N° INFORME: OCI-2021-037

PROCESO/SUBPROCESO / ACTIVIDAD: Gestión de TIC

RESPONSABLE DEL PROCESO/SUBPROCESO / ACTIVIDAD: Director de TIC.

EQUIPO AUDITOR: Néstor Orlando Velandia Sosa – Contratista, Auditor.

Luz Marina Díaz Ramírez - Contratista, Coordinadora.

OBJETIVOS:

1. Evaluación del proceso de Gestión de TIC:
   a. Administración de los Riesgos del proceso Gestión de TIC
   b. Diseño y la efectividad operativa de los controles del proceso.
   c. Cumplimiento de la normativa externa e interna, incluyendo la verificación de las políticas y procedimientos establecidos para el proceso.

2. Seguimiento a la implementación de la norma NTC-ISO-IEC 27001: 2013 (Sistema de Gestión Seguridad de la Información) por parte de la Entidad

ALCANCE:

El alcance definido para el presente trabajo de auditoría corresponde al proceso gestión de TIC para las actividades definidas en la caracterización y demás documentos del proceso, dentro de los que se incluyen los mapas de riesgos de gestión y de corrupción publicados en la intranet al corte de la evaluación.

De las seis (6) actividades claves del proceso registradas en la caracterización, fueron objeto de evaluación en el presente informe cuatro (4), las cuales se describen en la descripción del trabajo. Las actividades “Toma de acciones correctivas y preventivas” y “Formulación del Plan de Acción de TIC”, no se evaluaron, toda vez que fueron objeto de auditoría en los informes de evaluación por dependencias y seguimiento a planes de mejoramiento realizados durante el 2021 por la Oficina de Control Interno. De igual forma, la gestión de activos de información (identificación, clasificación y sistemas de información), el intercambio seguro de información, instalación,

actualización y desinstalación de software tampoco fueron evaluados toda vez que fueron cubiertos en las evaluaciones que dieron lugar a los informes OCI-2020-019 y OCI-2021-028.

El alcance de la auditoría consideró de las cuatro (4) actividades evaluadas y definidas en la caracterización las siguientes:

ACTIVIDAD DE LA CARACTERIZACIÓN	ITEM EVALUADO
Formulación y/o Actualización del Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETIC	• Fueron probados los controles del riesgo "Imposibilidad de ejecutar los proyectos asociados al plan estratégico PETI de acuerdo a la meta establecida" y los del "El plan estratégico de Seguridad de la Información (PESI) no se pueda implementar de acuerdo a la hoja de ruta establecida*".* • Se validó la labor en responsabilidad de la Dirección de TIC sobre las metas a través de del formato R-DT-4 para ocho (8) proyectos definidos en la hoja de ruta de los proyectos del PETI- PESI.
Ejecutar las acciones para que los componentes TIC, incluidos los ITS (Sistema Inteligente de Transporte)de la Entidad y del Sistema Integrado de Transporte Público estén disponibles en operación	• En relación con los ITS de la entidad (no SIRCI), se verificó la gestión adelantada en relación con el ciclo de desarrollo del sistema visión BRT. • Se verificó la existencia de controles automáticos asociados al directorio activo. • Fue verificado en la plataforma SECOP II la publicación de certificados de cumplimiento e informe de supervisión, del año 2020 para el contrato 001 de 2011 (SIRCI). • Se validó la existencia de controles en el ciclo de desarrollo del SIAPO (Sistema de apoyo a la interventoría). • Se validó que durante el 2020 la Dirección de TIC a través del proveedor Agilitix S.A.S., haya adelantado en la plataforma de hiperconvergencia, las actividades de gestión requeridas sobre la línea base de operación, gestión del cambio, procesos de gestión de capacidad, gestión de disponibilidad y los servicios de backup. • Se realizó inventario del total de colaboradores existentes en la Dirección de TIC al 31 de diciembre de 2020

	verificando la distribución de las actividades y funciones de la dependencia.
Diseñar e implementar la estrategia de seguridad de la información para TRANSMILENIO S.A. alineado con la normatividad legal vigente aplicable	• Se realizó seguimiento al análisis GAP del Sistema de Seguridad de la Información que incluyó evaluación a la implementación de los 114 controles definidos en la NTC-ISO-IEC 27001:2003.
Verificar, analizar, reportar y actualizar los instrumentos de gestión como son: mapa de riesgos, matriz de acciones correctivas y preventivas y de mejora, los indicadores de gestión del proceso y normograma, planes operativos del área, Plan de adquisiciones, proyectos de inversión y plan anticorrupción.	• Fueron evaluadas las matrices de riesgos de gestión y corrupción del proceso. • Fue evaluado el Indicador NASI

PERÍODO AUDITADO:

Proceso de gestión de TIC: 1 de enero de 2020 al 31 de diciembre de 2020

Análisis GAP al cumplimiento de la norma ISO27000: 1 de abril de 2020 al 31 de mayo de 2021

DECLARACIÓN:

Para el desarrollo del trabajo fueron aplicadas técnicas de muestreo, basadas en la adaptación de la Norma Internacional de Auditoria 530 y cuyo alcance cubre el diseño y la selección de las muestras para pruebas de control y de detalle. Una consecuencia que resulta de la aplicación de las técnicas de auditoría es la presencia del riesgo de muestreo, es decir, el riesgo de que la conclusión basada en la muestra analizada no coincida con la conclusión a la que se habría llegado en caso de haber examinado todos los elementos que componen la población.

CRITERIOS:

- Caracterización del proceso de gestión de TIC, manuales, procedimientos, protocolos, instructivos, indicadores, mapas de riesgos y demás documentos del Sistema de Gestión de

TRANSMILENIO S. A. vigentes y publicados en la intranet de la Entidad al corte de la presente evaluación.

- Normativa legal colombiana aplicable al sector de las TIC.
- Norma NTC-ISO-IEC 27001: 2013 (dentro del contexto del Modelo de Seguridad y Privacidad de la Información conforme a los lineamientos de la Política de Gobierno Digital, reglamentada mediante Decreto 1078 de 2015 y modificado por el Decreto 1008 de 2018).
- Ley 1712 de 2014 Ley de transparencia y del derecho de acceso a la información pública nacional
- Ley 1581 de 2012, Ley de Protección de Datos Personales
- Manual de Políticas de la Seguridad y Privacidad de la Información de TMSA M-DT-001 Versión 4
- Formatos, Manuales, Procedimientos, Instructivos, Protocolos del MIPG de TMSA
- Guía de auditoría No.10 Seguridad y Privacidad de la Información (MINTIC)

RIESGOS CUBIERTOS:

Para el desarrollo del trabajo fueron considerados los riesgos del Proceso de Gestión de TIC que figuran en el mapa de riesgos de gestión (3 riesgos catalogados en bajo en su nivel residual) y corrupción (1 riesgo catalogado en alto en su nivel residual). A continuación, lo enunciado:

MATRIZ DE RIESGOS DE GESTIÓN SEPTIEMBRE 2020					
#	DESCRIPCIÓN DEL RIESGO	RIESGO INHERENTE	# CONTROLES	RIESGO RESIDUAL	PRESENTAN PLAN DE TTO?
RG-1	Imposibilidad de ejecutar los proyectos asociados al plan estratégico PETI de acuerdo a la meta establecida	MODERADO	3	BAJO	NO
RG-2	El plan estratégico de Seguridad de la Información (PESI) no se pueda implementar de acuerdo a la hoja de ruta establecida	MODERADO	4	BAJO	NO
RG-2	Imposibilidad de apoyar técnicamente las necesidades relacionadas con TIC que afectan los procesos críticos de la entidad. Nota: Se entiende como proceso critico aquellos que afectan de manera difecta la operación del sistema.	MODERADO	4	BAJO	NO

Fuente: Mapa de riesgos del Proceso Gestión TIC vigente al 31 de diciembre de 2020

MATRIZ DE RIESGOS DE CORRUPCIÓN 01/02/21					
#	DESCRIPCIÓN DEL RIESGO	RIESGO INHERENTE	# CONTROLES	RIESGO RESIDUAL	PRESENTAN PLAN DE TTO?
RG-1	Configuraciones no autorizadas o indebidas para perfiles de acceso a usuarios de sistemas de información	ALTO	1	ALTO	Reducir el riesgo

Fuente: Mapa de riesgos de corrupción del Proceso Gestión TIC vigente al 31 de diciembre de 2020

FORTALEZAS.

- La Oficina de Control Interno identificó los siguientes controles implementados por la Dirección de TIC, los cuales se orientan a reducir la materialización de riesgos de seguridad de la información en la Entidad: (uso de cámaras de seguridad en sitios estratégicos tales como data center y cuarto de suministro UPS), condiciones técnicas generales del data center, uso de redes segmentadas por piso mediante *VLAN (*Red de Área Local Virtual*),* mantenimiento y soporte de los recursos tecnológicos existentes, uso de servicios tecnológicos en la nube, servidores configurados en alta disponibilidad, servicio de internet con operador principal y alterno, uso de herramientas *firewall* y *antivirus, c*ontroles restrictivos a los recursos de TI por medio de Directorio Activo, UPS (Unidad Ininterrumpida de Potencia) y generador de corriente eléctrica con soporte para servidores y estaciones de trabajo, conexiones de Red Pública Virtual *(VPN)* para el acceso remoto a sistemas de información, uso de protocolo *"HTTPS"* en la página web e intranet, herramientas de cifrado en los discos duros de los equipos, correo cifrado de Office 365, uso de ambientes separados de desarrollo, pruebas y producción, Contrato de monitoreo 7X24 de las bases de datos *Oracle* y *SQL Server*, uno de plataforma de colaboración empresarial *MS-Sharepoint y Teams,* y *c*ontrol centralizado de hardware y software con *ProactivaNet entre otros.*

DESCRIPCIÓN DEL TRABAJO REALIZADO:

Durante la auditoría efectuada al Proceso de Gestión de TIC fueron desarrolladas las siguientes actividades:

a) **Entendimiento del proceso**: Se llevó a cabo el entendimiento del proceso basado en entrevista realizadas a los colaboradores de las actividades claves del proceso y en la revisión de la documentación existente aplicable a la Dirección de TIC.

b) **Revisión de la Documentación**: Se consultó y analizó el mapa de riesgos del proceso, caracterización, manuales, procedimientos, instructivos, formatos, políticas y en general documentos definidos para el proceso de gestión de TIC y publicados en la intranet de la Entidad al corte de la evaluación, de acuerdo con el Sistema de Gestión, con el fin de verificar el cumplimiento de los requisitos del proceso.

c) **Identificación de riesgos y controles:** Se identificaron los riesgos claves que pudieran afectar o impactar las actividades y objetivos del proceso auditado y se verificó la existencia y efectividad de controles que mitiguen su materialización. De igual manera, los riesgos identificados fueron cotejados contra los registrados en el Mapa de Riesgos de Gestión.

