampoco con un procedimiento documentado para la revisión periódica de los derechos de acceso a usuarios.

9. Dar cumplimiento a las Políticas definidas en el Manual de las Políticas de la Seguridad y la Privacidad de la Información, respecto al uso de la Criptografía en la Entidad.

- No se evidencio un procedimiento para el uso, protección y tiempo de vida de las llaves criptográficas.

10. Diseñar, elaborar e implementar procedimientos para: el retiro de equipos, información o software que requiera previa autorización, procedimiento para la seguridad de los equipos que se encuentran fuera de las instalaciones, teniendo en cuenta los diferentes riesgos que esto conlleva y procedimiento para la disposición segura o reutilización de equipos.

- No se evidenciaron elaborados, diseñados ni implementados los documentos mencionados.

11. Definir los Procedimientos de operación requeridos para la mejora continua del sistema de gestión de seguridad de la información, así mismo deben estar documentados, publicados y socializados.

- No se evidenciaron elaborados, diseñados ni implementados los documentos mencionados.

12. Elaborar, formalizar, socializar e implementar el documento de gestión de la capacidad para asegurar el desempeño requerido del sistema, hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.

13. Diseñar, elaborar e implementar procedimientos para: gestión de la capacidad, para asegurar el desempeño requerido del sistema, procedimiento encaminado a revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información, tampoco se evidencia un procedimiento para revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

- No se evidenció implementación de los documentos mencionados.

14. Diseñar, elaborar e implementar procedimientos mediante los cuales: se definan los pasos para evaluar la exposición de la organización a vulnerabilidades y para cuando el desarrollo de Software

es subcontratado en la Entidad, con el fin de que se definan los detalles para proteger, supervisar y monitorear el desarrollo de esta actividad.

- No se evidenció implementación de los documentos mencionados.

15. Diseñar, elaborar e implementar procedimientos, para reportar los eventos de la Seguridad de la Información, donde los usuarios puedan reportarlos y procedimiento para reportes de eventos de debilidades de los sistemas, servicios y redes, así como mecanismos para cuantificar y monitorear los tipos, los volúmenes y los costos de los incidentes de la Seguridad de la Información

- No se evidenció implementación de los documentos mencionados.

16. Implementar las políticas definidas en materia de Continuidad del negocio.

- No se tiene implementado un BCP (Plan de Continuidad del Negocio), que permita apoyar las estrategias de todas las dependencias de la Entidad, se cuenta con un DRP (Plan de Restauración ante Desastres), sin embargo no hay evidencias que demuestren que haya sido puesto en prueba, no se cuenta con un documento BIA (Análisis de Impacto del negocio), de igual forma la descripción de la infraestructura del Centro de computo alterno formalmente documentado, en el cual se determinen proceso que son esenciales para la continuidad de las operaciones de la Entidad, Dado que no se implementa un BIA, se establece que no se ha definido una Matriz de Riesgos VS. Controles en donde se identifiquen y analicen las posibles amenazas y/o vulnerabilidades de personas, sistemas, infraestructura y procesos que podrían ocasionar riesgo de continuidad para la Entidad y no se cuenta con la matriz donde se registren los riesgos de operación (Matriz SARO: Sistema de Administración de Riesgos Operativos) y los riesgos de TI. Estos servirán para determinar el Plan de Contingencias, no se cuenta con un sitio alterno de operaciones (con cubrimiento tecnológico, operativo y de funciones), que permita tener continuidad de las Operaciones en caso de contingencia.

Cualquier aclaración adicional, con gusto será suministrada.

Bogotá D.C., 28 Junio 2019

Oscar Pulgarín Lara

Jefe Oficina de Control Interno (E)

Elaboró: Jorge Iván Flórez, Auditor Contratista - Oficina de Control Interno.