MEMORANDO INTERNO	
Para	**Ing. Felipe A. Ramírez Buitrago** Gerente General
De	**Luis Antonio Rodríguez Orozco** Jefe Oficina de Control Interno
Asunto	Informe No. OCI-2020- 037 Seguimiento a la Implementación del Sistema de Gestión de Seguridad de la Información - SGSI en TRANSMILENIO S.A.

Respetado Ingeniero Ramírez:

La Oficina de Control Interno como parte del Plan de Auditorías para la vigencia 2020 y en su rol de enfoque hacia la prevención, ha realizado el Seguimiento a la Implementación del Sistema de Gestión de Seguridad de la Información - SGSI en TRANSMILENIO S.A. Dentro del informe del asunto se incluyen conclusiones y recomendaciones, entre las cuales destacamos:

1. Estructurar y reforzar los procedimientos para la continuidad del negocio, esto es, revisar y documentar un BIA (Análisis del Impacto del Negocio) , con base en este ajustar el BCP (Plan de continuidad del negocio) y así obtener un DRP (Plan de recuperación ante desastre) fuerte, a fin de que la Entidad cuente con los riesgos asociados al tema enunciado, se encuentre preparada y de efectiva respuesta ante la continuidad del negocio, especialmente de cara a los centros de control, tanto de BUSES como de BRT, ya que se encuentran vulnerables y no se cuenta, con un plan de contingencia para operar de otra manera (Dominio A.17).
2. Se recomienda tomar acciones oportunas, para que las debilidades identificadas, 31% de los dominios, alcancen el nivel de madurez deseado, en procura de mejorar su porcentaje de cumplimiento y robustecer a la Entidad en el Sistema de Seguridad de la Información.

TRANSMILENIO S.A.
Avenida Eldorado No. 69 - 76
Edificio Elemento - Torre 1 Piso 5
PBX: (57) 2203000
FAX: (57) 3249870 - 80
Código postal: 111071
www.transmilenio.gov.co
Información: línea 4824304

3. Realizar las acciones tendientes al cumplimiento de la normatividad expedida por la Entidad (Manual de Políticas de Seguridad Numeral 9,5 y el procedimiento P-DT-016 numeral 6) para dar cumplimiento a lo referente a Instalación de Software tal como se describe en el informe de Derechos de Autor de la presente vigencia.
4. Se recomienda adelantar la gestión para la implementación de un protocolo de retorno de funcionarios a la Entidad e incluir en él temas como el recibo de equipos, verificación de los mismos, cómo se realizarán las copias de seguridad, incorporación de información a los repositorios de la Entidad, entre otros.

Cualquier información adicional con gusto será suministrada.

Cordialmente,

LUIS ANTONIO RODRIGUEZ OROZCO
Jefe Oficina de Control Interno

Anexo: Dieciocho (18) folios

Copia: Dra. Maria Fernanda Ortiz Carrascal, Subgerente General
Dra. Tatiana García Vargas, Subgerente Jurídica (E)
Dr. Álvaro José Rengifo Campo - Subgerente Económico
Dr. Nicolás Adolfo Correal Huertas- Subgerente Técnico y de Servicios
Dra. Yolima Pérez Ariza, Subgerente de Atención al Usuario y Comunicaciones
Dra. Sofia Zarama Valenzuela- Jefe de la Oficina Asesora de Planeación, Subgerente de Desarrollo de Negocios(E)
Dr. José Guillermo Del Río Baena, Director Corporativo

OCI – 123- 2020 / 01 de julio de 2020

Elaboró: Oscar Pulgarin Lara, Profesional Universitario Oficina Control Interno
Revisó: Luz Marina Díaz Ramírez, Contratista Oficina de Control Interno

TRANSMILENIO S.A.
Avenida Eldorado No. 69 - 76
Edificio Elemento - Torre 1 Piso 5
PBX: (57) 2203000
FAX: (57) 3249870 - 80
Código postal: 111071
www.transmilenio.gov.co
Información: línea 4824304

N° INFORME: OCI-2020-xx

PROCESO / ACTIVIDAD REALIZADA: Seguimiento a la Implementación del Sistema de Gestión de Seguridad de la Información - SGSI en TRANSMILENIO S.A.

EQUIPO AUDITOR: Oscar Pulgarin Lara, Profesional Universitario Grado 4

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 y la Ley 1712 de 2014 Protección de Datos Personales, Transparencia y Acceso a la Información Pública, Guía de auditoría No.10 Seguridad y Privacidad de la Información (MINTIC).

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 2019 y marzo 31 de 2020, para los 14 dominios de la norma NTC-ISO-IEC 27001:2013.

CRITERIOS:

1. Norma NTC-ISO-IEC 27001: 2013
2. Ley 1712 de 2014 Ley de Transparencia y del Derecho de Acceso a la Información Pública
3. Ley 1581 de 2012, Ley de Protección de Datos Personales
4. Manual de Políticas de la Seguridad y Privacidad de la Información de TMSA M-DT-001 Versión 3 de abril de 2019.
5. Formatos, Manuales, Procedimientos, Instructivos, Protocolos del MIPG de TMSA
6. Guía de auditoría No.10 Seguridad y Privacidad de la Información (MINTIC)
7. Seguimiento a las recomendaciones efectuadas por la Oficina de Control Interno mediante informe OCI-2019-055

DESCRIPCIÓN DEL TRABAJO REALIZADO:

El siguiente informe describe un análisis GAP (cuestionario que permite tener una percepción de la brecha entre expectativas y la realidad con el fin de mejorar continuamente) del estándar ISO 27001:2013, el cual fue aplicado por la Oficina de Control Interno en la Entidad (Dirección de TIC) y que contempla diversos aspectos que se deben tener en cuenta como buenas prácticas para la seguridad de la información y permite además, verificar el grado de cumplimiento que se tiene actualmente, con respecto al anexo de la mencionada norma. Para esto se solicitó mediante correo electrónico del 13 de mayo de 2020 a la Dirección de TIC, el diligenciamiento del anexo y que aportara las evidencias correspondientes. De acuerdo con lo anterior, la Dirección de TIC respondió por la misma vía el 20 de mayo de 2020, anexando una serie de documentos, los cuales fueron analizados y valorados por la Oficina de Control Interno, lo que permitió la determinación del grado de avance en la implementación del SGSI en la entidad.

VALORACIÓN

Para conocer el estado de avance o implementación de los controles que se evalúan, la herramienta Diagnóstico GAP cuenta con una descripción de seis (6) estados tal como se muestra en la siguiente tabla calorimétrica:

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.

Fuente: Diagnóstico GAP de IEC 27001 2013 diligenciado por la Dirección de TIC el 20 de mayo de 2020

SITUACIÓN ENCONTRADA

La herramienta cuenta con una serie de dominios y subdominios que a medida que se evalúan los controles establecidos para cada uno de ellos se define un valor de cumplimiento en porcentaje. Para el caso de TRANSMILENIO S.A., el resultado arrojado en cada dominio es el siguiente:

Item	Dominios	Cumplimiento
5	POLÍTICA DE SEGURIDAD	95%
6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	64%
7	SEGURIDAD DE LOS RECURSOS HUMANOS	75%
8	GESTIÓN DE ACTIVOS	61%
9	CONTROL DE ACCESO	83%
10	CRIPTOGRAFÍA	75%
11	SEGURIDAD FÍSICA Y DEL ENTORNO	71%
12	SEGURIDAD DE LAS OPERACIONES	65%
13	SEGURIDAD DE LAS COMUNICACIONES	62%
14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	60%
15	RELACIONES CON LOS PROVEEDORES	68%
16	GESTIÓN DE INCIDENTES DE SEGURIDAD	61%

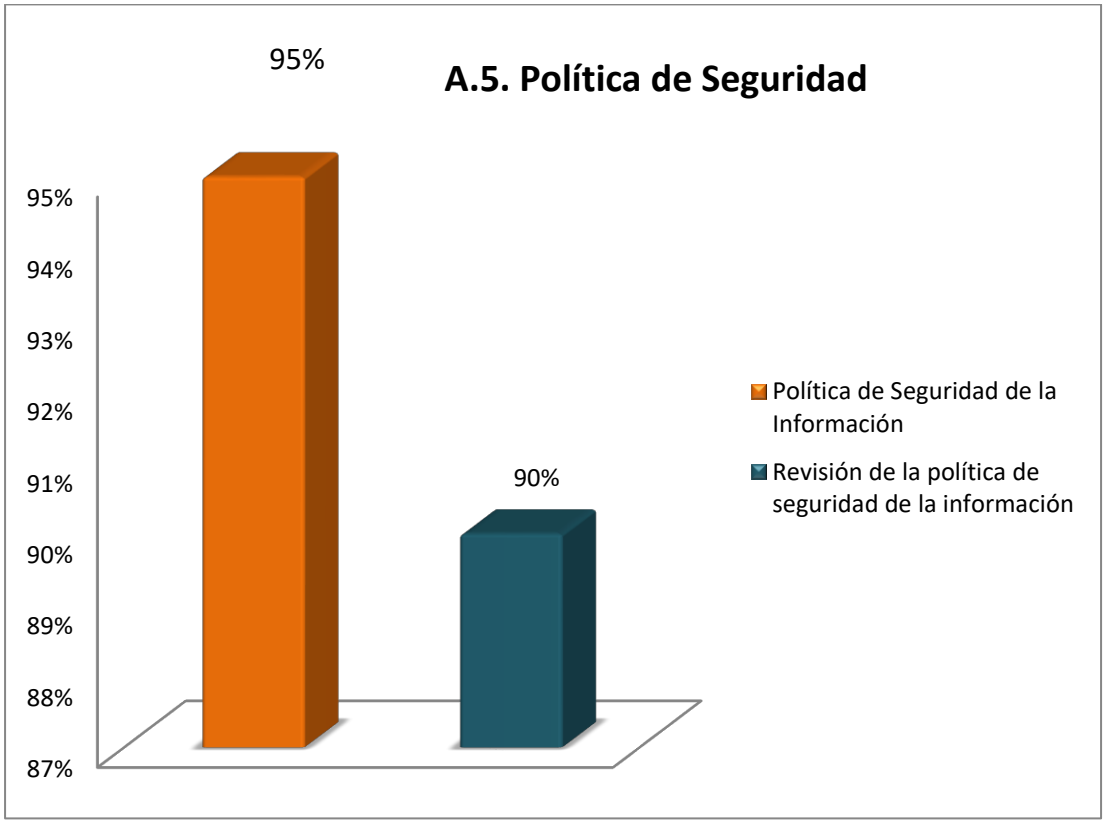
17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	48%
18	CUMPLIMIENTO	81%
TOTAL		69%

Fuente: Diagnóstico GAP de IEC 27001 2013 hoja de cálculo Rep_SubDom con fecha de diligenciamiento por la OCI del 4 de junio de 2020

ANÁLISIS DE NIVELES DE MADUREZ ALCANZADO POR CADA UNO DE LOS DOMINIOS

A continuación, se describe el nivel de porcentaje alcanzado por cada uno de los dominios, según lo analizado y evidenciado por la Oficina de Control Interno, y se hacen las respectivas recomendaciones:

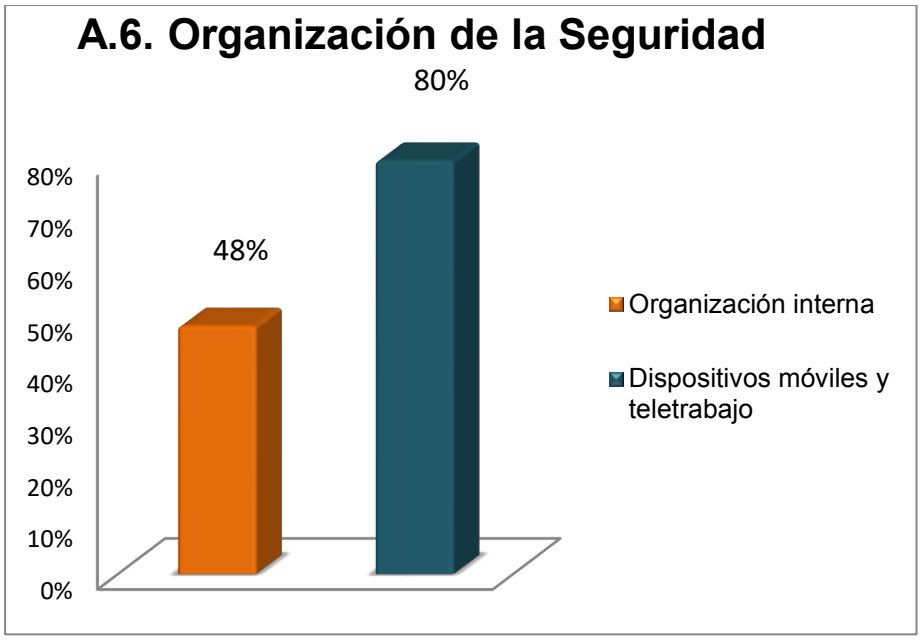
A.5. Política de Seguridad: Cumplimiento: 95%



POLÍTICA DE SEGURIDAD

Política de Seguridad de la Información	OBSERVACIÓN Y RECOMENDACIÓN
Documento de la política de seguridad de la información	Se cuenta con el Manual M-DT-001 Políticas de seguridad y privacidad de la información Disponible en https://www.transmilenio.gov.co/publicaciones/150328/anexo-3-m-dt-001-politicas-de-seguridad-de-la-informacion/ -Socialización: Se cuenta con el Plan de Cultura y Sensibilización en Seguridad de la información. Este Plan está Publicado en la Intranet y adicionalmente tiene una nueva actualización que próximamente será Publicada, según lo manifestado por la Dirección de TIC, se encuentra en poder de la OAP para publicación. Se recomienda realizar una revisión integral de la Política de Seguridad teniendo como marco las actuales circunstancias que afectan a la Entidad, a raíz de la pandemia por el COVID-19 teniendo en cuenta las disposiciones que ha expedido el Gobierno Nacional y Distrital. Se recomienda una socialización más frecuente utilizando los diferentes canales con que cuenta la Entidad para lograr fijación e interiorización de ésta.
Revisión de la política de seguridad de la información	La última actualización al Manual Políticas de Seguridad de la Información M-DT-001 V3 aparece con fecha 26 de marzo de 2019. Se recomienda la revisión y actualización, teniendo en cuenta la recomendación anterior.

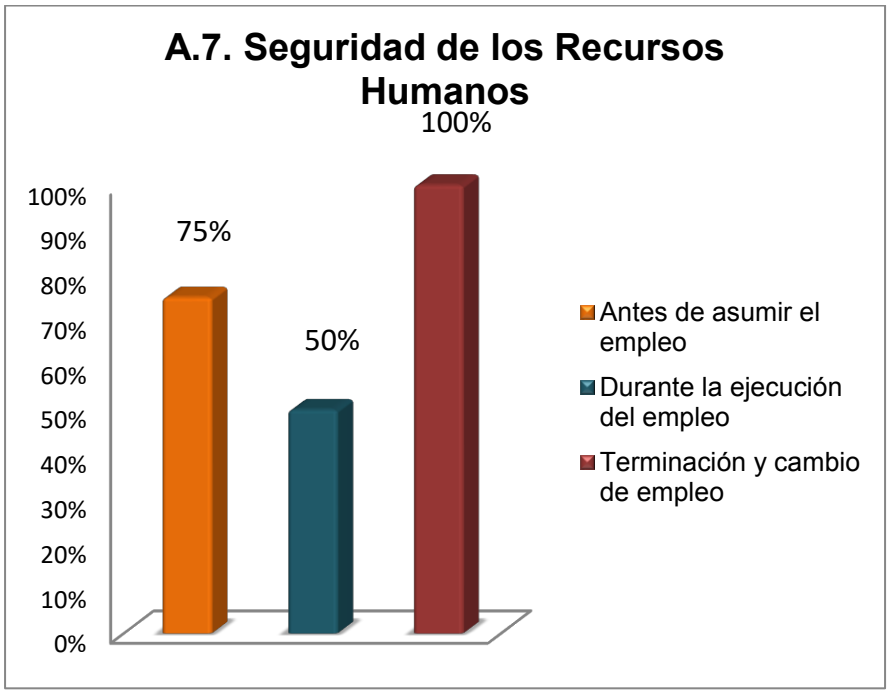
A6. Organización de la Seguridad. Cumplimiento: 64%



ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	OBSERVACIÓN Y RECOMENDACIÓN
Organización Interna	
Asignación de responsabilidades para la seguridad de la información	El manual M-DT-001 con tiene la política general que deben cumplir la entidad en cuanto a seguridad de la Información. Las responsabilidades se encuentran definidas en el Manual del SGSI el cual contiene los roles y responsabilidades de seguridad de la información. Este documento está en proceso de construcción Se adjunta el borrador como anexo. Se recomienda agilizar la oficialización del documento borrador Manual del Sistema de Gestión de Seguridad de la Información ya que es en éste en donde se especifican cada una de las responsabilidades. Lo anterior en razón a que falta la oficialización y respectiva implementación
Distribución (segregación) de funciones	Las responsabilidades se encuentran definidas en el Manual del SGSI el cual contiene los roles y responsabilidades de seguridad de la información. -El inventario de activos de información establece la dependencia responsable y la dependencia que custodia los activos. -Los sistemas de información manejan perfiles de acuerdo con el rol y las responsabilidades de cada usuario. Disponible en https://www.transmilenio.gov.co/publicaciones/150328/anexo-3-m-dt-001-politicas-de-seguridad-de-la-informacion/ Se recomienda, actualizar y publicar la Matriz de activos de información de acuerdo con la normativa vigente.
Contacto con las autoridades	Se cuenta con el "Instructivo Contacto con autoridades externas y grupos de interés". En revisión y publicación por la OAP. Se recomienda Gestionar con la OAP la oficialización del documento. El borrador del anexo tiene fecha de septiembre de 2019.
Contactos con grupos de interés especiales	Según lo indicado por la Dirección de TIC, Transmilenio hace parte del Comando Conjunto de Operaciones Cibernéticas CCOC de Las fuerzas militares del sector Transporte. -Se cuenta con suscripción a boletines de Ciberseguridad del Centro Cibernético Policial, estas suscripciones se pueden evidenciar en el correo de Seguridaddigital@transmilenio.gov.co
Seguridad de la información en gestión de proyectos	El control se encuentra en etapa de diseño y aún no se ha implementado. Se está iniciando con la verificación de esta actividad en la Dirección de TIC. Considerando que el seguimiento realizado en el año 2019 este Ítem no se había desarrollado, se recomienda acelerar su implementación teniendo en cuenta las recomendaciones que se dieron en esa oportunidad

Dispositivos móviles y teletrabajo	
Política para dispositivos móviles	Se tiene la política de seguridad para dispositivos Móviles dentro del M-DT-001. -Se implementa la política con Bloqueo de medios removibles (kaspersky y TRAPS), Acceso de portátiles y dispositivos móviles a red WIFI. Los lineamientos de teletrabajo aplican solamente para Trabajadores Oficiales y empleados públicos, más no para los contratistas. Se recomienda realizar una revisión a la documentación existente y actualizarla de acuerdo con lo que se está viviendo actualmente con la contingencia a raíz del Coronavirus. Creación de protocolos de seguridad para el descargue de la información, utilización de memorias USB, escritorios virtuales, procedimiento para la utilización de equipos de cómputo tanto de propiedad de la Entidad, como en alquiler para los equipos que fueron llevados a las casas de los funcionarios. -Se cuenta con las políticas de seguridad para teletrabajo dentro del M-DT-001. -Se cuenta con el procedimiento P-DA-010 Teletrabajo en TRANSMILENIO S.A. y su respectivo formato R-DA-124 Solicitud de Teletrabajo. Disponible en https://www.transmilenio.gov.co/publicaciones/150328/anexo-3-m-dt-001-politicas-de-seguridad-de-la-informacion/ No obstante, en la Entidad no se aplica el teletrabajo de acuerdo con lo definido en la normativa vigente Distrital.
Teletrabajo	

A.7 Seguridad de los Recursos Humanos: Cumplimiento 75%

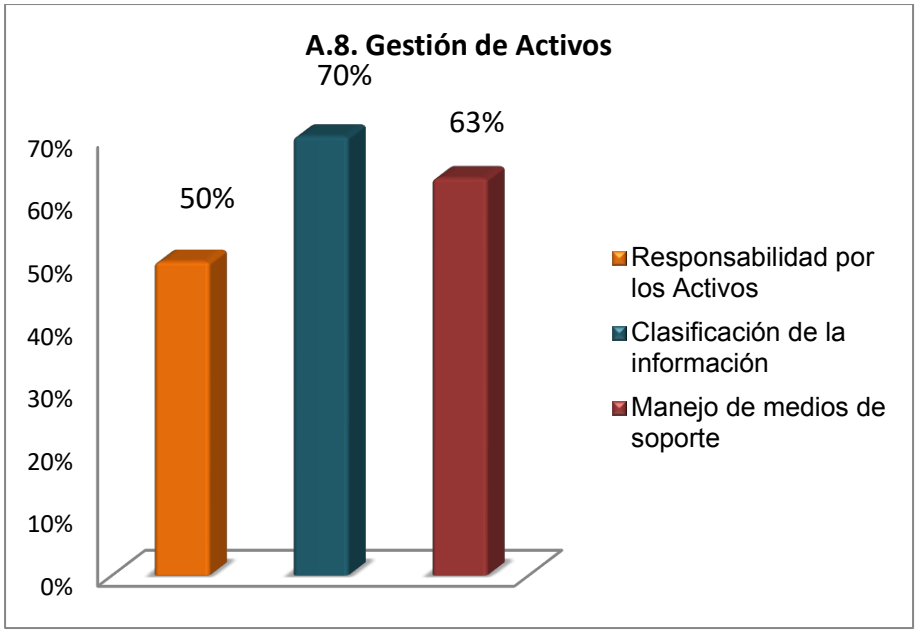


SEGURIDAD DE LOS RECURSOS HUMANOS	
Antes de Asumir el Empleo	**OBSERVACIONES Y RECOMENDACIONES**
Selección	Se tiene el procedimiento de investigación de antecedentes de funcionarios (P-DA-001). Disponible en la intranet de la Entidad. Se tiene el procedimiento de Selección e investigación de antecedentes de contratistas (MSJ-001). Está pendiente hacer un seguimiento y revisión de este procedimiento para ver si requiere alguna actualización adicional Se recomienda una revisión de los documentos e incluir en ellos temas como: - Información crediticia - Antecedentes penales Además, se recomienda crear un control para determinar el nivel de cumplimiento y aplicación de las directrices relacionadas en los procedimientos y demás documentos
Términos y condiciones del empleo	Se cuenta con una cláusula de confidencialidad en los contratos actuales. De igual forma se incluye en los contratos la obligación relacionada con el cumplimiento de las políticas de los sistemas