d) **Diseño del programa de trabajo:** Basados en el entendimiento adquirido del Proceso, la Oficina de Control Interno diseñó el plan de pruebas, dirigido a determinar el adecuado diseño y aplicación de los controles, así como el cumplimiento de los requisitos identificados para el proceso.

e) **Reunión de Apertura:** Se efectuó la reunión de apertura el 18 de marzo de 2021, con el Director de TIC y su equipo de trabajo.

f) **Obtención y análisis de la información objeto de la auditoría:** Teniendo en cuenta la metodología definida por la Oficina de Control Interno, fue solicitada la información objeto de la auditoría con el fin de validar el diseño y aplicación de los controles claves y requisitos establecidos en el proceso.

g) **Ejecución de pruebas:** El trabajo de auditoría fue realizado bajo los estándares previstos en los procedimientos adoptados para la Oficina de Control Interno y la participación de los profesionales designados por el Director de TIC a través de los cuales se realizaron pruebas de indagación, comparación, inspección, observación y análisis efectuado sobre la documentación soporte remitida por la dependencia.

h) **Definición de hallazgos y recomendaciones:** Surgieron de un proceso de comparación entre el criterio (el estado correcto del requisito) y la condición (el estado actual). Teniendo en cuenta que durante la auditoría se evidenciaron diferencias entre ambos, éstos fueron y pre-validados con los responsables de las actividades del proceso y tomadas como hallazgos, los cuales se dan a conocer en el presente informe.

i) **Observaciones y recomendaciones:** Surgieron como sugerencias de mejores prácticas y contribuyen al mejoramiento del proceso y al fortalecimiento del Sistema de Control Interno de la Entidad.

j) **Análisis y Socialización del Informe con los responsables y líderes del proceso:** Se realizó la socialización de los resultados los días 21, 26 y 27 de mayo y se realizó reunión de cierre y socialización al Director de TIC el 1 de junio de 2021.

En particular, durante el desarrollo del trabajo fueron realizadas las siguientes actividades:

1. Evaluación al proceso de gestión de TIC

a. Matriz de Riegos.

- Fueron evaluados los tres (3) riesgos y once (11) controles registrados en la matriz de riesgos de gestión de la Dirección de TIC vigente al 31 de diciembre de 2020 y el riesgo existente en la matriz de riesgos de corrupción, verificando que se diera cobertura al objetivo del proceso, el diseño y la ejecución de los controles, la probabilidad y el impacto, así como la solidez individual y en conjunto de los controles. En cuanto al documento denominado "Anexo 5. Plan de tratamiento de Riesgos Seguridad de la información" (uno de los anexos del Plan Estratégico de TI), con fecha julio de 2018, la cual contiene 23 “escenarios de riesgo” de seguridad de la información, fue realizada una evaluación general dirigida a validar su alineación metodológica con lo establecido en el Manual de Gestión del Riesgo de TRANSMILENIO S.A. M-OP-04 de noviembre de 2020. Como resultado de dicha evaluación fue identificado el hallazgo 1.

b. Cumplimiento de actividades de TI en ocho (8) proyectos de la hoja de ruta de los proyectos del PETI- PESI; validación del ciclo de desarrollo del sistema visión BRT

Fue evaluada la gestión frente a los siguientes aspectos:

- Prácticas de programación utilizadas en la construcción del sistema aseguren el cumplimiento de las políticas de seguridad de la información aplicables y que se hayan considerado condiciones de seguridad a nivel de infraestructura de TI
- Que la especificación de requerimientos de software se realice a través del formato de requerimientos R-DT-04.
- Que la Dirección Técnica de BRT cuente con documentación de las pruebas funcionales realizadas al sistema
- Que la Dirección Técnica de BRT cuente con un registro de solicitud de creación de las cuentas de usuario del sistema
- Que la Dirección Técnica de BRT cuente con procedimientos que permitan atender eventuales fallas en la infraestructura tecnológica que soporta el sistema
- Que se cuente con documentación actualizada del sistema (descripción funcional).

Sobre lo anterior, no fueron identificados hallazgos.

c. Validación de controles a nivel de directorio activo

Fue revisada la existencia de políticas, lineamientos y controles en virtud de los Manuales de Políticas de Seguridad de la Información M-DT-01 y el Manual de administración de usuarios (M-DT-002). Sobre lo anterior no se evidenciaron incumplimientos.

d. Gestión del cambio a través de la plataforma de hiperconvergencia.

Se validó que durante el 2020 la Dirección de TIC a través del proveedor Agilitix S.A.S., haya adelantado en la plataforma de hiperconvergencia, las actividades de gestión requeridas sobre la línea base de operación, gestión del cambio, procesos de gestión de capacidad, gestión de disponibilidad y los servicios de backup. Sobre lo anterior se verificó la existencia de respaldo de base de datos para las aplicaciones T-DOC, JSP7, CORDIS y Sistema de Remuneración de Agentes; se verificó, el diseño de los controles

definidos en el procedimiento P-DT-019 Copias de respaldo y restauración de información en lo relativo a los sistemas de información de la Entidad, información usuarios, configuración dispositivos de comunicación y redes, servicios Office365 y solución de hiperconvergencia. De igual forma se probó la restauración del sistema de información T-DOC (aplicativo y base de datos) incluyendo el servidor de aplicación en una máquina virtual, la base de datos con corte al 14 de mayo de 2020 y que dicha aplicación es operativa con la base de datos restaurada. Sobre el particular no se evidenciaron incumplimientos.

e. Validación existencia de controles en el ciclo de desarrollo del sistema SIAPO (Sistema de apoyo a la interventoría).

Para esta actividad se realizaron las siguientes validaciones, sobre lo cual no se evidenciaron incumplimientos:

- Las prácticas de aseguramiento de la calidad del software a través de revisiones del código fuente
- Uso del formato de requerimientos R-Dt-04 en la especificación de requerimientos de software.
- Existencia de documentación sobre pruebas funcionales realizadas al sistema.
- Existencia de un registro de solicitud de creación de las cuentas de usuario del sistema
- Uso del formato de control de cambios del sistema R-DT-11
- Existencia de documentación sobre la descripción funcional del sistema.

f. Mantenimiento y Soporte

- Se verificó que existieran soportes de que la UPS y el sistema de aire acondicionado que reside en el Data Center hubieran recibido mantenimiento durante el año 2020 y que los resultados finales de dicho mantenimiento indicaran que opera en condición de normalidad. En relación con este aspecto, no fueron identificados hallazgos.

- En relación con la política de Gobierno Digital, la Oficina de Control Interno validó el cumplimiento del el Decreto 1008 de 2018 por parte de la Entidad en lo

relacionado con: Plan Estratégico de TI (incluida la gestión de los proyectos de TI), avances en la implementación de la Arquitectura Empresarial, documentación de los servicios de TI, gestión de los sistemas de información, operación de los servicios tecnológicos, adopción del cambio a IPv6, diagnóstico de seguridad de la información, y plan de tratamiento de riesgos. También validó el cumplimiento del plan de acción para la implementación de Servicios Ciudadanos Digitales.

Como resultado de esta verificación se documentó el hallazgo 6 y la oportunidad de mejora 2.

g. Alcance del Sistema de Gestión de Seguridad de la información

En relación con la gestión de los activos de la información, se verificó que el alcance del Sistema de Gestión de Seguridad de la Información establecido en el Plan Estratégico de Seguridad de la Información PESI V0 incluyera la totalidad de los sistemas de información de la Entidad y que la Dirección de TIC llevara a cabo acciones de monitoreo en relación con el cumplimiento de las políticas de seguridad de la información en los diferentes sistemas de información existentes en la Entidad. Como resultado de esta verificación se documentó el hallazgo 2.

h. Servicios de TI

A nivel de Directorio Activo (DA) se revisó la existencia de controles sobre la vinculación de sistemas de información de la Entidad al DA y el acceso a los recursos de TI asignados al personal de la Entidad.

i. Plan de cultura y sensibilización en seguridad de la información

Se validó la actualización y cumplimiento del documento T-DT-007 en su versión 0 publicado en el micro sitio del proceso, evidenciando debilidades en su gestión, las cuales fueron documentadas en el hallazgo 3.

j. Plan de recuperación de Desastres

Se validó el documento Plan Gestión de Seguridad de la Información en Continuidad del Negocio V0" de enero de 2021, el cual no ha sido probado integralmente, entre otros aspectos, razón por la cual se documentó el hallazgo 4.

k. Normas de seguridad en el Data center y en el cuarto de suministro UPS

Se evaluó el cumplimiento de las normas de seguridad y en el cuarto de suministros UPS en el marco del Plan de Gestión de la Seguridad de la Información en la Continuidad del Negocio (T-DT-011) V0, evidenciando debilidades, las cuales fueron registradas en el hallazgo 5.

l. Indicador NASI

Fue evaluada la formulación y diseño del indicador NASI el cual se encuentra documentado para medir la efectividad del Sistema de gestión de Seguridad de la información, evidenciando debilidades las cuales fueron documentadas en el hallazgo 7. Los indicadores definidos en el cuadro de mando integral no fueron evaluados en el presente trabajo en razón a que su verificación se dio en el marco de la evaluación por dependencias realizada en enero de 2021.

2. Análisis GAP al cumplimiento de la norma ISO27000

Se efectuó un seguimiento al análisis GAP de la norma NTC ISO27001:2013 realizado por la Dirección de TIC con corte al 31-may-2021, entendido como el nivel de cumplimiento por parte de la Entidad a cada uno de los 114 controles de la norma. El trabajo realizado consistió en evaluar la documentación aportada por la Dirección de TIC como evidencia del cumplimiento de los controles, y con base en el criterio del auditor, determinar si el valor de calificación dado por la Dirección de TIC a dichos controles se encuentra dentro de un umbral razonable. Los resultados de la evaluación fueron cotejados y socializados con los responsables de la información de la Dirección de TIC.

HALLAZGOS

A. Evaluación al proceso de gestión de TIC

Hallazgo N° 1 – Debilidad en la gestión y administración del riesgo del proceso de Gestión de TIC

Descripción del hallazgo o situación encontrada:

1.1. Se evidenció debilidad en la administración del riesgo del proceso, toda vez que está publicado en la intranet, en el micro sitio de la Dirección de TIC, en la carpeta de protocolos, un archivo en Excel denominado " Anexo 5. Plan de tratamiento de Riesgos Seguridad de la información", cuya fecha data de julio de 2018, que contiene entre otras cosas, riesgos en materia de seguridad de la información, cuya metodología de identificación, análisis y valoración no corresponde a la definida en el Manual de Gestión del Riesgo de TRANSMILENIO S.A. M-OP-04 de noviembre de 2020 y cuenta con las siguientes hojas de cálculo:

- Índice
- Matriz Act Valorados (con listado de vulnerabilidades, su tipo de soporte, número de activos, criticidad cualitativa, criticidad cuantitativa y amenazas por cada riesgo detectado)
- Selección de Esc (Selección de escenarios de riesgo con amenazas, nivel de criticidad y valoración de las amenazas).
- Matriz esc riesgos (con listado de escenario de riesgos, aceptabilidad del riesgo, opciones, variables para el tratamiento de riesgo entre otros).
- Mapa de riesgos (Con mapa calorimétrico del estado de riesgo inherente, actual y residual)
- Plan de Tratamiento de Riesgos
- Criticidad
- Valoración escenario de riesgos
- Probabilidad
- Impacto
- Riesgo (con nivel de probabilidad e impacto)

- Variables TTO (Con variables para el tratamiento del riesgo)
- Servidores (con listado de hardware: servidores)
- Aplicaciones (con listado de aplicaciones en la entidad)
- Base de datos
- Segmentos de red

1.2. De otra parte, verificado el diseño, efectividad y aplicación de los once (11) controles asociados a los tres (3) riesgos de gestión y del único control asociado al riesgo de corrupción, se encontró debilidad en el diseño de dos (2) controles tal y como se muestra a continuación:

Para el riesgo *"El Plan estratégico de seguridad de la información (PESI)no se pueda implementar de acuerdo a la hoja de ruta establecida"*, en las pruebas realizadas a la evaluación de los siguientes controles:

> *"La Dirección de TIC elabora y emite periódicamente los documentos asociados al PESI para conocimiento de los usuarios, por medio de la publicación y oficialización que realiza la Oficina Asesora de Planeación en la Intranet Corporativa. La Dirección de TIC´S realizará dos actividades anuales de sensibilización y socialización a los usuarios en relación con las políticas de seguridad de la información, dejando como evidencia la publicación de documentos en la intranet y las actas de asistencia a las sesiones respectivas. Ante la detección específica de desconocimiento de las políticas establecidas, se realizarán acciones de refuerzo que aseguren el conocimiento de las mismas", y*
>
> *"Revisión por parte de la Dirección de TIC de la aplicación de las políticas de Seguridad de la información por parte de los usuarios, a través de la Medición del indicador de seguridad de la información propio del SGSI y de acuerdo con la periodicidad de medición de dicho indicador"*

Se evidenció que no se describe para qué realizan los controles, lo cual incrementa la posibilidad de materialización. Lo anterior evidencia incumplimiento al numerales 8.4.1 "Diseño de los controles", del Manual de Gestión del riesgo de TRANSMILENIO S.A. (M-OP-02 V4), que define entre otras cosas, que al momento de definir si un

control o los controles de los mapas de riesgos mitigan de manera a adecuada el riesgo, deben considerar desde la redacción del mismo las siguientes variables:

"Paso 3": Debe indicar cuál es el propósito del control. "El control debe tener un propósito para mitigar la causa de la materialización del riesgo".

- *Para cada causa debe existir un control*
- *Las causas se deben trabajar de manera separada*
- *Un control puede ser tan eficiente que puede ayudar a mitigar varias causas, en esos casos se debe repetir el control asociándolo a la causa que mitiga.*

1.3. Para el Riesgo *"El plan estratégico de Seguridad de la Información (PESI) no se pueda implementar de acuerdo a la hoja de ruta establecida"*, se evidenció debilidad en la ejecución de uno (1) de los cuatro (4) controles los cuales se presentan a continuación:

"La Dirección de TIC elabora y emite periódicamente los documentos asociados al PESI para conocimiento de los usuarios, por medio de la publicación y oficialización que realiza la Oficina Asesora de Planeación en la Intranet Corporativa. La Dirección de TIC´S realizará dos actividades anuales de sensibilización y socialización a los usuarios en relación con las políticas de seguridad de la información, dejando como evidencia la publicación de documentos en la intranet y las actas de asistencia a las sesiones respectivas. Ante la detección específica de desconocimiento de las políticas establecidas, se realizarán acciones de refuerzo que aseguren el conocimiento de las mismas",

Si bien se evidenciaron soportes de sensibilización en seguridad de la información, el 23 de septiembre de 2020 a colaboradores de la Dirección técnica de BRT, el 23 de noviembre de 2020 a colaboradores de la Subgerencia Jurídica y el 9 de diciembre en la cual participaron 126 colaboradores de todas las dependencias, denominada sensibilización de seguridad de la información, no se evidenciaron soportes de una de las dos actividades previstas para la totalidad de los usuarios. Lo anterior deja descubierto el riesgo asociado.

Con lo anterior, tanto la solidez de los controles individuales como la solidez del conjunto de controles para el riesgo "El plan estratégico de Seguridad de la Información (PESI) no se pueda implementar de acuerdo a la hoja de ruta establecida" presenta debilidad, toda vez que la probabilidad y el impacto del nivel de riesgo residual, no son acordes con la realidad del proceso.

Posibles causas identificadas por la Oficina de Control Interno:

1. Desconocimiento de la metodología en TRANSMILENIO S.A. para la gestión y administración del riesgo definida en el M-OP-02 v4

2. Falta de revisión y monitoreo por parte de la Dirección de TIC, a la matriz de riesgos de gestión, específicamente en el diseño de los controles.

Descripción del riesgo:

Inobservancia a la normativa interna en materia de gestión del riesgo

Descripción del impacto:

1. Materialización del riesgo del proceso; particularmente de los relacionados en la matriz de riesgos de gestión de TIC

2. Investigaciones debido a la no aplicación del numeral 8.4.1 "Diseño de los controles" del Manual para la gestión del riesgo en TRANSMILENIO S.A. M-OP-02 versión 4 de noviembre de 2020

Recomendaciones:

1. Revisar, ajustar y actualizar el documento: Anexo 5. Plan de tratamiento de riesgos, que forma parte del proceso gestión de TIC a fin de que se encuentre alineado a la metodología aprobada por la Alta Dirección para la administración y gestión del Riesgo en TRANSMILENIO S.A.

2. Revisar, ajustar y actualizar los controles definidos en el mapa de riesgos de gestión que presentaron debilidad en su diseño.

3. Solicitar asesoría y acompañamiento de la Oficina Asesora de Planeación en la actualización y ajustes de los documentos mencionados.

4. Revisar, ajustar y actualizar en el mapa de riesgos de gestión la solidez individual y en conjunto, de los controles asociados a los riesgos

Hallazgo N° 2 – Alcance insuficiente del SGSI en la Entidad

Descripción del hallazgo o situación encontrada:

El numeral 2 del Plan Estratégico de Seguridad de la Información PESI V.0 (T-DT-006) establece el alcance del SGSI institucional de la siguiente forma:

"TRANSMILENIO S.A. define el alcance de su Sistema de Gestión en Seguridad de la Información (SGSI) y del PESI, en términos de las características de la entidad, su ubicación, sus activos y su tecnología, así:

TRANSMILENIO S.A adopta, establece, implementa, opera, verifica y mejora el SGSI para el proceso estratégico Gestión de TIC.

Asimismo, el SGSI se ira implementado y adoptando a cada uno de los procesos de manera gradual.

Conforme a esta delimitación de alcance, la implementación de los controles establecidos en el marco del Modelo de Seguridad y Privacidad de la Información del MINTIC (los cuales se encuentran alineados con la norma ISO27000) solo resultan aplicables a los activos de información que son gestionados o gobernados por la Dirección de TIC y excluye implícitamente a aquellos activos (incluidos los sistemas de información) que son gestionados por las demás dependencias de la Entidad.

Aunque durante el año 2020, la Dirección de TIC llevó a cabo gestiones para incorporar los procesos de Subgerencia Jurídica y Supervisión y Control de la Operación del SITP (perteneciente a la Dirección Técnica de Seguridad) como parte del alcance del SGSI, en la actualidad ambos procesos se encuentran al margen del alcance descrito dado que el

numeral 2 del Plan Estratégico de Seguridad de la Información solo considera al proceso de la Dirección de TIC dentro del alcance.

A manera de ejemplo, de los 40 sistemas de información con que cuenta la Entidad y que figuran en el Catálogo de Sistemas de Información V 3.1., 25 de ellos (es decir, el 62,5%) corresponden a sistemas cuyo responsable técnico no es la Dirección de TIC, y, por lo tanto, se encuentran excluidos dentro de la declaración de alcance del SGSI de la Entidad. Conforme a las indagaciones realizadas por la Oficina de Control Interno con la Dirección de TIC, para los anteriores sistemas dicha dependencia no realiza acciones de monitoreo que validen el cumplimiento de las políticas de seguridad de la información formalmente establecidas (en el Anexo 1 del presente informe se indican los responsables técnicos de los 40 sistemas de información existentes).

La anterior situación contraviene lo establecido en el numeral 4 del documento de MINTIC "Modelo de Seguridad y Privacidad de la Información" versión 3.0.2., el cual señala que: *"Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, se trabaja en el fortalecimiento de la seguridad de la información en las entidades, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación colombiana"*, es decir que el Modelo de Seguridad y Privacidad de la información debe procurar la protección de la información al interior de la entidad y no solamente de aquella cuyo responsable técnico es el área de tecnología.

Por otro lado, el alcance del SGSI mencionado en el PESI tampoco corresponde con lo establecido en el literal 8. Políticas de Seguridad de la Información del manual de políticas de seguridad y privacidad de la información V3, el cual señala que: *"Las políticas de seguridad de la información conceptualizan el modelo de manejo de los recursos tecnológicos, humanos, datos y físicos de TRANSMILENIO S.A., en los roles de funcionarios públicos, oficiales, proveedores, contratistas y terceras partes que manejan administran y custodian la información"*; es decir, que establece como alcance de las políticas de seguridad de la información a toda la Entidad.

Posibles causas identificadas por la Oficina de Control Interno:

1. No se asigna a la Dirección de TIC la responsabilidad técnica de todos los sistemas de información de la Entidad.

2. Debilidad en la gestión y administración del riesgo de seguridad de la información por parte de la Dirección de TIC, toda vez que se limita el alcance del Sistema de Gestión de Seguridad de la información corporativo al proceso de Gestión de TIC.

Descripción del riesgo:

1. Imposibilidad del grupo de seguridad de la información para identificar eventuales incumplimientos de las políticas de seguridad de la información.

2. Incumplimiento de los controles de seguridad de la información en las diferentes dependencias de la Entidad.

Descripción del impacto:

1. Afectación del cumplimiento del objetivo misional de la Entidad por la incapacidad de identificar y corregir oportunamente eventuales incumplimientos o desviaciones al cumplimiento de las políticas y directrices de seguridad de la información para aquellos sistemas de información cuyo responsable técnico no es la Dirección de TIC.