	de gestión, en este caso, las políticas del SGSI. De igual forma esto se cubre con el cumplimiento de las leyes 1712, ley de transparencia. 1581 Hábeas Data que deben cumplirse a cabalidad por ser ciudadanos. Se recomienda estar verificando las mismas, teniendo en cuenta las actuales circunstancias por las que atraviesa actualmente el país.
Durante la Ejecución del Empleo	
Responsabilidades de la dirección	Para el 2020 no se han programado capacitaciones y/o sensibilizaciones en materia de Seguridad de la Información. Se recomienda la verificación, actualización y divulgación de la política y del Plan de Cultura y Sensibilización del Sistema de Gestión de la Seguridad de la información. Hecha la consulta con la Dirección Corporativa sobre el tema, se informó mediante correo electrónico de fecha 3 de junio que para el año 2020 la Dirección de TIC no ha programado el tema de seguridad de la información para capacitaciones.
Toma de conciencia, educación y formación en la seguridad de la información	El área de Talento Humano tiene el plan de capacitación. Durante el 2020 se han realizado varias charlas de sensibilización tanto a contratistas como a directores de áreas. en el 2019 se realizó a los influenciadores. La información está a cargo de Talento Humano. Realizada la consulta, a la fecha no existe ni plan de capacitación ni sensibilización, sobre el tema. Se recomienda definir con el área de capacitación lo referente a la sensibilización en materia de seguridad de la información. Realizada la consulta, a la fecha no existe ni plan de capacitación ni sensibilización De igual forma trabajar con el área de comunicación interna y transmitir los tips necesarios. Tener presente para este control la recomendación anterior. Si bien la Dirección de TIC ha adelantado sensibilizaciones, no se ha evaluado el grado de interiorización de las políticas de seguridad de la información
Proceso disciplinario	Se cuenta con un procedimiento de asuntos Disciplinarios. Se hace a través del cumplimiento de la ley 734, la cual incluye cualquier violación a la información de la entidad.
Terminación o Cambio de la Relación Laboral	
Terminación o cambio de responsabilidades de empleo	Se cuenta con una cláusula de confidencialidad en los contratos actuales. De igual forma se incluye en los contratos la obligación relacionada con el cumplimiento de las políticas de los sistemas de gestión, en este caso, las políticas del SGSI. La cláusula tendrá una vigencia de la confidencialidad posterior a la terminación del contrato. Para constar el cumplimiento se verificaron los contratos de Prestación de Servicios:

	Cto. 248-19 Cto. 312-19 Cto. 716-19 Cto. 359-20 Cto. 379-20 y se evidenció la inclusión de la cláusula de confidencialidad

A8. Gestión de Activos: Cumplimiento 61%

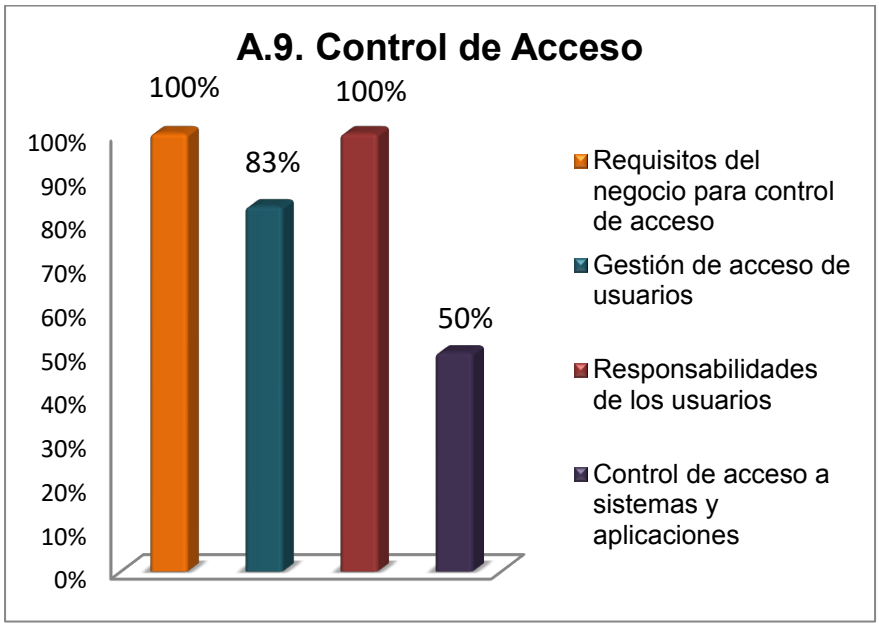


GESTIÓN DE ACTIVOS	OBSERVACIONES Y RECOMENDACIONES
Responsabilidad por los Activos	
Inventario de Activos	Se cuenta con la política de activos de información dentro del manual de políticas de seguridad, Disponible en la intranet.
Propiedad de los activos	Se cuenta con el Instructivo de identificación y clasificación de activos de información. De igual forma se tiene diligenciada la Matriz de inventario de activos. ´ Se recomienda, actualizar y publicar la Matriz de activos de información de acuerdo con la normativa vigente. Se recomienda la revisión y si es procedente la actualización del Manual de Políticas de Seguridad de la Información M-DT-001 V3, la versión publicada corresponde a abril de 2019

	teniendo en cuenta las circunstancias que se vienen presentado a raíz de la emergencia por el COVID-19. Se recomienda igualmente revisar periódicamente y mantener actualizada la matriz de activos de información tal como se recomendó en el informe OCI-2019-074
Uso aceptable de los activos	Se tienen las políticas de TI que forman parte del PETI, publicadas en la intranet. De igual forma el Manual M-DT-001 indica esta información. Se recomienda la actualización de los documentos aportados como evidencia teniendo en cuenta las circunstancias que se están presentando a raíz de la emergencia por el COVID-19. Tener muy presente el Teletrabajo, el Trabajo en casa, los Backups, la implementación de escritorios virtuales, etc. Se deben realizar campañas de socialización recalcando el uso correcto de los activos que le han sido asignado a cada funcionario.
Devolución de activos	Consultado el sitio MIPG de la Dirección Corporativa, lo único existente para este tema es el formato R-DA-059 Acta de entrega puesto de trabajo, Se recomienda que en conjunto con la Dirección Corporativa y la Dirección de TIC se cree un control fuerte para la devolución de los activos por parte de los funcionarios, en donde se incluyan los que se facilitaron a los funcionarios con ocasión del confinamiento.
Clasificación de la Información	
Clasificación de la Información	-Se cuenta con la política de activos de información dentro del manual de políticas de seguridad, publicada en la intranet. Se define el etiquetado en el Instructivo de identificación y clasificación de activos. El etiquetado se está implementando en T-DOC (ya hay carpetas que cuentan con las etiquetas) y se está implementando a nivel físico en Archivo. Está pendiente hacer la clasificación en el servidor de archivos con estas etiquetas. Se cuenta con el Instructivo de identificación y clasificación de activos de información De acuerdo con el informe OCI -2019-074 la matriz de activos de la información, está desactualizada. Se recomienda la revisión y actualización de los documentos aplicables teniendo en cuenta la actual situación por la emergencia a raíz del COVID-19. Se recomienda igualmente la actualización de la matriz de activos de información tal como se solicitó en el informe OCI-2019-074
Etiquetado y manejo de la información	
Manejo de activos	
Manejo de medios de soporte	
Gestión de medios de soporte removibles	Se cuenta con el Protocolo T-DT-003 Gestión de medios removibles.

	Se recomienda su revisión y si es procedente su actualización teniendo en cuenta las actuales circunstancias. Se recomienda hacer seguimiento a su cumplimiento. Lo anterior teniendo en cuenta, que, si bien se cuenta con el mencionado procedimiento y con un sistema de información que no permite acceder a puertos USB o CD removibles, se tiene una brecha, en cuanto a que fue habilitado el uso de OneDrive para transmitir, consultar y descargar información desde sitios diferentes a la Entidad.
Disposición de los medios de soporte	Se tiene el procedimiento de borrado seguro en borrador. Adicional, se cuentan con políticas dentro del Manual M-DT-001 que indican la disposición de medios Se recomienda la pronta implementación del procedimiento de borrado seguro para así dar cumplimiento al control.
Transferencia de medios de soporte físicos.	Se cuenta con el procedimiento P-DT-012. Intercambio seguro de información Se recomienda revisar y hacer ajuste del documento aportado teniendo en cuenta las circunstancias actuales por la emergencia del COVID-19. Adicionalmente, tener en cuenta la recomendación dada por la OCI en el informe OCI-2019-074 con relación a definir y/o formalizar un procedimiento de cambios para la plataforma del SIRCI que incorpore todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción

A9. Control de Acceso. Cumplimiento:83%



CONTROLES	OBSERVACIONES Y RECOMENDACIONES
CONTROL DE ACCESO	
Requisitos del negocio para control de acceso	
Política de control de acceso	Se cuenta con el Manual M-DT-001 Políticas de seguridad y privacidad de la información el numeral 8.5.1. Gestión de la seguridad de las redes. Adicional a esto se tienen controles de VLANs, usuarios del directorio activo, permisos a nivel de aplicaciones, Se solicito evidencia y se entregó por parte de TIC mediante correo del 12 de junio de 2020 el directorio activo en donde se diferencia quienes están autorizados como administradores y quienes como funcionarios normales. Se recomienda realizar una revisión integral de la Política de Seguridad teniendo como marco las actuales circunstancias que afectan a la Entidad en materia de informática a raíz de la pandemia por el COVID-19. Actualizar de acuerdo con las directrices impartidas por la Entidad en esta materia.
Acceso a redes y a servicios en red	
Gestión de acceso de usuarios	