2. Sanciones y Multas para la Entidad.

3. Incumplimiento normativo y de las directrices impartidas por los diferentes órganos de control del Estado (MINTIC y DAFP entre otros)

Recomendaciones:

1. Ajustar el alcance del SGSI que se encuentra establecido en el PESI de forma que éste considere a la totalidad de los procesos de la Entidad y no únicamente al proceso de Gestión de TIC.

2. Llevar a cabo un diagnóstico del cumplimiento de las políticas de seguridad de la información por parte de los responsables técnicos de los sistemas de información en las diferentes dependencias de la Entidad con el apoyo de la dirección de TIC, acompañándolas en el proceso de cierre de las eventuales brechas de seguridad identificadas.

3. Establecer por parte de la Dirección de TIC, un plan de monitoreo y supervisión periódica del cumplimiento de las políticas de seguridad de la información por parte de las áreas que ejercen como responsables técnicos de los sistemas de información existentes.

4. Incluir en el mapa de riesgos de gestión de la Dirección de TIC, los riesgos asociados al posible incumplimiento de las políticas de seguridad de la información por parte de las diferentes dependencias que son responsables técnicos de los sistemas de información hasta que finalice el proceso de diagnóstico, cierre de brechas e implementación del proceso periódico de monitoreo del cumplimiento de las políticas de seguridad de la información por parte de las dependencias que son responsables técnicos de los sistemas de información.

Hallazgo N° 3 – Desactualización del Plan de Cultura y sensibilización en seguridad de la información y debilidades en la cobertura de las sesiones de sensibilización de éste.

Descripción del hallazgo o situación encontrada:

a. Como resultado de la revisión efectuada al Plan de Cultura y Sensibilización del Sistema de Gestión de Seguridad de la Información SGSI (T-DT-007) Ver 0 de agosto de 2018 se evidenció que no se está dando cumplimiento al numeral 3.5.3. "Evaluación y renovación del plan de cultura de sensibilización del SGSI", el cual señala que:

"El Plan de Cultura y Sensibilización del SGSI de la Entidad, debe ser revisado y actualizado al inicio del año; teniendo en cuenta los resultados del año anterior con base en los indicadores de cumplimiento obtenidos".

Aunque la Dirección de TIC suministró para nuestra evaluación un documento Word denominado "Plan de Cultura y Sensibilización en Seguridad de la Información V1 (fechado en septiembre de 2020), éste no se encontraba publicado en la Intranet; tampoco se aportó evidencia de su aprobación por parte del comité de Gestión y Desempeño, tal como lo establece el literal b de la política de cultura y sensibilización en seguridad de la información, contenida en el Manual de Políticas de Seguridad de la Información V3 (M-DT-001), el cual señala:

"(…)
Para realizar el contenido de los Programas o Planes de Cultura y Sensibilización de Seguridad de la Información deben enmarcarse en tres (3) fases:

- *Diseño. Deben ser diseñados teniendo en cuenta la misión de la entidad, identificación de las necesidades y prioridades (verificación de Incidentes de Seguridad), elaboración de indicadores o métricas de desempeño que permitan generar resultados.*

- *Desarrollo. Elaborar material de entrenamiento en el que se pueda emplear una buena pedagogía para la difusión de los temas de Seguridad y este debe ser sometido a aprobación por el comité integrado de Gestión SIG (hoy Comité Institucional de Gestión y Desempeño), antes de la puesta en marcha.*

- *Implementación. Socializar el programa o Plan de Cultura Sensibilización de Seguridad de la Información de la entidad que fue diseñado y desarrollado al igual que emplear los indicadores o métricas para evaluar el desempeño del Programa o Plan.*

(…)"

Dado que el citado Plan no ha tenido un proceso de revisión ni actualización formal por parte de la Dirección de TIC para los años 2019, 2020 y 2021, las actividades de cultura y sensibilización adelantados durante dicho período por la Dirección de TIC sobre Seguridad de la Información se encuentran al margen de un Plan de Cultura y

Sensibilización de Seguridad de la Información formalmente establecido. Cabe señalar que, conforme a las validaciones realizadas por la Oficina de Control Interno, en el año 2020 la Dirección de TIC gestionó ante la Dirección Corporativa, la incorporación dentro del Plan Institucional de Capacitación, actividades de sensibilización en temas de seguridad de la información.

b. Limitación en la cobertura de las gestiones de cultura y sensibilización en seguridad de la información adelantadas por la Dirección de TIC durante el 2020:

Conforme a la documentación aportada por la Dirección de TIC sobre las gestiones adelantadas por dicha dependencia durante el 2020 para fomentar la cultura y sensibilización en seguridad de la información, fueron adelantadas las siguientes actividades:

- Charla de políticas de seguridad de la Información realizada el 9 de diciembre de 2020 dirigida al personal de la Entidad (registro de asistencia de 126 personas)

- Sensibilización en seguridad de la información realizada el 23 de septiembre de 2020 a la Dirección Técnica de BRT (registro de asistencia de 61 personas),

- Sensibilización en seguridad de la información realizada el 23 de noviembre de 2020 a la Subgerencia Jurídica realizada (registro de asistencia de 18 personas), y

- Presentación de los resultados de las pruebas de Ingeniería Social e Informe Sensibilización, por parte de la firma Password, en desarrollo del contrato 772 de 2019 cuyo objeto es: "Contratar la prestación de servicios a través de una empresa especializada, para la realización de un test de intrusión (Ethical hacking), con el fin de detectar las posibles vulnerabilidades de seguridad de la red de datos de TRANSMILENIO S.A., en los segmentos que el ente gestor determine". Aunque el período de vigencia del contrato fue entre el 18 de diciembre de 2019 y el 17 de febrero de 2020, la documentación aportada no precisa la fecha en que fue realizada dicha socialización; tampoco se indica quiénes conformaron el auditorio de la charla debido a que no fue aportado el registro de asistencia correspondiente.

Teniendo en cuenta que el numeral 2.1. del Plan de Cultura y Sensibilización del Sistema de Gestión de Seguridad de la Información SGSI (T-DT-007) V0 vigente en la Entidad señala como objetivo general:

> *"Sensibilizar y crear conciencia al personal TRANSMILENIO, frente a las buenas prácticas de Seguridad de Información, con el fin de proteger y resguardar los activos de Información a través de campañas y estrategias definidas en el Plan de Cultura de Sensibilización del SGSI".*

Y que el numeral 2.2. indica que el objetivo específico del Plan es:

- *Definir campañas de sensibilización para TRANSMILENIO S.A.*
- *Utilizar los medios de difusión institucionales como herramientas para fomentar el Plan de Cultura de Sensibilización del "SGSI" de la entidad.*
- *Promover las campañas de sensibilización al interior de la Entidad.*
- *Definir encuestas y evaluaciones para medir la percepción de la Seguridad de la información en los funcionarios, contratistas, proveedores y/o terceros de TRANSMILENIO S.A.*

Con lo anterior, falta dar total cobertura a los colaboradores de la entidad, teniendo en cuenta que el número de personas con que contaba la entidad al 31 de diciembre de 2020, es de un total de 1214 (833 contratistas, 362 trabajadores oficiales y 18 empleados públicos existentes en el 2020), la cobertura dada corresponde al 10,38% del total de personal.

Posibles causas identificadas por la Oficina de Control Interno:

1. Debilidad en la gestión y administración del riesgo de seguridad de la información por parte de la Dirección de TIC, toda vez que no se llevan a cabo evaluaciones y renovaciones anuales del plan de cultura de sensibilización del SGSI conforme a lo establecido.

2. Poca concientización por parte de los colaboradores de la Entidad frente a los riesgos y amenazas de seguridad de la información que pueden presentarse o a su responsabilidad para cumplir con las políticas de seguridad de la información.

Descripción de los riesgos:

1. Incumplimiento de las políticas de seguridad de la información por parte de la Dirección de Tecnología.

2. Inobservancia a la normatividad aplicable en términos de SGSI

Descripción del impacto:

1. Afectación del cumplimiento del objetivo misional de la Entidad por incumplimientos de las políticas y directrices de seguridad de la información.

2. Sanciones y Multas para la Entidad.

3. Incumplimiento normativo y de las directrices impartidas por los diferentes órganos de control del Estado (MINTIC y DAFP entre otros)

Recomendaciones:

1. Llevar a cabo revisiones y actualizaciones anuales del Plan de Cultura y Sensibilización del SGSI establecido conforme lo menciona el propio Plan de Cultura y Sensibilización del Sistema de Gestión de Seguridad de la Información SGSI (T-DT-007) que se encuentra vigente en la actualidad.

2. Establecer e implementar instancias de supervisión anual del cumplimiento de la política de actualización anual del Plan de Cultura y Sensibilización del SGSI.

3. Con el fin de asegurar un nivel adecuado de cobertura y efectividad en las acciones que adelante la Dirección de TIC para fomentar la cultura de sensibilización del SGSI se recomienda:

    a. Diseñar y llevar a cabo diferentes estrategias de comunicación con los colaboradores de la Entidad a fin de socializar los temas previstos de SGSI (teniendo en cuenta que se cuenta tanto con personal administrativo (en sede),

como operativo (en vía), considerando el uso de los diferentes canales y estrategias de comunicación para tal fin.

b. Medir después de cada actividad de sensibilización realizada, el nivel de cobertura alcanzado, teniendo en cuenta el número de asistentes reales frente al número total de invitados, para lo cual se sugiere obtener imágenes o pantallazos que evidencien la cantidad de personas que efectivamente asistieron al evento.

c. Definir un porcentaje de cobertura mínimo anual que deba cumplirse frente a las actividades de sensibilización en SGSI realizadas y medir su cumplimiento durante el desarrollo del Plan de Cultura y Sensibilización establecido. Complementar con actividades adicionales en caso de incumplimiento de la meta establecida.

d. Llevar a cabo evaluaciones a los asistentes de las diferentes charlas de sensibilización realizadas.

4. Solicitar apoyo de la alta Dirección para motivar la participación del personal en los procesos de sensibilización que adelante la Dirección de TIC

5. En futuras ocasiones, coordinar con la Dirección Corporativa la inclusión del plan de Cultura y sensibilización de seguridad de la información en el PIC.

Hallazgo N° 4 – Debilidades en el Plan de Recuperación de Desastres en cuanto pruebas, cobertura, tiempos de restauración y formalización de los roles.