Registro y cancelación del registro de usuarios	Se cuenta con el procedimiento P-DT-007 Administración de usuarios. Todos los usuarios tienen acceso restringido a sus equipos excepto por aquellos que han solicitado o requieren para su trabajo usuarios administradores. Se recomienda a la Dirección de TIC crear un control para la revisión periódica de retiro de los sistemas de los funcionarios de planta o contratistas que ya no laboren en la Entidad. Se recomienda buscar los mecanismos para el cumplimiento de la política cuando el trabajo se está haciendo fuera del dominio de la Entidad.
Suministro de acceso de usuarios	
Gestión de derechos de acceso privilegiado	
Gestión de información de autenticación secreta de usuarios	Se cuenta con el procedimiento P-DT-007 Administración de usuarios. Actualmente, debido a la contingencia, las contraseñas no son temporales. Se recomienda establecer una política para que por la contingencia que se está atravesando se realicen los cambios de clave tal como está establecido en el procedimiento
Revisión de los derechos de acceso de usuarios	Hasta ahora se está creando el procedimiento de Monitoreo que incluye la revisión de privilegios de los usuarios. Se recomienda dar celeridad a la implementación del documento borrador aportado por la Dirección de TIC.,
Retiro o ajuste de los derechos de acceso	No hay recomendación
Responsabilidades de los usuarios	No hay recomendación
Uso de información de autenticación secreta	No hay recomendación
Control de acceso a sistemas y aplicaciones	No hay recomendación
Restricción de acceso a información	Se cuenta con el manual M-DT-001 de políticas de seguridad de la información. Se aplican restricciones a la información por áreas y subgrupos según sea el requisito. Los responsables de la información del área son los líderes de proceso y por lo tanto ellos autorizan el acceso de sus colaboradores a sus propias carpetas. Se recomienda realizar una revisión integral de la Política de Seguridad teniendo como marco las actuales circunstancias que afectan a la Entidad en materia de informática a raíz de la pandemia por el COVID-19. Actualizar de acuerdo con las directrices impartidas por la Entidad en esta materia. Se recomienda la pronta implementación del Manual del Sistema de Seguridad de la Información, anexo como soporte

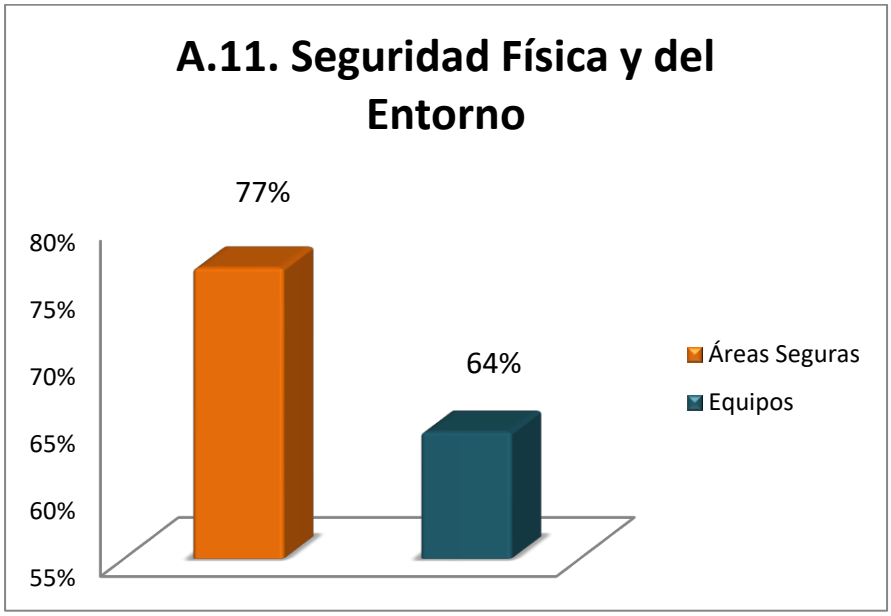
	en borrador, en el cual se define la autoridad, roles y responsabilidades.
Procedimiento de ingreso seguro	Se cuenta con el procedimiento P-DT-007 Administración de usuarios. A través del directorio activo se cuenta con política de contraseñas y complejidad, así como tiempo de cambio. Los usuarios tienen perfiles estándar, no pueden usar los programas utilitarios a menos que se requiera un usuario administrador para hacer el uso respectivo. Los documentos presentados como soporte corresponden a los mismos que se presentaron en el seguimiento anterior por tanto no se han realizado los ajustes sugeridos en la evaluación anterior.
Sistema de gestión de contraseñas	
Uso de programas utilitarios privilegiados	
Control de acceso a códigos fuente de programas	El código fuente se maneja a través de los contratos con terceros, quienes custodian el código fuente. Los programas que se desarrollan internamente y que están debidamente notificados a TIC se controlan a través de repositorios internos donde se garantiza confidencialidad, integridad y disponibilidad. Se recomienda el levantamiento de un procedimiento para mantener el control de aplicaciones y evitar la corrupción del código fuente y así evitar copias no autorizadas.

A.10 Criptografía. Cumplimiento: 50%

CRIPTOGRAFÍA	**OBSERVACIONES Y RECOMENDACIONES**
Controles criptográficos	
Política sobre el uso de controles criptográficos	Se cuenta con el manual M-DT-001 de políticas de seguridad de la información. Se recomienda la revisión y si es procedente la actualización de la política que se encuentra descrita en el Manual de Políticas de Seguridad de la Información M-DT-001 V3, ya que se debe cumplir con el control que aquí se detalla (Cuándo deben implementarse y con qué nivel de seguridad, etc.).
Gestión de claves	Se cuenta con el directorio activo, donde se administran contraseñas. En algunos sistemas donde no se tiene autenticación con el DA, entonces se realiza manual a través de los administradores específicos de cada sistema. Se tiene planeada la documentación de los controles criptográficos completos que usa TRANSMILENIO Se recomienda definir un procedimiento o política para la realización de esta actividad. Esta misma recomendación se

	realizó en el informe OCI-2019-055 y se reitera en el presente informe

A.11 Seguridad Física y del Entorno: Cumplimiento 71%

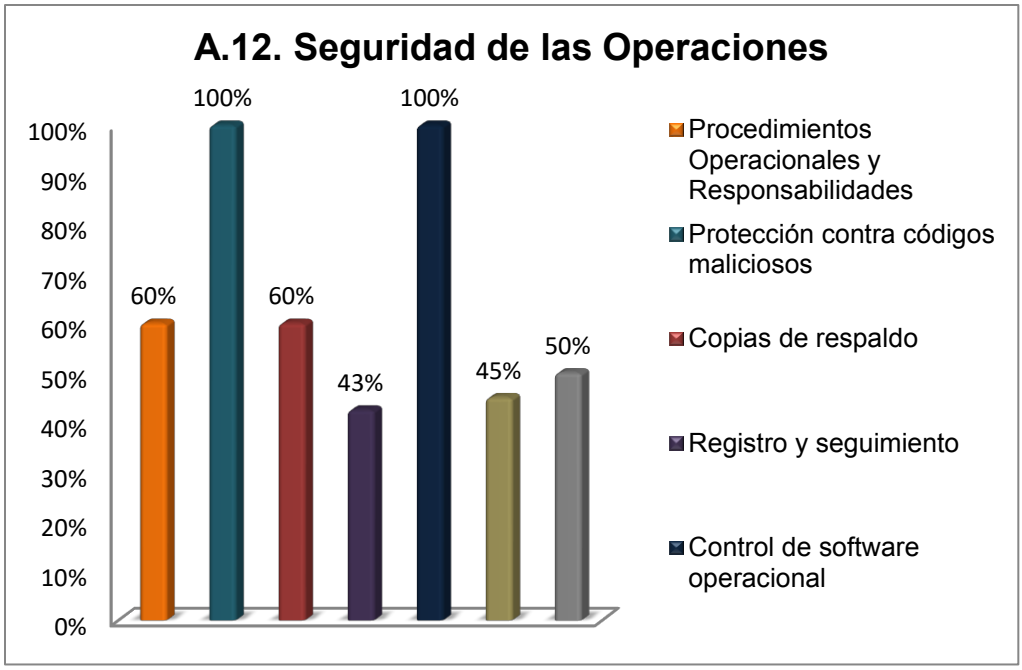


SEGURIDAD FÍSICA Y DEL ENTORNO	OBSERVACIONES
Áreas Seguras	
Perímetro de seguridad física	-El edificio cuenta con diferentes controles de seguridad como control de acceso al edificio, protección física y detección de intrusos, cámaras entre otros. -Todos los pisos de TMSA están protegidos con vigilancia privada. -Todos los funcionarios deben presentar su carné al ingresar al edificio y a los pisos.
Controles de acceso físico	- Al data center tiene únicamente acceso a personal autorizado con tarjeta de proximidad. -Todos los funcionarios deben presentar su carné al ingresar al edificio y a los pisos. Se recomienda la implementación de los controles en todas las áreas seguras de la Entidad en el centro de la UPS, centro de cableado y planta eléctrica, de acuerdo con lo recomendado anteriormente por la OCI en informe de auditoría al proceso de Gestión de Servicios Logístico OCI-2019-083.
Seguridad de oficinas, recintos e instalaciones	El edificio cumple con lo requerido con el control.
Protección contra amenazas externas y ambientales	El edificio cumple con lo requerido con el control.

	Se recomienda la revisión de los protocolos de seguridad actuales teniendo en cuenta que el entorno ha cambiado a raíz de la llegada del Ministerio de Defensa y otras Entidades al sector
Trabajo en áreas seguras	El edificio cumple con lo requerido con el control. Sin embargo, el procedimiento de Áreas Seguras está en desarrollo. Se recomienda agilizar el desarrollo e implementación del procedimiento de áreas seguras aportado como borrador para ser aplicado en la Entidad.
Áreas de carga, despacho y acceso público	No se cuenta con áreas de carga y despacho. Sin embargo, Corporativa tiene un procedimiento para el ingreso y retiro de elementos de las instalaciones de Transmilenio. La Entidad no cuenta con zonas de carga, sin embargo, hay ingreso tanto de personal como de elementos. Se recomienda desarrollar un procedimiento o formatos para el ingreso o salida de elementos ya que desde la Dirección Corporativa no se tiene.
Equipos	
Ubicación y protección de los equipos	Se cuenta con el data center debidamente protegido Se cuenta con política de escritorio y pantalla limpia dentro del manual M-DT-001 de políticas de seguridad de la información. Se recomienda la implementación de una política para el manejo de los equipos que fueron entregados en las casas de los funcionarios en la que se incluyan aspectos como: el adecuado uso de éstos, la seguridad de la información, la seguridad física.
Servicios públicos de soporte	-Se cuenta con infraestructura de suministro UPS y Planta Eléctrica -Se cuenta con redundancia de canales de internet para comunicaciones. Se recomienda definir programas de mantenimiento para los servicios con los que se cuenta en la entidad (agua, aire acondicionado, etc.). Adicional definir un programa en el que se garantice la protección de los equipos que han sido entregados en la casa de los funcionarios. Mediante correo electrónico de junio 1 de 2020 se solicitó el cronograma de mantenimiento, pero éste no fue allegado.
Seguridad del cableado	-Se cuenta con piso falso donde se transportan los cables de energía -El cableado de red se transporta por bandejas por encima de los Racks.
Mantenimiento de los equipos	Se recomienda generar un documento que contenga la descripción del mantenimiento mensual, semestral, anual según lo determinen en el área de los equipos informáticos que posee la Entidad. Mediante correo electrónico de junio 1 se solicitó el cronograma de mantenimiento, pero éste no fue allegado. Se recomienda la revisión del procedimiento para los equipos que se encuentran fuera de la Entidad teniendo en cuenta las actuales circunstancias por la pandemia a raíz del COVID-19.
Retiro de activos	Este control se implementa por la Dirección Corporativa. Se recomienda revisar esta actividad pues consultado el módulo de MIPG no existe este control en el proceso de Recursos Físicos.

Seguridad de los equipos fuera de las instalaciones	Se cuenta con política y procedimiento de Teletrabajo Realizar una revisión al procedimiento e incluir en este políticas y procedimientos en el marco de la contingencia que viene afectando al país por el COVID-19. Incluir el trabajo en casa.
Disposición segura o reutilización de equipos	Se cuenta con el procedimiento de borrado seguro. Se recomienda agilizar el levantamiento e implementación del procedimiento de borrado seguro. El borrador que se anexa es de 2015 versión 1 y consultada la OAP no tienen este documento para revisión Se recomienda que a los equipos que son alquilados una vez se elaboren las actas de entrega se especifique en estas que se ha realizado el borrado seguro ya que éstos no vuelven a la Entidad. Los equipos de la Entidad una vez se den de baja deben evidenciar el borrado de sus medios de almacenamiento removibles (discos duros, removibles etc.).
Equipos de usuario desatendido	-Se cuenta con la política de bloqueo de equipos, sensibilización y configuración de los equipos para bloqueo automático antes de 5 y 10 minutos. -Se realizan pruebas de Ing. social donde se validan los equipos desatendidos. Se tiene informe de equipos desatendidos del 2019.
Política de escritorio limpio y pantalla limpia	Se cuenta con política de escritorio y pantalla limpia dentro del manual M-DT-001 de políticas de seguridad de la información. Se recomienda realizar campañas para que el personal interiorice la política de modo que no solamente sea aplicada en la sede administrativa sino en el lugar de trabajo en el que actualmente este ubicado el funcionario, esto teniendo en cuenta la contingencia que se viene presentando a raíz del COVID-19.

A. 12 seguridad de las Operaciones: Cumplimiento 65%

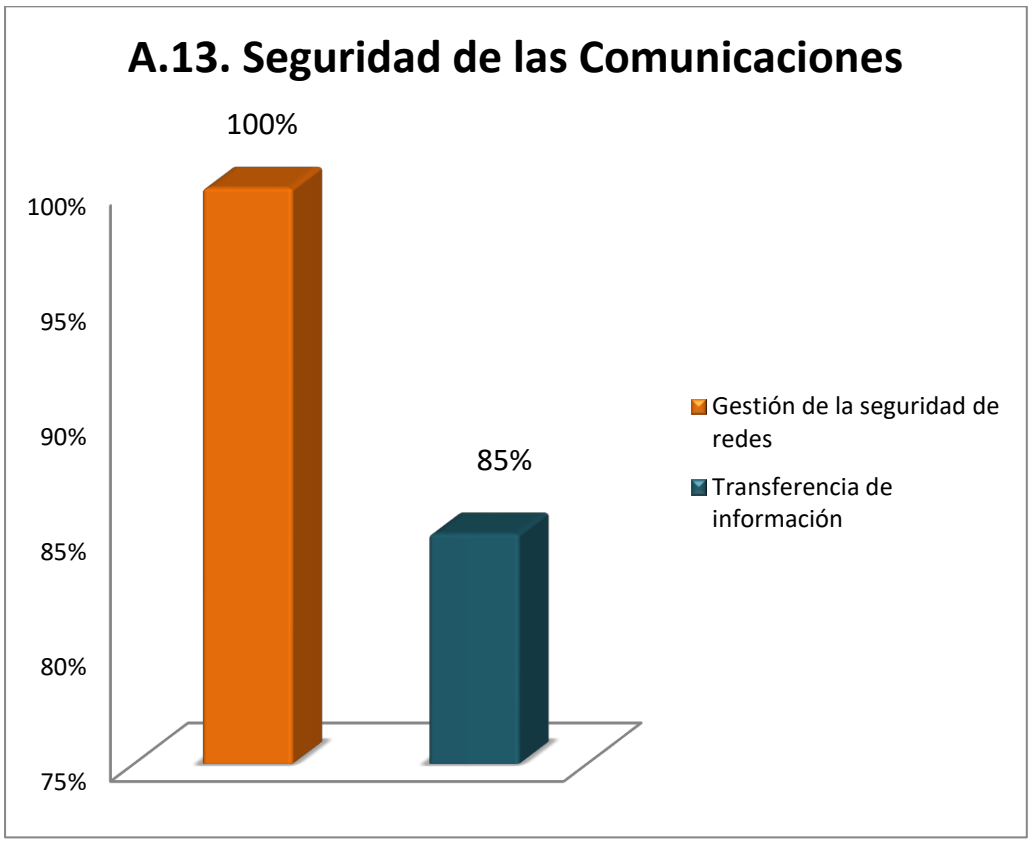


SEGURIDAD DE LAS OPERACIONES	OBSERVACIONES
Procedimientos Operacionales y Responsabilidades	
Documentación de los procedimientos de operación	Se tienen diferentes procedimientos aprobados y publicados para la dirección de TIC. Por ejemplo, el de Gestión de usuarios, instructivos de medios, de activos, protocolos, etc. Se recomienda agilizar la oficialización de los procedimientos de continuidad del negocio y procedimiento de copias de respaldo los cuales se encuentran en borrador para así dar cumplimiento a este control.
Gestión del cambio	Se cuenta con el procedimiento P-DT-017 Control de cambios de infraestructura Tecnológica. Se recomienda realizar una revisión y si es del caso ajustar los diferentes documentos teniendo en cuenta las circunstancias actuales a raíz de la contingencia por el COVID-19
Gestión de la capacidad	Se realiza monitoreo manual de los equipos. Sin embargo, se está construyendo el procedimiento de monitoreo que permite determinar los informes de capacidad. Se recomienda agilizar el levantamiento e implementación del procedimiento de monitoreo de tal manera que se pueda asegurar el desempeño requerido y optimo del sistema.
Separación de las instalaciones de desarrollo, pruebas y operación	Los sistemas los desarrollan los terceros, quienes manejan su ambiente de desarrollo y pruebas. Luego se pasan a ambiente de producción que está dentro de Transmilenio a través del procedimiento de control de cambios.

Protección contra códigos maliciosos	
Controles contra códigos maliciosos	Se cuenta con el software de antivirus Kaspersky -Se cuenta con un control de instalación de software -Se realiza verificación de ejecución de archivos: TRAPS -Se cuenta con controles de acceso y navegación de internet Se recomienda realizar campañas de sensibilización para que los funcionarios interioricen la política Se recomienda la implementación de una política para los equipos teniendo en cuenta el trabajo en casa y que cubra bajo ese marco los elementos que se están evaluando.
Copias de respaldo	
Copias de respaldo de la información	Se cuenta con la política de Backus en Manual M-DT-001 Políticas de seguridad y privacidad de la información. Se recomienda la realización de pruebas las cuales permitan mostrar la efectividad y eficiencia de lo establecido en el procedimiento. Se recomienda y tal como se expresó en el informe OCI-2019-074 la documentación e implementación de un procedimiento de Backup que dé cumplimiento a lo requerido en el Manual de políticas de seguridad de la información. Realizar revisión del documento teniendo en cuenta las actuales circunstancias que se están viviendo en razón al CORONAVIRUS y la utilización de equipos de la Entidad.
Registro y seguimiento	
Registro de eventos	-Se encuentra en implementación la herramienta SIEM para correlación de eventos y recolección de Logs. - Se cuenta con políticas que indican que se deben generar, proteger y revisar los registros. Ver M-DT-001. Se recomienda fortalecer las herramientas, es decir, implementar un procedimiento, revisar periódicamente las actividades de los usuarios y demás eventos relacionados con la seguridad de la información.
Protección de la información de registro	
Registros del administrador y del operador	
Sincronización de relojes	Los relojes se toda la infraestructura se encuentra sincronizados con el servidor de Hora Legal Colombiana. Se recomienda determinar un método, política u otro medio para dar cumplimiento para éste control teniendo en cuenta que varios equipos han sido trasladado al sitio de habitación de los funcionarios
Control de software operacional	
Instalación de software en sistemas operativos	Se cuenta con el procedimiento P- DT-016 Instalación y desinstalación de software Se recomienda la divulgación de la normatividad expedida por la Subgerencia General de la Entidad mediante comunicación con radicado 2018IE3984 en materia de instalación e implementación de software. Se recomienda realizar las acciones tendientes al cumplimiento de la normatividad expedida por la Entidad (Manual de Políticas de Seguridad Numeral 9,5 y el procedimiento P-DT-016 numeral 6) para dar cumplimiento a lo referente a Instalación de Software tal como se describe en el informe de Derechos de Autor de la presente vigencia.

Gestión de la vulnerabilidad técnica	
Gestión de las vulnerabilidades técnicas	Se tiene el procedimiento de gestión de vulnerabilidades en borrador listo para ser publicado. Se realizan pruebas de vulnerabilidad anualmente. Se recomienda la implementación pronta del procedimiento. El borrador entregado es una versión del 2015 el cual no presenta ningún cambio. Se recomienda incluir en este documento temas como solicitud de servicios por vulnerabilidad, gestión, ejecución, evaluación y seguimiento de las vulnerabilidades.
Restricciones sobre la instalación de software.	Se cuenta con el procedimiento P- DT-016 Instalación y desinstalación de software. Se está trabajando en la publicación del listado de software autorizado para que sea la guía para determinar qué debe y que no debe quedar instalado. Se recomienda agilizar la publicación del listado de software autorizado y establecer un control que no permita la instalación de estos sin la debida autorización del área de TIC. Se recomienda realizar las acciones tendientes al cumplimiento de la normatividad expedida por la Entidad (Manual de Políticas de Seguridad Numeral 9,5 y el procedimiento P-DT-016 numeral 6) para dar cumplimiento a lo referente a Instalación de Software tal como se describe en el informe de Derechos de Autor de la presente vigencia. Se recomienda realizar un monitoreo permanente para verificar la instalación de software en los equipos y realizar campañas de sensibilización sobre el tema
Consideraciones sobre auditorías de sistemas de información	
Controles de auditorías de sistemas de información.	-Se cuenta con la herramienta SIEM para correlación de eventos y recolección de Logs. Está en implementación. Se tiene primer reporte de la herramienta SIEM. Adicional, el procedimiento de monitoreo está en desarrollo. Sin embargo, este incluirá los requisitos que deben cumplir las herramientas de monitoreo de auditoría. Se recomienda la implementación de un procedimiento en donde se definan los lineamientos claros para la realización de autoevaluaciones o autoinspecciones de los controles automáticos y que éstas sean planeadas y acordadas para minimizar el riesgo de interrupción del proceso del negocio y en el cual se describa el pasa a paso para la realización de las mismas.