Descripción del hallazgo o situación encontrada:

Como resultado de la revisión efectuada al documento "Plan Gestión de Seguridad de la Información en Continuidad del Negocio V0" (T-DT-011) de enero de 2021 establecido por la Entidad, cuyo objetivo es: "Establecer la gestión de la seguridad de la información en la continuidad del negocio a través del Plan de Recuperación de Desastres de la infraestructura tecnológica de TRANSMILENIO S.A.", se identificaron las siguientes situaciones:

1. Aunque la Dirección de TIC dispone de mecanismos tecnológicos de control importantes que soportan de manera transversal los diferentes procesos corporativos, minimizando posibles impactos en escenarios de recuperación de desastres, algunos de los cuales se listan en el Anexo 3 del presente informe, conforme a las indagaciones realizadas con la Dirección de TIC, el mencionado Plan no ha sido probado integralmente, hecho que, además de limitar el cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) en el numeral A.17.1.3 (verificación, revisión y evaluación de la continuidad de la seguridad de la información), genera incertidumbre sobre la efectividad del mismo en caso de presentarse una contingencia que llegue a afectar severamente las instalaciones, la infraestructura de TI, los sistemas de información y los datos que apoyan los procesos críticos de negocio.

2. Conforme lo señala el documento, al momento de su publicación, la Dirección de TIC había evaluado la estrategia de contingencia para los servicios de Directorio Activo, DNS y DHCP, Switch de Core y Conectividad, Firewall, canales de internet, Bases de datos de los Sistemas de Información de APRA, JSP7, T-DOC, CORDIS, y Proactivanet respectivamente, los cuales, de acuerdo con el catálogo de sistemas de información versión 3, forman parte de la responsabilidad técnica de la Dirección de TIC. De esta forma, se encuentra pendiente validar la estrategia de contingencia para los demás sistemas de información que soportan los procesos críticos de negocio, hecho que también afecta el cumplimiento del MSPI en el numeral A.17.1.3 y genera incertidumbre sobre los resultados de dicha estrategia para los servicios no probados.

3. En el numeral 11 del documento se presenta una tabla con tiempos y momentos de recuperación (ver Anexo 2) (RPO o volumen de datos en riesgo de pérdida que la Entidad considera tolerable, y RTO o el tiempo durante el cual la Entidad pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio). En este numeral se presenta la siguiente nota:

   "TRANSMILENIO S.A contempla actualmente los tiempos como deseables para proporcionar los servicios de manera óptima. Sin embargo, si no se cuenta con la estrategia de recuperación implementada, entonces el RTO se alinea con los valores definidos en la tabla de "Retorno a la normalidad".

Teniendo en cuenta que la determinación del RTO real puede diferir del RTO deseado que se presenta en el Anexo 2, y que esta variable, junto con el RPO constituyen uno de los pilares fundamentales del diseño de un Plan de Recuperación de Desastres (debido a que tanto las estrategias como las actividades de recuperación de los servicios deben diseñarse y probarse de forma que aseguren su cumplimiento), se advierte que los RTO sobre los cuales se basa el DRP existente son deseados (es decir, no necesariamente reales) para cada uno de los procesos críticos de negocio, por lo que no habría certeza de que los tiempos realmente empleados por la Dirección de TIC para restaurar a condiciones de normalidad cualquier servicio afectado de un proceso crítico de negocio será tolerable para la Entidad. Así las cosas, y mientras la Entidad no defina los RTO reales por cada proceso crítico, ni se ajusten los procedimientos para asegurar la restauración de los servicios dentro de estos tiempos, será incierto el nivel de aceptación de los tiempos que efectivamente pueda tomar la Dirección de TIC para restaurar los servicios.

Las situaciones anteriores podrían implicar un incumplimiento de la Política de Gestión de Continuidad del Negocio y la Recuperación de Desastres (DRP), mencionada en el numeral 6 del Plan de Gestión de la Seguridad de la Información en la Continuidad del Negocio (T-DT-011) V0, la cual menciona:

> *"TRANSMILENIO S.A adelantará las gestiones necesarias para que los servicios tecnológicos críticos soportados por la Dirección de TIC se recuperen en los tiempos objetivo, definidos por la entidad y ante la ocurrencia de un incidente significativo que los afecte parcial o totalmente. Lo anterior, alineado con la política de Continuidad de Negocio que se encuentra dentro del Manual M-DT-001- Políticas de Seguridad y Privacidad de la Información, en su numeral: 9.9 POLÍTICA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO".*

4. El literal 7.2. "Roles Frente a la Continuidad de Negocio y la Recuperación de Desastres" establece los roles correspondientes para los líderes de proceso, funcionarios y Contratistas de la Dirección de TIC, Director de TIC, para el Profesional Especializado Grado 6 – Seguridad Informática (Oficial de Seguridad de la Información), para el Profesional Especializado Grado 6 – Coordinador de Procesos Corporativos, así como para otros contratistas y terceros, antes y después de un evento

de continuidad del negocio; sin embargo, no se encuentran formalmente establecidos los procedimientos respectivos a cada uno de estos roles, por lo que se desconoce la eficacia de los mismos.

Posibles causas identificadas por la Oficina de Control Interno:

1. Debilidad en la gestión y administración del riesgo de seguridad de la información por parte de la Dirección de TIC, toda vez que no se ha probado el Plan de Recuperación de Desastres en aquellos escenarios de riesgo de mayor probabilidad de ocurrencia o de mayor impacto para los procesos críticos de la Entidad (incluidos los sistemas de información que soportan dichos procesos).

2. Falta de articulación con la Oficina Asesora de Planeación en lo concerniente a disponer de los RTO y los RPO reales de cada proceso crítico de negocio, conforme al Plan de Continuidad del Negocio en proceso de elaboración.

3. Debilidad en la documentación, implementación y publicación del DRP en relación con los procedimientos correspondientes a los diferentes roles que fueron establecidos para atender el Plan de Recuperación de Desastres.

Descripción del riesgo:

Posible pérdida en la continuidad del negocio, materializado en uno o más de los procesos críticos de la Entidad

Descripción del impacto:

1. Pérdida de información y de registros automatizados, que podrían afectar el cumplimiento de los objetivos estratégicos de la entidad.

2. Pérdida de credibilidad en el cumplimiento de los objetivos misionales o estratégicos

3. Investigaciones por posibles incumplimientos derivados en la pérdida continuidad de la operación por un tiempo inaceptable.

4. Incumplimiento normativo y de las directrices impartidas por los diferentes órganos de control del Estado (MINTIC y DAFP entre otros)

Recomendaciones:

1. Llevar a cabo mesas de trabajo con la Oficina Asesora de Planeación y con los líderes de los procesos críticos de negocio, con el fin de definir los RPO y los RTO reales o aceptables, y de esta forma, ajustar los procedimientos que debe adelantar la Dirección de TIC para asegurar la restauración de las condiciones mínimas de operación de los procesos, dentro de los tiempos de recuperación establecidos.

2. Programar y ejecutar pruebas al Plan de Recuperación de Desastres, considerando dentro de su alcance, posibles escenarios de pérdida de continuidad derivado de daños en componentes tecnológicos que soportan los procesos críticos de negocio; ajustar el DRP en lo pertinente, de acuerdo con los resultados obtenidos en las pruebas realizadas al mismo.

3. Llevar a cabo los ajustes del caso al Plan de Recuperación de Desastres, validando que el personal se encuentre debidamente capacitado y entrenado para atender cualquiera de las contingencias previstas en el mismo y asegurando que se dé cobertura total a los procesos críticos de la Entidad.

4. Someter a aprobación por parte de la Alta Dirección (Comité Institucional de Gestión y Desempeño) el documento del DRP establecido, a fin de garantizar su apoyo.

5. Efectuar revisiones y mantenimientos periódicos al DRP y ajustarlo de igual forma, en caso de presentarse cambios en la arquitectura tecnológica existente o cualquier otra circunstancia que lo amerite.

Hallazgo N° 5 – Debilidades en la aplicación normas de seguridad en el Data Center y en el cuarto de suministro UPS

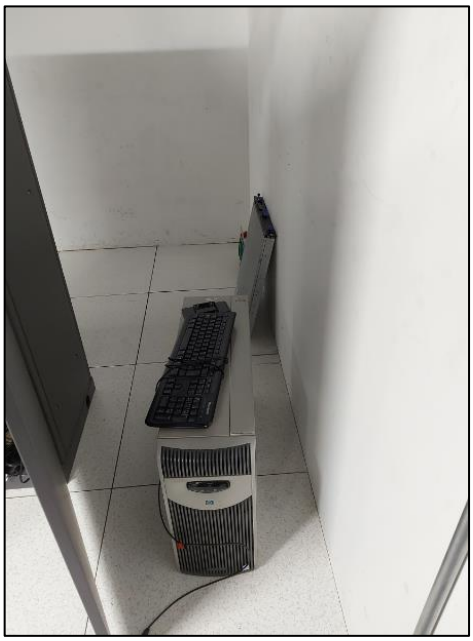
Descripción del hallazgo o situación encontrada:

a. **Situación identificada en el Data Center:** Como resultado de la visita realizada al data center de la Entidad el 11 de mayo de 2021, se identificaron los elementos de protección que se listan en el Anexo 4 del presente informe y que están dirigidos a favorecer la seguridad de los activos tecnológicos existentes en el lugar; sin embargo, en su interior también fueron encontrados los siguientes elementos que no guardan el orden esperado, y podrían propiciar incidentes y/o accidentes de trabajo, así como conatos de incendio que afectarían negativamente la salud y seguridad laboral en la sede administrativa de la Entidad. Dichos elementos obstaculizan algunos pasillos en la circulación normal del personal técnico requerido para atender con prontitud cualquier situación que demande su presencia inmediata en el lugar:

Puertas de gabinete de rack (dificulta la libre circulación del personal)

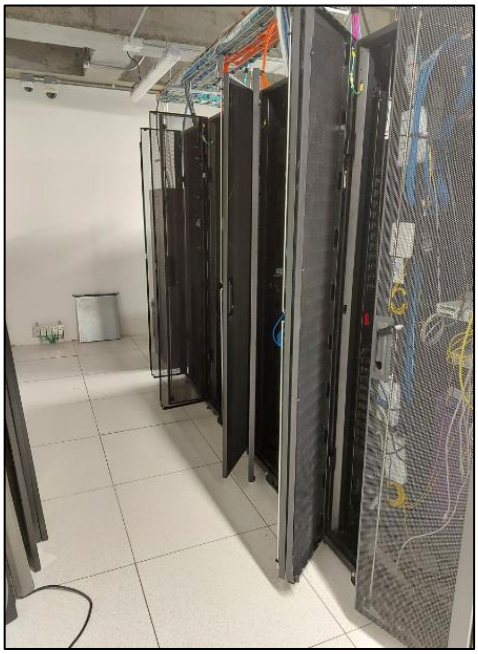
Tabletas de piso falso, paneles de rack, componentes tecnológicos (dificultan la libre circulación del personal)

Gabinet con el rótulo: "Servidor de BD Operaciones" (inadecuada protección de los activos tecnológicos, posible pérdida de información, dificulta la libre circulación del personal)



Gabinete de un computador, teclado de computador y gabinete tipo *blade* (inadecuada protección de los activos tecnológicos, posible pérdida de información, dificultan la libre circulación del personal)

Gabinete de UPS (inadecuada protección de los activos tecnológicos, posible pérdida de información, dificulta la libre circulación del personal)



Puertas de los gabinetes rack abiertas UPS (inadecuada protección de los activos tecnológicos, posible pérdida de información, dificulta la libre circulación del personal)

b. **Situación identificada en el Cuarto de Suministro UPS:** En la misma visita del 11 de mayo de 2021, la Oficina de Control Interno también inspeccionó el cuarto de suministro UPS, contiguo al Data Center, en el cual también fueron identificados

elementos que, además de no formar parte integral del sitio, propician la materialización de incidentes y accidentes de trabajo, podrían facilitar la existencia de un conato de incendio, dado que algunos de ellos están compuestos de material inflamable. Aunque el sitio está protegido por un sistema de detección y extinción contra incendios, la situación identificada constituye un factor de riesgo, no solo sobre los equipos que aseguran el fluido eléctrico de la Entidad, sino sobre las personas que deben atender este tipo de incidentes.