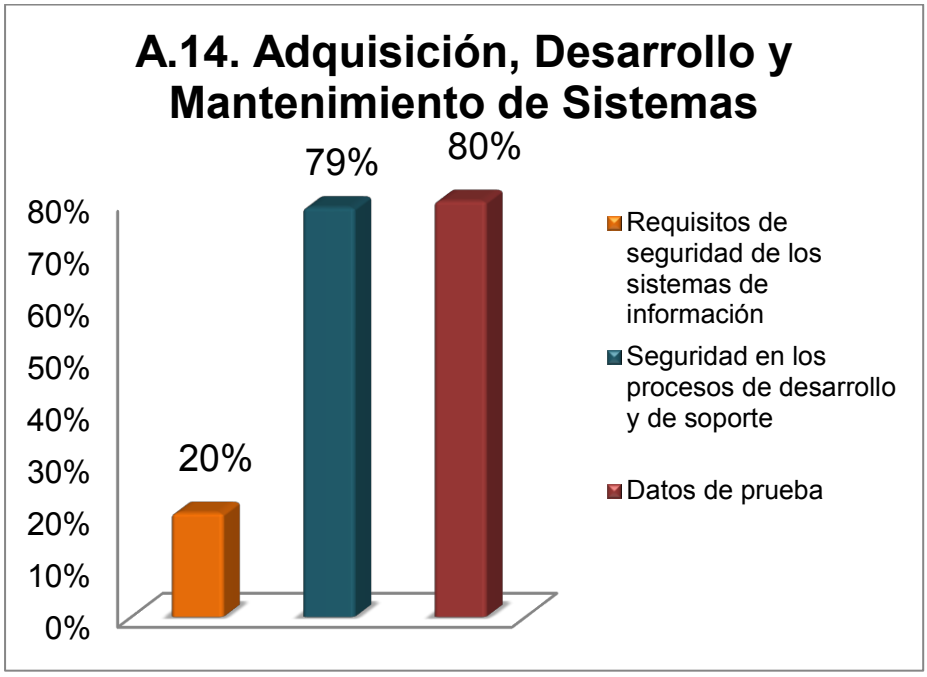
A. 13 Seguridad de las Comunicaciones. Cumplimiento 62%



SEGURIDAD DE LAS COMUNICACIONES	OBSERVACIONES Y RECOMENDACIONES
Gestión de la seguridad de redes	
Controles de redes	-La entidad cuenta con separación de redes a través de VLANs, se cuenta con controles perimetrales e internos para proteger la red. -Se tiene control de acceso a las redes wireless -El proveedor de comunicaciones es diferente al de infraestructura. -Se cuenta con alta disponibilidad en los switch de core y otros dispositivos. -Los sistemas de información y los equipos de red requieren autenticación para su ingreso a administración u operación. Se recomienda documentar un procedimiento e implementarlo para los Controles en las Redes y la Seguridad de los Servicios de Red, teniendo en cuenta el informe OCI-2019-055.
Seguridad de los servicios de red.	-La entidad cuenta con separación de redes a través de VLANs, se cuenta con controles perimetrales e internos para proteger la red. -Se tiene control de acceso a las redes wireless

	-El proveedor de comunicaciones es diferente al de infraestructura. -Se cuenta con alta disponibilidad en los switch de core y otros dispositivos -los sistemas de información y los equipos de red requieren autenticación para su ingreso a administración u operación.
Separación en las redes	La entidad cuenta con separación de redes a través de VLANs, se cuenta con controles perimetrales e internos para proteger la red.
Transferencia de información	
Políticas y procedimientos de transferencia de información	Se cuenta con el procedimiento P-DT-012 intercambio seguro de información. Los contratos con terceros cuentan con políticas de confidencialidad y de manejo de la información, así como adaptarse a las políticas que tenga Transmilenio. Se recomienda crear una política o modificar el procedimiento e incluir en este las transferencias electrónicas que realiza la Entidad. Se recomienda y tal como se mencionó en el informe de Auditoría Interna N° OCI-2019-074 la formalización de un procedimiento para que el concesionario del SIRCI realice la gestión de cambios apropiada.
Acuerdos sobre transferencia de información	Se cuenta con el procedimiento P-DT-012 intercambio seguro de información
Mensajes electrónicos	Se cuenta con controles de protección de mensajería electrónica a través de seguridad de Office365
Acuerdos de confidencialidad o de no divulgación	--Se cuenta con las cláusulas de confidencialidad dentro de los contratos de los contratistas. -Se cuenta con acuerdos de confidencialidad en los contratos con proveedores No obstante, al corte del presente informe no se han gestionado las cláusulas de confidencialidad de la información para los contratos laborales de los funcionarios de planta. Se recomienda agilizar las actividades tendientes a evidenciar las correspondientes cláusulas para estos contratos.

A. 14 adquisición, Desarrollo y Mantenimiento de Sistemas: Cumplimiento 60%

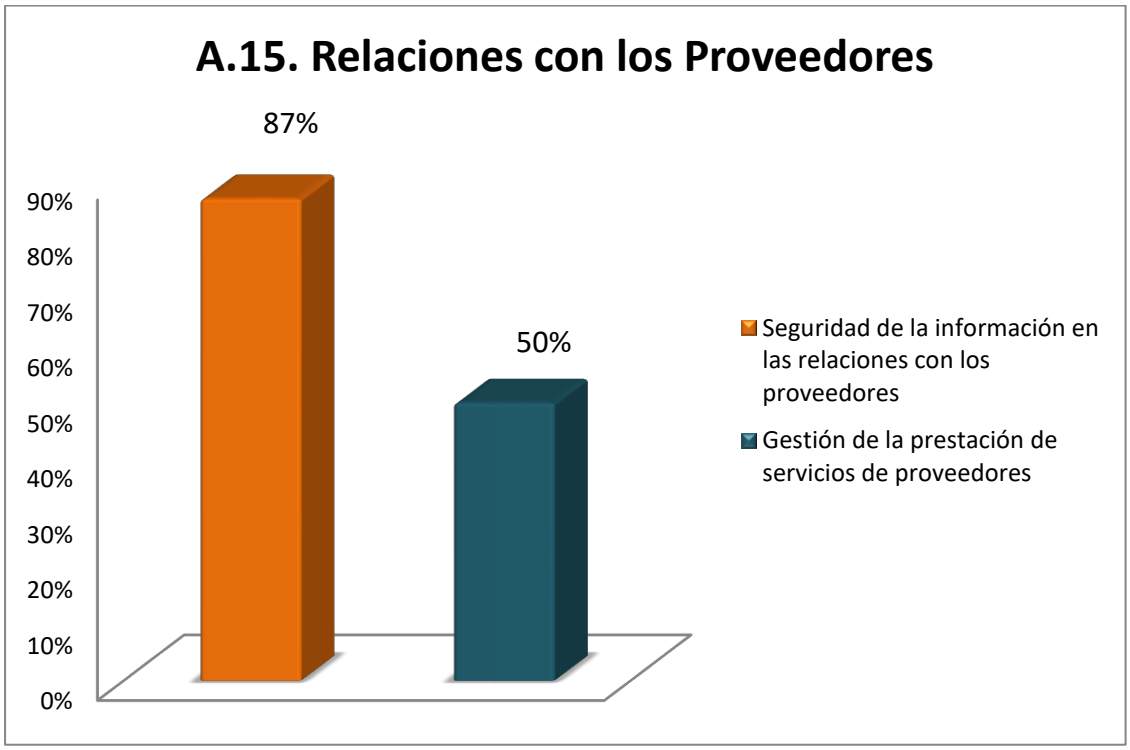


ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	OBSERVACIONES Y RECOMENDACIONES
Requisitos de seguridad de los sistemas de información	
Análisis y especificación de requisitos de seguridad de la información	Se cuenta con el procedimiento P-DT-013 Construcción de Sistemas de Información. Además, se cuenta con protocolo de verificación de seguridad en desarrollo. Está enviado a la OAP para publicación. Se adjunta borrador como anexo, se cuenta con infraestructura de protección perimetral para las aplicaciones públicas. Firewall Ips. Aunque no aplican transacciones en línea. Se recomienda la revisión del procedimiento que se relaciona cuya fecha de versión corresponde a enero de 2018 y agilizar la implementación del protocolo de verificación de seguridad. Adicional a lo anterior la Oficina de Control Interno en la evaluación anterior recomendó definir lineamientos de seguridad de servicios de las aplicaciones en redes públicas, que contemplara: a) Definir el nivel de confianza que cada parte requiere con relación a la identidad declarada por medio de autenticación. b) Establecer los procesos de autorización
Seguridad de servicios de las aplicaciones en redes públicas	

Protección de transacciones de servicios de aplicaciones	asociados con quien puede aprobar el contenido o expedir o firmar documentos transaccionales. c) Establecer los requisitos de protección de cualquier información confidencial. d) definir la confidencialidad e integridad de cualquier transacción de pedidos, información de pagos, etc. e) Evitar la pérdida o duplicación de información de la transacción; f) Se deben usar mecanismos de chequeo de las integridades para verificar la integridad del software, firmware, e información; actividades que no se reflejan en un nuevo documento.
Seguridad en los procesos de desarrollo y de soporte	
Política de desarrollo seguro	Se cuenta con la política de desarrollo seguro dentro del manual M-DT-001 Políticas de seguridad y privacidad de la información Se recomienda revisar la política y adaptar, si da lugar teniendo en cuenta la contingencia generada por el COVID-19
Procedimientos de control de cambios en sistemas	Se cuenta con el procedimiento P-DT-017 Control de cambios de infraestructura Tecnológica Se cuenta con el procedimiento P-DT-013 Construcción de Sistemas de Información
Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	Se cuenta con el procedimiento P-DT-017 Control de cambios de infraestructura Tecnológica Se cuenta con el procedimiento P-DT-013 Construcción de Sistemas de Información
Restricciones en los cambios a los paquetes de software	Se cuenta con el procedimiento P-DT-017 Control de cambios de infraestructura Tecnológica Se cuenta con el procedimiento P-DT-013 Construcción de Sistemas de Información
Principios de construcción de los sistemas seguros	Se recomienda realizar las acciones tendientes al cumplimiento de la normatividad expedida por la Entidad (Manual de Políticas de Seguridad Numeral 9,5 y el procedimiento P-DT-016 numeral 6) para dar cumplimiento a lo referente a Instalación de Software tal como se describe en el informe de Derechos de Autor de la presente vigencia. Se recomienda realizar un monitoreo permanente para verificar la instalación de software en los equipos y realizar campañas de sensibilización sobre el tema Se recomienda tener en cuenta lo informado por la OCI en informe OCI-2019-055
Ambiente de desarrollo seguro	No hay recomendación