Cajas de cartón en la parte posterior de la UPS (generan riesgo de conato de incendio, no forma parte integral del lugar y afectan el orden y la libre circulación del personal requerido para atender una eventual contingencia eléctrica)

Dos carreteles de madera (favorecen la aparición conatos de incendio) y un rollo de cable (no forma parte integral del lugar). Ambos afectan el orden y la libre circulación del personal requerido para atender una eventual contingencia eléctrica.

Secciones de lámina (no forman parte integral del lugar, dificultan la libre circulación del personal requerido para atender una eventual contingencia eléctrica)

Cajas de cartón (genera riesgo de conato de incendio, no forma parte integral del lugar y afectan el orden y la libre circulación del personal requerido para atender una eventual contingencia eléctrica)

Las anteriores situaciones contravienen lo establecido en las siguientes normas:

- Numeral 6 del Plan de Gestión de la Seguridad de la Información en la Continuidad del Negocio (T-DT-011) V0, el cual menciona:

  "TRANSMILENIO S.A adelantará las gestiones necesarias para que los servicios tecnológicos críticos soportados por la Dirección de TIC se recuperen en los tiempos objetivo, definidos por la entidad y ante la ocurrencia de un incidente significativo que los afecte parcial o totalmente. Lo anterior, alineado con la política de Continuidad de Negocio que se encuentra dentro del Manual M-DT-001-Políticas de Seguridad y Privacidad de la Información, en su numeral: 9.9 POLÍTICA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO".

- Numeral A.17.1.3 del Modelo de Seguridad y Privacidad de la Información, denominado Verificación, revisión y evaluación de la continuidad de la seguridad de la información, el cual, de acuerdo con la norma ISO27001, implica revisar periódicamente la aplicabilidad de los controles, el alcance del plan de continuidad en el sentido en que no queden nuevos activos de información fuera del plan de continuidad y revisar la

implicación del personal en las tareas de recuperación verificando que todo el mundo esté al tanto de sus responsabilidades al respecto.

- Literal d. del numeral 8.9.2 "Seguridad de oficinas, recintos e instalaciones", el cual señala: "Todas las oficinas de la entidad que procesen almacenen y/o gestionen información reservada o sensible deben implementar y adoptar las medidas tendientes a asegurar dicha información"
- Literal g. del numeral 8.9.2 "Seguridad de oficinas, recintos e instalaciones", el cual señala: *"Los materiales peligrosos o combustibles deben ser almacenados de manera segura a una distancia prudente de las áreas seguras. Los suministros como papelería no deben almacenarse en áreas seguras hasta que sea requerido".*
- Artículo 2.2.46.24 *"medidas de prevención y control" Decreto 1072 de 2015,* que define lo siguiente: …

- *"Las medidas de prevención y control deben adoptarse con base en el análisis de pertinencia, teniendo en cuenta el siguiente esquema de jerarquización: 1. Eliminación del peligro/riesgo: Medida que se toma para suprimir (hacer desaparecer) el peligro/riesgo; 2. Sustitución: Medida que se toma a fin de remplazar un peligro por otro que no genere riesgo o que genere menos riesgo; 3. Controles de Ingeniería: Medidas técnicas para el control del peligro/riesgo en su origen (fuente) o en el medio, tales como el confinamiento (encerramiento) de un peligro o un proceso de trabajo, aislamiento de un proceso peligroso o del trabajador y la ventilación (general y localizada), entre otros; 4. Controles Administrativos: Medidas que tienen como fin reducir el tiempo de exposición al peligro, tales como la rotación de personal, cambios en la duración o tipo de la jornada de trabajo. Incluyen también la señalización, advertencia, demarcación de zonas de riesgo, implementación de sistemas de alarma, diseño e implementación de procedimientos y trabajos seguros, controles de acceso a áreas de riesgo, permisos de trabajo, entre otros; (…)"*

  PARÁGRAFO 2. El empleador o contratante debe realizar el mantenimiento de las instalaciones, equipos y herramientas de acuerdo con los informes de inspecciones y con sujeción a los manuales de uso y PARÁGRAFO 4. El empleador o contratante debe corregir las condiciones inseguras que se presenten en el lugar de trabajo, de acuerdo con las condiciones específicas y riesgos asociados a la tarea".

Posibles causas identificadas por la Oficina de Control Interno:

1. Uso no adecuado del Data Center, llevando elementos que pueden generar accidentes, incidentes de trabajo

2. Uso no adecuado del cuarto de suministro UPS (cuarto eléctrico), llevando elementos que pueden generar connato de incendio.

3. El control de acceso al cuarto eléctrico no se encuentra gestionado por una única dependencia: tanto el personal de la Dirección Corporativa como de la Dirección de TIC tienen acceso al lugar, lo cual dificulta la implementación de los controles de seguridad industrial.

Descripción del riesgo:

1. Posibilidad de que se presente un accidente sobre las personas o un incendio en el cuarto de suministro UPS

2. Pérdida en la continuidad en el fluido eléctrico con posible efecto sobre la continuidad del negocio ocasionada por connato de incendio en el cuarto de suministro de la UPS.

Descripción del impacto:

1. Pérdida de información en los sistemas de información que residen en los servidores ubicados en el centro de cómputo y daño en los equipos ante una posible conflagración.

2. Pérdida de credibilidad en el cumplimiento de los objetivos misionales o estratégicos

3. Investigaciones debido a incumplimientos derivados en la pérdida continuidad de la operación por un tiempo inaceptable.

4. Incumplimiento normativo y de las directrices impartidas por los diferentes órganos de control del Estado (MINTIC y DAFP entre otros)

Recomendaciones:

1. Retirar del centro de cómputo y del cuarto de control eléctrico los elementos mencionados en el hallazgo.

2. Prohibir la incorporación de material no relacionado con la operación del lugar y que pueda llegar a afectar negativamente la seguridad de los activos tecnológicos existentes y la salud y seguridad de los colaboradores de la entidad.

3. Implementar acciones periódicas de supervisión y control sobre el cumplimiento de las medidas de seguridad aplicables al Data Center y al cuarto de suministro UPS, dejando evidencia documentada sobre la aplicación del control.

4. Coordinar con la Dirección Corporativa el cumplimiento y la verificación periódica de las medidas de seguridad que deben adoptarse en cuarto de suministro UPS, asignando responsables de dicho control.

Hallazgo N° 6 – Carencia de un Plan de Servicios Ciudadanos Digitales al interior de la Entidad

Descripción del hallazgo o situación encontrada:

La Entidad no dispone de un plan de acción para la implementación de Servicios Ciudadanos Digitales conforme lo exige el numeral 3.1. del MANUAL DE GOBIERNO DIGITAL. Este habilitador busca que todas las entidades públicas implementen lo dispuesto en el Decreto 1413 de 2017, que establece los lineamientos para la prestación de los servicios ciudadanos digitales y para permitir el acceso a la administración pública a través de medios electrónicos. En dicho Decreto los servicios digitales se clasifican en: servicios básicos, autenticación biométrica, autenticación con cédula digital, autenticación electrónica, carpeta ciudadana e interoperabilidad, los cuales son de obligatorio uso y adopción; y servicios especiales, que son adicionales a los servicios básicos, como el desarrollo de aplicaciones o soluciones informáticas para la prestación de los servicios ciudadanos digitales básicos. El diseño de servicios ciudadanos digitales se encuentra también soportado en la Ley 1955 de 2019 y en el Plan Nacional de Desarrollo.

Tal como lo establece la Guía para el diseño de Servicios Ciudadanos Digitales, se espera que el Plan Institucional de cada entidad pública desarrolle los servicios digitales a través de la conceptualización, diseño y evaluación de los servicios, apalancando los servicios base (Interoperabilidad, Carpeta Ciudadana y Autenticación Digital) y las capacidades propuestas por la Política de Gobierno Digital, incluyendo Arquitectura y Seguridad, para lo cual se debe:

- Comprender las necesidades del ciudadano
- Abordar la experiencia del ciudadano de principio a fin
- Desarrollar un servicio simple e intuitivo
- Apalancar la prestación del servicio con los servicios ciudadanos digitales base
- Construir el servicio usando prácticas ágiles e iterativas
- Interactuar con los demás actores del ecosistema
- Atraer equipos de trabajo experimentados
- Escoger una estructura de tecnología moderna
- Automatizar pruebas y despliegues
- Fomentar seguridad y privacidad a través de los procesos, y
- Mejora continua de los servicios

Posibles causas identificadas por la Oficina de Control Interno:

1. Posible desconocimiento de la normatividad relacionada con la política de Gobierno Digital

2. Debilidad en la gestión de cumplimiento regulatorio relacionada con temas de la gestión de TI

3. Falta de actividades encaminadas a diseñar, documentar, publicar, implementar y mantener el Plan de acción para la implementación de Servicios Ciudadanos Digitales

Descripción del riesgo:

Incumplimiento de las normativas legales aplicables, relacionadas con el sector de las TI en materia de Gobierno Digital.

Descripción del impacto:

Investigaciones por incumplimientos de las normas legales de TI aplicables en la Entidad.

Recomendaciones:

Definir, documentar, establecer, implementar y mantener al interior de la Entidad el Plan de acción para la implementación de Servicios Ciudadanos Digitales, en cumplimiento del Manual de Gobierno Digital y del Decreto 1413 de 2017.