Desarrollo contratado externamente	Se recomienda agilizar la implementación de los documentos que se encuentran en revisión por la OAP y anexados como borrador para así dar cumplimiento con el control. Incluir en éstos los apartes relacionados en la evaluación anterior como son: a) los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente; b) establecer los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas; c) definir el suministro del modelo de amenaza aprobado, al desarrollador externo; d) realizar los ensayos de aceptación para determinar la calidad y exactitud de los entregables; e) definir la evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad; f) definir la evidencia de que se han hecho pruebas suficientes para proteger contra contenido malicioso intencional y no intencional en el momento de la entrega; g) definir la evidencia de que se han hecho pruebas suficientes para proteger contra la presencia de vulnerabilidades conocidas; h) definir los certificados de depósito de títulos en garantía; (el código fuente ya no está disponible); i) establecer el derecho contractual con relación a procesos y controles de desarrollo de auditorías; j) documentar eficaz del ambiente de construcción usado para crear entregables; k) establecer que la organización es responsable de la conformidad con las leyes aplicables y con la verificación de la eficiencia del control. Se recomienda realizar pruebas aleatorias con más frecuencia y así poder tener un mejor control de las posibles incidentes que se puedan presentar teniendo en cuenta las recomendaciones y los resultados arrojados en el informe Hacking.
Pruebas de seguridad de sistemas	
Prueba de aceptación de sistemas	Se recomienda agilizar la modificación al procedimiento teniendo en cuenta que actualmente se vienen haciendo desarrollos en la Entidad motivo por el cual estos riesgos deben quedar cubiertos.
Datos de prueba	
Protección de datos de prueba	Realizar una revisión al procedimiento e incluir en él temas como: '-Control de acceso aplicación de pruebas - autorización separada cada vez que se copia información operacional a un ambiente de pruebas - Se debe definir que la información operacional se debe borrar del ambiente de pruebas una vez se termine la prueba - establecer que el copiado y uso de la información operacional debe ser registrada y así poder suministrar un rastro de auditoría.

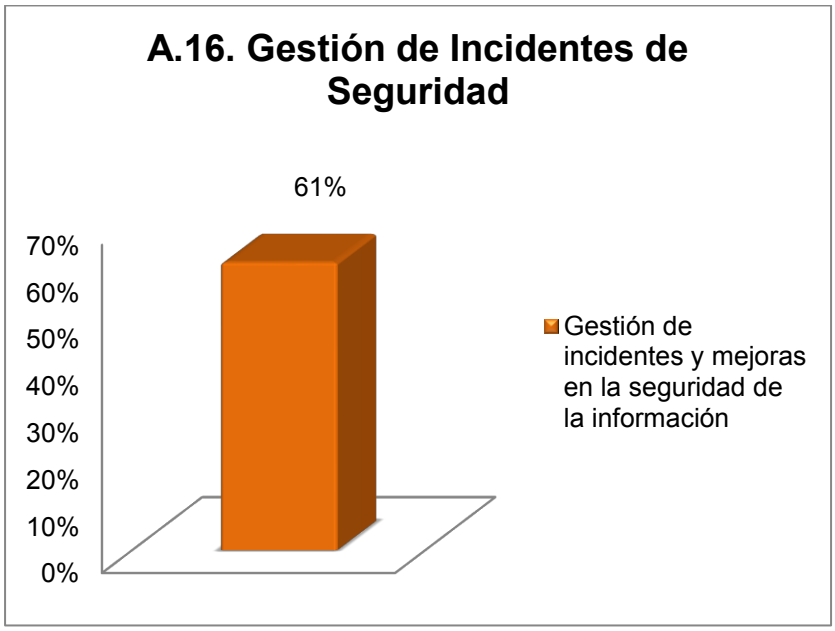
A. 15 Relaciones con los proveedores: Cumplimiento 68%



RELACIONES CON LOS PROVEEDORES	OBSERVACIONES Y RECOMENDACIONES
Seguridad de la información en las relaciones con los proveedores	
Política de seguridad de la información para las relaciones con proveedores	Se recomienda revisar la política actual y si es del caso actualizarla teniendo en cuenta las disposiciones impartidas por el Gobierno a raíz de la contingencia por el COVID-19
Tratamiento de la seguridad dentro de los acuerdos con proveedores	Si bien se cuenta con acuerdos de confidencialidad y cláusulas en los contratos con los proveedores de TRANSMILENIO S.A., No se evidenció documento que defina la metodología que la Entidad utiliza para tratar la seguridad dentro de los acuerdos con los proveedores. Se recomienda implementar un procedimiento o control de revisión del cumplimiento de los lineamientos establecidos.
Cadena de suministro de tecnología de información y comunicación	Se recomienda la revisión de la política establecida teniendo en cuenta la contingencia que se viene presentando a raíz del COVI-19.
Gestión de la prestación de servicios de proveedores	

Seguimiento y revisión de los servicios de los proveedores	El Objetivo del dominio evaluado es que TRANSMILENIO S.A. 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. Sobre lo enunciado, 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 necesarios 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. Se recomienda la implementación de este control y poder dar cumplimiento al mismo. No obstante, esta recomendación fue realizada en el informe OCI-2019-55 la cual no fue adoptada por la Dirección de TIC
Gestión de cambios a los servicios de los proveedores	No hay recomendación

A. 16 Gestión de Incidentes de Seguridad 61%

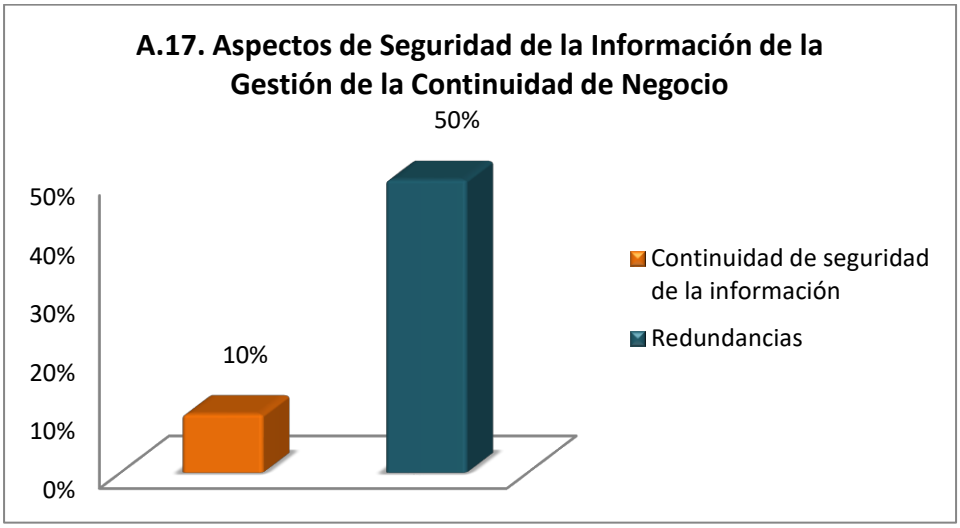


GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN	OBSERVACIONES Y RECOMENDACIONES

Gestión de incidentes y mejoras en la seguridad de la información	
Responsabilidades y procedimientos	Se 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 Se recomienda agilizar la implementación del procedimiento el cual debe cubrir temas como: '- Que el personal competente maneje las cuestiones relacionadas con incidentes de seguridad de la información dentro de la organización - Se implemente un punto de contacto para la detección y reporte de incidentes de seguridad - Se mantengan contactos apropiados con las autoridades, grupos de interés o foros externos que manejen las cuestiones relacionadas con incidentes de seguridad de la información, - los procedimientos para respuesta, incluyendo aquellos para llevar el asunto a una instancia superior, recuperación controlada de un incidente y comunicación a personas u organizaciones internas y externas, - establecer un control de seguridad ineficaz; - definir la violación de la integridad, confidencialidad o expectativas de disponibilidad de la información; - definir los errores humanos; - definir las no conformidades con políticas o directrices; - definir las violaciones de acuerdos de seguridad física, entre otros. En el informe OCI–2019-55, se efectuó la presente recomendación, por tanto, se evidencia que no fue tenida en cuenta. Se recomienda incluir la evaluación del nivel de riesgo para cada tipo de incidente, estableciendo los controles necesarios
Reporte de eventos de seguridad de la información	
Reporte de debilidades de seguridad de la información	Se recomienda adelantar más campañas a través de la intranet y correos electrónicos.
Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Se recomienda la revisión de la política establecida teniendo en cuenta la contingencia que se viene presentando a raíz del COVI-19.
Respuesta a incidentes de seguridad de la información	Se recomienda la pronta implementación del documento de gestión de incidentes en donde se relacionen los planes de respuesta para cada categoría y así minimizar las vulnerabilidades del sistema.

Aprendizaje obtenido de los incidentes de seguridad de la información	Se recomienda la pronta implementación del documento de gestión de incidentes en donde se relacionen los planes de respuesta para cada categoría y así minimizar las vulnerabilidades del sistema.
Recolección de evidencia	

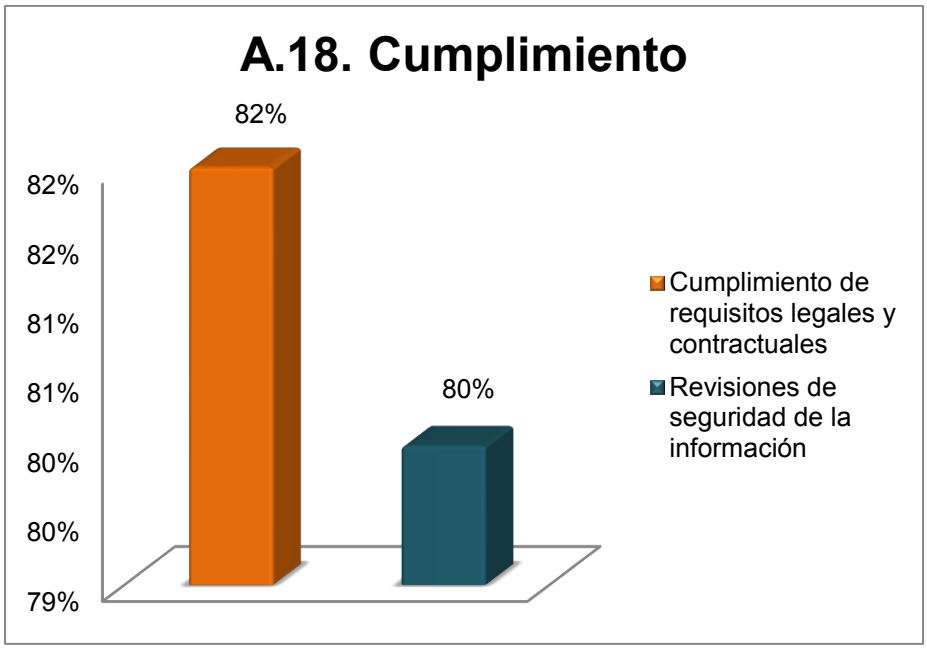
A.17 Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio: Cumplimiento 30%



ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	OBSERVACIONES Y RECOMENDACIONES
Continuidad de seguridad de la información	
Planificación de la continuidad de la seguridad de la información	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. No se cuenta con un documento BIA (Análisis de Impacto del negocio), de igual forma la descripción de la infraestructura del Centro de cómputo alterno formalmente documentado, en el cual se determinen proceso que son esenciales para la continuidad de las operaciones de la Entidad. Se recomienda el adecuado diseño e implementación de estos controles teniendo en cuenta la actual situación (COVID - 19), ya que las vulnerabilidades son mayores. Tener presente que se deben estructurar y reforzar los procedimientos para la continuidad del negocio, esto es, revisar y documentar un BIA (Análisis del Impacto del Negocio) , con base en este ajustar el BCP (Plan de continuidad del negocio) y así obtener un DRP (Plan de recuperación ante desastre) fuerte, a fin de que la Entidad cuente con los riesgos asociados al tema enunciado y sus respectivos controles que den respuesta a un escenario de
Implementación de la continuidad de la seguridad de la información	
Verificación, revisión y evaluación de la continuidad de la seguridad de la información	

	continuidad del negocio, en especialmente a lo que corresponde a los centros de control de operación, tanto de BUSES como de BRT, toda vez que se encuentran vulnerables y no se cuenta con un plan de contingencia para operar de otra manera. Frente a los proveedores externos (tercerizados), se recomienda generar una cultura de verificación técnica operativa de los servicios que se le han transferido y así asegurar que el riesgo se esté controlando y éstos no afecten la continuidad del negocio. La recomendación efectuada en el informe OCI-2019-055 No fue tenida en cuenta ya que persiste la misma situación.
Redundancias	
Disponibilidad de instalaciones de procesamiento de información	

A.18 Cumplimiento: Cumplimiento 81%



CUMPLIMIENTO	
Cumplimiento de requisitos legales y contractuales	**OBSERVACIONES Y RECOMENDACIONES**

Identificación de la legislación aplicable y de los requisitos contractuales	La entidad cuenta con normograma en donde se encuentra la reglamentación aplicable a seguridad de la información. Disponible en la intranet. Se debe realizar una revisión a la matriz del normograma teniendo en cuenta la nueva normatividad que se ha expedido en razón a la contingencia presentada por el COVID-19. Se recomienda realizar las acciones tendientes al cumplimiento de la normatividad expedida por la Entidad (Manual de Políticas de Seguridad Numeral 9,5 y el procedimiento P-DT-016 numeral 6) para dar cumplimiento a lo referente a Instalación de Software tal como se describe en el informe de Derechos de Autor de la presente vigencia. Se recomienda realizar un monitoreo permanente para verificar la instalación de software en los equipos y realizar campañas de sensibilización sobre el tema, pues para este control se estaría violando lo establecido En el artículo 2 de la Ley 603 de 2002
Derechos de propiedad intelectual	Se recomienda realizar las acciones tendientes al cumplimiento de la normatividad expedida por la Entidad (Manual de Políticas de Seguridad Numeral 9,5 y el procedimiento P-DT-016 numeral 6) para dar cumplimiento a lo referente a Instalación de Software tal como se describe en el informe de Derechos de Autor OIC-2020-021 de la presente vigencia. Se recomienda realizar un monitoreo permanente para verificar la instalación de software en los equipos y realizar campañas de sensibilización sobre el tema, pues para este control se estaría violando lo establecido En el artículo 2 de la Ley 603 de 2002
Protección de registros	Sin recomendación
Privacidad y protección de información de datos personales	Sin recomendación
Reglamentación de controles criptográficos	En el informe 2019-OCI-055 se recomendó que se implementaran controles criptográficos, si bien está la política de uso criptográfico en el manual de seguridad de la información, no se evidenció la existencia de un sistema o procedimiento formalizado e implementado para soportar el uso en la entidad de las llaves públicas y privadas. Esta recomendación se reitera ya que no fue tenida en cuenta.
Revisiones de seguridad de la información	
Revisión independiente de la seguridad de la información	-Se realiza Informe de Diagnostico del MSPI para Transmilenio. -Se tiene planeada la revisión independiente para el año 2021. - Se cuenta con el seguimiento por parte de la OCI.
Cumplimiento con las políticas y normas de seguridad	Sin recomendación
Revisión del cumplimiento técnico	La Dirección de TIC indicó que se realizan pruebas de vulnerabilidad y hacking ético anual.

	No obstante, está en proceso la revisión de remediación de vulnerabilidades. Si bien se evidenció un trabajo realizado por TIC, Se recomienda la pronta implementación de las recomendaciones dadas en el trabajo realizado en el tema por los expertos contratados (PASSWORD). No fueron adoptadas las recomendaciones efectuadas por la Oficina de Control Interno mediante el informe OCI-2019-55

- **Afectación y/o cambios que se han generado en razón de la contingencia por COVID-19**

La oficina de Control Interno solicitó a la Dependencia de TIC, informara las situaciones que se ha presentado en materia de Seguridad de la Información, teniendo en cuenta la contingencia que se presenta a raíz del COVID-19 y mediante correo electrónico de fecha mayo 28 de 2020 respondieron al asunto así: *En lo que hemos visto, la situación actual ha afectado positivamente al SGSI. Me refiero a que se ha logrado recibir más retroalimentación por parte de los usuarios con respecto a situaciones de seguridad que les ocurren correos que llegan o envío de boletines de seguridad y eso definitivamente le permite al sistema mejorar.*

Por otro lado, se ha evidenciado también de forma positiva que se indaga aún más en los controles que tenemos, mejorándolos y afinándolos para proporcionar un ambiente más seguro. También, nos hemos dado cuenta de que nuestros controles de seguridad técnicos y procedimentales están en un nivel muy cercano al óptimo dado que hemos detenido varios ataques y hemos identificado nuevas formas de proteger a la Entidad. Por ejemplo, la revisión por nuestras herramientas de SIEM, Firewall y Endpoint permiten proteger nuestra red interna, así como los servicios dispuestos para teletrabajo.

No obstante, también hay mejoras que deben hacerse, cosas que normalmente hacemos en oficina no es posible desarrollar presencialmente, tales como la sensibilización presencial o reunirse y planear con mayor frecuencia la expansión del alcance del SGSI

a nuevos procesos. Aunque se hace de forma virtual, también hace falta mejorar la metodología para que la forma virtual sea más interactiva.

CONCLUSIONES:

De acuerdo con el análisis realizado por la Oficina de Control Interno a las observaciones relacionadas en la Matriz denominada Diagnóstico GAP de IEC 27001, anexa al presente informe y la valoración de los documentos aportados por la Dirección de TIC para las mismas, se evidenció un nivel de cumplimiento del 69%, ubicándola, según la tabla calorimétrica, en un nivel de implementación entre definido y medible, lo cual representa un cumplimiento medio aceptable. De igual forma se identificaron debilidades en el 31% de los dominios frente al total de la herramienta aplicada al Sistema de Seguridad de la Información.

Se observa, que la Entidad ha realizado actividades en procura de la mejora de la gestión de seguridad de la información, lo cual permite que el estado del nivel de madurez se encuentre alineado con los objetivos y estrategias definidas en cuanto a la preservación de la confidencialidad, integridad, disponibilidad y seguridad de la información.

Se considera importante mencionar que las Oficina de Control Interno mediante el informe OCI-2019-055 realizó recomendaciones sobre el Sistema de seguridad de la información que no han sido tenidas en cuenta y se reiteran en el presente informe, dentro de las que destacamos:

1. Adelantar acciones tendientes a la agilización del diseño e implementación del procedimiento relacionado con reporte de eventos de seguridad (Dominio A.16).
2. Estructurar y reforzar los procedimientos para la continuidad del negocio, esto es, revisar y documentar un BIA (Análisis del Impacto del Negocio) , con base en este ajustar el BCP (Plan de continuidad del negocio) y así obtener un DRP (Plan de recuperación ante desastre) fuerte, a fin de que la Entidad cuente con los riesgos asociados al tema enunciado, se encuentre preparada y de efectiva respuesta ante la continuidad del negocio, especialmente de cara a los centros de control, tanto de

BUSES como de BRT, ya que se encuentran vulnerables y no se cuenta, con un plan de contingencia para operar de otra manera (Dominio A.17).

3. Implementar controles criptográficos, si bien está la política de uso criptográfico en el manual de seguridad de la información, no se evidenció la existencia de un sistema o procedimiento formalizado e implementado para soportar el uso en la entidad de las llaves públicas y privadas. Esta recomendación se reitera ya que no fue tenida en cuenta (Dominio A.18).
4. Se recomienda tomar acciones oportunas, para que las debilidades identificadas, 31% de los dominios, alcancen el nivel de madurez deseado, en procura de mejorar su porcentaje de cumplimiento y robustecer a la Entidad en el Sistema de Seguridad de la Información.

Adicional a lo anterior la Oficina de Control Interno llama la atención a recomendaciones reiterativas y que se plasman en este informe como son:

5. Realizar las acciones tendientes al cumplimiento de la normatividad expedida por la Entidad (Manual de Políticas de Seguridad Numeral 9,5 y el procedimiento P-DT-016 numeral 6) para dar cumplimiento a lo referente a Instalación de Software tal como se describe en el informe de Derechos de Autor de la presente vigencia.
6. Se recomienda realizar un monitoreo permanente para verificar la instalación de software en los equipos y realizar campañas de sensibilización sobre el tema, pues para este control se estaría violando lo establecido En el artículo 2 de la Ley 603 de 2002.
7. Se recomienda adelantar la gestión para la implementación de un protocolo de retorno de funcionarios a la Entidad e incluir en él temas como el recibo de equipos, verificación de los mismos, cómo se realizarán las copias de seguridad, incorporación de información a los repositorios de la Entidad, entre otros.

8. La Dirección de TIC en las distintas evaluaciones que ha realizado la Oficina de Control interno manifiesta que los documentos se encuentran en borrador y revisión por parte de la Oficina de Planeación. Reiteramos la recomendación de agilizar la implementación de estos documentos ya que afectan el desempeño y genera un gran riesgo en lo que tiene que ver con la seguridad de la información al no tener la documentación actualizada y legalizada en el sitio MIPG. Al respecto la Oficina de Planeación en correo recibido el 30 de junio de 2020 informó que únicamente tiene pendiente por oficializar los siguientes documentos: Protocolo para asegurar los desarrollos de software de TRANSMILENIO S.A.; Procedimiento para gestionar las vulnerabilidades Tecnológicas; Protocolo a seguir para el contacto con las autoridades y grupos de interés especial encargadas de gestionar el SGSI.

Este informe fue socializado con los Ingeniero Javier Castañeda y Daniel Leonardo Beltran de la Dirección de Tic el 30 de junio de 2020.

Cualquier información adicional con gusto será suministrada.

Bogotá D. C., 01 de julio de 2020

Luis Antonio Rodriguez Orozco
Jefe Oficina de Control Interno

Elaboró: Oscar Pulgarin Lara, Profesional Universitario Grado 04 – Oficina de Control Interno

Revisó: Luz Marina Díaz Ramírez, Contratista – Oficina de Control Interno.