Hallazgo N° 7 – Diseño deficiente del Indicador de gestión de TIC NASI

Descripción del hallazgo o situación encontrada:

Se evidenció debilidad en el diseño de algunas fórmulas del indicador NASI, generando incumplimiento del numeral 6.6 del procedimiento Indicadores de Gestión (P-OP-023-2) de marzo de 2019, el cual señala:

> *Los dueños de cada proceso deben evaluar permanentemente los indicadores en aspectos como medición, forma de cálculo o periodicidad, con objeto de determinar si su cálculo realmente se asocia con el desarrollo del proceso, si los resultados permiten el alcance de los objetivos propuestos o si representan metas de mejora para el proceso.*
>
> *En caso de identificar que el indicador no aporta información asociada con el proceso, que los resultados no permiten evidenciar el alcance de los objetivos o que no representen metas de mejora, deben ser revisados por los líderes de los procesos para que se replanteen total o parcialmente, a través del formato Solicitud de Creación o Modificación de Documentos.*

Las debilidades identificadas también contravienen lo definido en la introducción del Plan Estratégico de Seguridad de la Información en referencia a indicadores de gestión, afectando la determinación de la veracidad y eficacia del indicador NASI y dificultando la toma de acciones de mejora continua por parte de la Dirección de TIC.

A continuación, se presenta el detalle de lo enunciado (para dar claridad del lector, antes de la presentación de las observaciones del indicador NASI, se transcribe una explicación técnica del mismo, la cual se basa en el documento "1. Formula general del indicador.docx" suministrado para nuestra evaluación. Dentro de este contexto, la Oficina de Control Interno utiliza el término "sub indicador" para referirse a los componentes A1 hasta A5 del indicador NASI):

INDICADOR NASI (Nivel de Adopción de Seguridad de la Información)

El indicador NASI es un indicador que busca medir el nivel de adopción del SGSI por parte de la Entidad; fue diseñado por la Dirección de TIC y presentado al Comité Institucional de Gestión y Desempeño el 19 de diciembre de 2019. Está conformado por cinco (5) sub indicadores denominados A1, hasta A5, los cuales miden los siguientes aspectos:

- A1: Nivel de Sensibilización
- A2: Nivel de Motivación
- A3: Nivel de Conocimiento
- A4: Nivel de Aptitud
- A5: Nivel de Constancia

Los anteriores sub indicadores se suman conforme a la siguiente fórmula:

$$NASI = \sum A1, A2, A3, A4, A5$$

Dado que el resultado de cada sub indicador es un porcentaje, éste finalmente se remplaza por el nivel de puntos que describe la siguiente tabla, de forma que el máximo puntaje del indicador NASI es 25 (cada indicador podría tener un valor máximo de 5):

Nivel porcentual resultante	***Nivel en puntos para el indicador***
De 0% a 20%	*1*
De 20.1% a 40%	*2*
De 40.1% a 60%	*3*

De 60.1% a 80%	*4*
De 80.1% a 100%	*5*

Tabla de conversión del sub indicador de porcentaje a puntos. Fuente: Archivo "Formula general del indicador.docx" suministrado por la Dirección de TIC

Con el fin de facilitar la interpretación de las debilidades identificadas por la Oficina de Control Interno, a continuación, se presenta el detalle de los sub indicadores:

A1: Nivel de Sensibilización:

Descripción: *Mide si los usuarios de la entidad son conscientes de la necesidad en la adopción de seguridad de la información. Emplea la siguiente fórmula:*

$$A1 = (V1 \times (0.25) + V2 \times (0.25) + V3 \times (0.5))/V4 \times (100\%)$$

Variables:

V1 = Cantidad de usuarios que han recibido las charlas de sensibilización durante el año.

V2 = Cantidad de usuarios que han recibido sensibilización por medios electrónicos durante el año.

V3 = Cantidad de usuarios que respondieron la encuesta de seguridad con un porcentaje igual o mayor al 80%

V4 = Total de usuarios de la entidad.

Nota: *El resultado será un valor entre 0% y 100%. Por lo tanto, dicho resultado deberá transformarse en la escala 1 a 5, de acuerdo con la siguiente tabla:*

A2: Nivel de Motivación:

Descripción: *Se mide si los usuarios de la entidad se encuentran motivados y desean adoptar la cultura de sensibilización de la información.*

$$A2 = \left(V1 \times (0.5\%) + V2 \times (0.25\%) + V3 \times (0.25\%)\right)$$

Variables:

V1 = Porcentaje de respuesta de encuesta de seguridad de la información

$$V1 = \sum \frac{UR}{UE} \times CE$$

UR: Usuarios que respondieron por cada encuesta

UE: Usuarios a los que se les envió la encuesta

CE: Cantidad de encuestas

V2 = Resultado de la evaluación de control de equipos desatendidos

$$V1 = \sum \frac{ED}{ET} \times CP$$

ED: Equipos desatendidos identificados por cada prueba de recorrido

ET: Equipos Totales

CP: Cantidad de Pruebas de recorrido

V3 = Cantidad de eventos e incidentes de seguridad de la información generados por los usuarios

$$V1 = \frac{IRU}{IT}$$

IRU: Incidentes reportados por los usuarios

IT: Incidentes totales

A3: Nivel de Conocimiento en SI

Descripción: *Se mide si los usuarios cuentan con el conocimiento suficiente para adoptar la seguridad de la información.*

$$A3 = \left(V1 \times (0.5\%) + V2 \times (0.5\%)\right)$$

Variables

V1: Conocimiento en seguridad de la información

$$V1 = \left(\frac{URE - UCB}{UT}\right)$$

URE: Cantidad de usuarios que respondieron la encuesta

UCB: Cantidad de usuarios que respondieron la encuesta con menos del 80%

UT: Cantidad total de usuarios a los que se les envió la encuesta

V2: Porcentaje de implementación *del anexo A (ISO27001:2013) en la entidad. Esto equivale al promedio de porcentajes de implementación de cada control de acuerdo con el análisis GAP.*

A4: Nivel de Aptitud

Descripción: *Se mide si los usuarios tienen la habilidad y capacidad de aplicar los controles al interior de la entidad.*

$$A4 = \left(V1 \times (0.5\%) + V2 \times (0.25\%) + V3 \times (0.25\%)\right)$$

V1: Porcentaje de implementación del anexo A (ISO27001:2013) en la entidad. Esto equivale al promedio de porcentajes de implementación de cada control de acuerdo con el análisis GAP.

V2: Nivel de seguridad de la infraestructura

$$V2 = \left(\frac{VEA}{VT}\right)$$

VEA. Cantidad de vulnerabilidades de nivel Extremo y Alto

VT: Cantidad de vulnerabilidades totales identificadas

V3: Porcentaje de remediación de vulnerabilidades en el año.

A5: Nivel de Constancia

Descripción: *Se mide la constancia de implementación de los controles y buenas prácticas, como un hábito. Lo anterior de acuerdo con los siguientes niveles:*

Nivel resultante de la auditoría	***Nivel en puntos para el indicador***
Óptimo (Optimizado)	*5*
Aceptable (Gestionado)	*4*
Moderado (Definido)	*3*
Inicial (Repetible)	*2*
Inexistente (Inicial)	*1*

Metodología del indicador NASI para la medición de la constancia de implementación de los controles

Resultados de la evaluación:

a. ***Debilidad en el diseño de la variable V1 del sub indicador A2: Nivel de Motivación:***

El componente V1 del indicador A2 no debería afectarse con la multiplicación de la cantidad de encuestas realizadas durante el año, debido a que el resultado del factor "sumatoria de UR / sumatoria de UE" contiene todos los elementos que requiere la medición del indicador. La variable CE incrementa el factor sin un sentido aparente. En caso de que UR=UE, cuando la cantidad de encuestas en el año es mayor que 1 el resultado del indicador es mayor que 1.

b. ***Debilidad en el diseño de la variable V2 del sub indicador A2: Nivel de Motivación:***

- El nombre de la variable "V1" está errada; corresponde a "V2"

- El componente V2 del indicador A2 no debería afectarse con la multiplicación de la cantidad de pruebas de recorrido realizadas durante el año, debido a que el resultado del factor "sumatoria de ED / sumatoria de ET" contiene todos los elementos que requiere la medición del indicador. La variable CP incrementa el factor sin un sentido aparente.

- El cociente V2 tiene un sentido inverso al esperado, debido a que, al aumentar el número de equipos desatendidos, aumenta también el resultado de la variable, lo cual es un contrasentido, si se tiene en cuenta que lo que se está midiendo es lo opuesto a una adecuada gestión en seguridad de la información.

- En caso de que ED=ET, cuando la cantidad de pruebas de recorrido realizadas en el año sea mayor que 1 el resultado del indicador será mayor que 1, es decir que el resultado no es un factor, porque al realizar la sumatoria el resultado sería 1 + el valor del cociente, lo que afecta el cumplimiento del objetivo del indicador NASI.

c. ***Debilidad en el diseño de la variable V3 del sub indicador A2: Nivel de Motivación:***

El nombre de la variable “V1” está errada; corresponde a “V3”

d. ***Debilidad en el diseño del Sub indicador A2: Nivel de Motivación:***

No es clara la asignación porcentual o peso asignado a las variables V1, V2 y V3 del indicador A2, dado que en el documento “1. Formula general del indicador.docx” (el cual presenta una explicación del indicador) no se mencionan los criterios técnicos empleados para asignar dicha ponderación.

e. ***Debilidad en el diseño de la variable V1 del indicador A3: Nivel de conocimiento en SI:***

La variable UT debería corresponder a la cantidad de usuarios que respondieron la encuesta (es decir, URE) y no a la cantidad total de usuarios a los que se les envió, debido a que el resultado del indicador se vería afectado por las personas que no contesten la encuesta, haciendo disminuir el resultado de la variable V1 sin un sentido aparente.

f. ***Debilidad en el diseño de las variables V2 y V3 del Sub indicador A4: Nivel de Aptitud:***

Dado que la variable V2 del sub indicador A4 mide la cantidad de vulnerabilidades de nivel Extremo y Alto / Cantidad de vulnerabilidades totales identificadas, y la variable V3 mide la Cantidad de vulnerabilidades de nivel Extremo y Alto / Cantidad de vulnerabilidades totales identificadas, se advierte que el sentido de ambas variables es opuesto al esperado, dado que su resultado mide condiciones de seguridad negativas desde la perspectiva de seguridad de la información. Teniendo en cuenta que, conforme a la fórmula de A3 ambas variables se computan con la variable V1, la cual mide una condición de seguridad positiva (porcentaje de implementación de la norma ISO27000), no parece lógico desde la perspectiva del resultado, el sentido del sub indicador A4.

g. ***Falta de claridad en la determinación porcentual de las variables que conforman el sub indicador A4: Nivel de Aptitud:***

En la fórmula del sub indicador A4, las variables V1, V2 y V3 tienen cada una asociado un factor o peso relativo, los cuales deben computarse con las variables para obtener el resultado del Sub indicador. El documento que hace la presentación técnica del indicador NASI no explica la justificación de los porcentajes de ponderación utilizados en la fórmula, hecho que puede poner en duda la credibilidad de su resultado.

Posible causa identificada por la Oficina de Control Interno:

Deficiencias en el diseño, implementación, seguimiento y monitoreo de los indicadores de seguridad de la información establecidos por la Dirección de TI.

Descripción del riesgo:

1. Inobservancia a la efectividad en el cumplimiento de las políticas de seguridad de la información formalmente establecidas (dado que el indicador NASI es integral para todo el SGSI, esta inobservancia aplica a la totalidad de las políticas de seguridad de la información establecidas)

2. Dificultada para evaluar la medida en que se están logrando los objetivos estratégicos de seguridad de la información en la Entidad, así como el desempeño de la Entidad frente al cumplimiento de las metas de seguridad de la información.

3. Incumplimiento del numeral 6.6 del procedimiento Indicadores de Gestión (P-OP-023-2) de marzo de 2019 y lo definido en la introducción del Plan Estratégico de Seguridad de la Información en referencia a indicadores de gestión.

Descripción del impacto:

1. Incapacidad para cumplir uno de los retos definidos en la hoja de ruta de seguridad de la información (Anexo 2. Mapa de Ruta de Proyectos Enero 2020.xlsx'), el cual señala:

"Lograr que la Entidad cumpla con las actividades y políticas estipuladas en el Marco de Seguridad de la Información de la Entidad"

2. Multas o sanciones por incumplimientos de metas o de las normas legales de TI aplicables en la Entidad.

3. Dificultar para asegurar una adecuada toma de decisiones en la implementación de acciones correctivas resultantes de la medición de los indicadores de TI y de Seguridad de la Información en la Entidad.

Recomendaciones:

1. Revisar y ajustar el diseño del indicador NASI, a partir de la revisión individual y detallada de cada uno de los indicadores y variables que lo componen. En particular se solicita revisar la pertinencia de sus cálculos individuales y cálculos grupales o de conjunto,

2. Validar la homogeneidad de los indicadores que participan en el indicador NASI (asociando en la formulación solo indicadores cuyo resultado es un factor, y solo indicadores cuyo resultado es un puntaje o un número entero perteneciente a un determinado rango).

OPORTUNIDADES DE MEJORA Y RECOMENDACIONES

1. <u>Insuficiente documentación del MSPI</u>

Llevar a cabo labores de revisión, ajuste y complementación aprobación, publicación, divulgación, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información requerido por la Entidad, considerando la incorporación de los temas presentados en nuestra observación de auditoría.

- Como parte de la revisión efectuada por la Oficina de Control Interno al análisis GAP de la norma ISO27001 adelantado por la Entidad (con corte al 30 de abril de 2021) a través del Instrumento de Diagnostico del MSPI de MINTIC, se evidenció que la Dirección de TIC dispone de los documentos:

- *“Anexo 3. M-DT-001 Manual de Políticas de Seguridad de la Información V.3”*
  En el cual se presenta la política de alto nivel del Sistema de Gestión de Seguridad de la Información (SGSI), el compromiso de la dirección, las autoridades y roles de seguridad de la información, las políticas de seguridad de la información establecidas en la Entidad, así como los responsables de su cumplimiento;

- *“Anexo 4 Plan Estratégico de SI - PESI V.0”*
  En el cual se presentan los objetivos generales y específicos del PESI, su alcance (incluye alcance del SGSI), las etapas del ciclo de vida del SGSI, el contexto de la Entidad, el análisis DOFA, la identificación de las partes interesadas, la metodología del PESI, su alineación con el PETIC y la priorización del portafolio de proyectos.

Con el fin de validar el cumplimiento del Modelo de Seguridad y Privacidad de la Información establecido por el MINTIC en la Entidad, conforme lo establecen las 21 guías que se encuentran publicadas en el sitio https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/, la Oficina de Control Interno realizó revisiones a algunas de ellas identificando las siguientes situaciones:

ASPECTO	DOCUMENTACIÓN EXISTENTE	OBSERVACIÓN
Guía # 4 - Numeral 6.3: Roles y responsabilidades de seguridad de la información	El numeral 7 del “Manual de Políticas de Seguridad de la Información V3” establece las siguientes autoridades y roles de seguridad de la información en la Entidad: - Comité de Coordinación del	a. El Manual de Políticas de Seguridad de la Información no menciona las responsabilidades a cargo de cada una de las autoridades y roles de seguridad de la información descritas, hecho que constituye un vacío en la implementación los controles de seguridad de la información. b. La guía 4 sugiere el conjunto de integrantes para el equipo al interior de las entidades, los cuales difieren de la propuesta mencionada en el Manual de Políticas de Seguridad de la Información:

ASPECTO	DOCUMENTACIÓN EXISTENTE	OBSERVACIÓN
	Sistema Integrado de Gestion (*incluye las* - Funciones del Comité del SGSI) - Profesional Especializado de Seguridad Información - Profesional Especializado - Procesos Corporativos - Operador de seguridad de la información - Propietarios de activos de información - Usuarios de la información	- <u>Responsable de Seguridad de la Información para la entidad</u>: Para este rol, la guía no solo presenta sus responsabilidades en relación con el SGSI, sino su responsabilidad para cada uno de los dominios del marco de Arquitectura Empresarial (servicios tecnológicos, estrategia TI, Gobierno TI, Sistemas de Información, información y Uso y apropiación. - <u>Equipo del Proyecto</u>: al cual deben pertenecer miembros directivos y representantes de las áreas misionales, con el propósito de asegurar que la información relevante de la entidad esté disponible oportunamente. De esta forma se busca asegurar que sea una iniciativa de carácter transversal a la entidad, y que no dependa exclusivamente de la oficina o área de TI. La Guía 4 pone a consideración el siguiente listado para establecer los miembros del equipo de seguridad y privacidad de la información o Personal de seguridad de la información. o Un representante del área de Tecnología. o Un representante del área de Control Interno. o Un representante del área de Planeación. o Un representante de sistemas de Gestión de Calidad. o Un representante del área Jurídica. o Funcionarios, proveedores, y ciudadanos - <u>Comité de seguridad:</u> pueden ser incluidas por el comité Institucional de desarrollo administrativo, como instancia orientadora de la implementación de la estrategia de

ASPECTO	DOCUMENTACIÓN EXISTENTE	OBSERVACIÓN
		Gobierno en línea de acuerdo al señalado en el Art. 2.2.9.1.2.4.
Guía # 12 Guía de seguridad en la nube	El Plan Estratégico de Seguridad de la Información menciona que: "TRANSMILENIO implementó el aprovisionamiento de servicios de plataforma tecnológica en la nube PaaS e IaaS a mediano y largo plazo, por demanda, la cual permite el despliegue de sistemas de información y/o soluciones de software, con la movilidad que proporciona la nube (acceso desde cualquier dispositivo y lugar), generando economías de escala."	La documentación del sistema de gestión disponible en la Dirección de TIC no incluye políticas ni procedimientos relacionados con seguridad en la nube en los términos mencionados en la guía # 12 del MINTIC.

La documentación formalmente establecida por la Dirección de TIC en su sistema de gestión tampoco incluye temas relacionados con la declaración de aplicabilidad, las acciones de monitoreo y medición del desempeño del SGSI, ni los resultados de las revisiones de gestión. Aunque la Dirección de TIC cuenta con un Manual del Sistema de Gestión de Seguridad de la Información en versión borrador, en el cual puede considerarse la incorporación de los temas anteriormente señalados; éste no ha sido aprobado ni se encuentra publicado en la Intranet de la Entidad. Teniendo en cuenta

la importancia de los temas que se encuentran pendientes por documentar, y mientras éstos no se incorporen formalmente al SGSI, se presentará vacío de control que limitará el cumplimiento de los controles de seguridad de la información por parte del personal de la Entidad.

2. <u>Debilidad en el cumplimiento de los lineamientos en materia de Gobierno Digital</u>

Definir, documentar, establecer, implementar y mantener en apoyo con la Alta dirección, la política de Gobierno Digital en los términos del Decreto 1008 de 2018 y bajo el contexto particular de la Entidad

- Aunque en cumplimiento del el Decreto 1008 de 2018 la Entidad ha avanzado en varios aspectos relacionados con la política de Gobierno Digital entre los que se destaca:
  - La existencia de un Plan Estratégico De TI (incluida la gestión de los proyectos de TI)
  - Avances en la implementación de la Arquitectura Empresarial
  - Documentación de los servicios de TI
  - Optimización del proceso de compras de TI
  - Gestión de los sistemas de información
  - Operación de los servicios tecnológicos
  - Adopción del cambio a IPv6
  - Diagnóstico de seguridad de la información, y
  - Plan de tratamiento de riesgos

  La Entidad no cuenta con una política de Gobierno Digital formalmente establecida, en los términos del artículo 2.2.9.1.1.1 del mencionado decreto, el cual señala que esta política debe ser: "*entendida como: el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital"*.

Dado que el contexto de cada entidad es distinto, la declaración de la Política de Gobierno Digital debería enmarcarse dentro de dicho contexto. Adicionalmente, es importante precisar que la política de Gobierno Digital es una de las diecisiete políticas de gestión y desempeño institucional que se debe desarrollar en el marco del MIPG y que tiene como objetivo "*Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital*".

RESULTADOS DEL SEGUIMIENTO AL ANÁLISIS GAP DEL CUMPLIMIENTO DE LA NORMA NTC ISO27001:2013 POR PARTE DE LA ENTIDAD:

La Oficina de Control Interno llevó a cabo una revisión conjunta con la Dirección de TIC al estado de implementación de los 114 controles definidos en la norma NTC ISO27001:2013 con el fin de establecer la brecha entre expectativas del cumplimiento de la norma y la realidad, así como de determinar su estado actual y proyectar las acciones de mejora continua esperadas. La Dirección de TIC puso a disposición de la Auditoría la documentación que evidencia su gestión frente a la adopción de cada uno de los citados controles, los cuales fueron analizados y valorados por la Oficina de Control Interno, con el fin de determinar el grado de avance en la implementación del SGSI por parte de la entidad. Como resultado del seguimiento realizado, en el presente informe se dan a conocer aquellos controles de la norma en los cuales se presentó diferencia entre la valoración realizada por la Dirección de TIC frente al nivel de implementación de cada uno de los 114 controles, frente a la misma valoración realizada por la Oficina de Control Interno. Se advierte, sin embargo, que aquellos controles sobre los cuales no se presentó diferencia en la valoración descrita, y que fueron calificados por la Dirección de TIC con un porcentaje inferior al 100% también presentan un GAP o brecha, que implica la necesidad de fortalecerlos. Las medidas necesarias para el fortalecimiento de los controles corresponden precisamente con aquellos controles sugeridos por la norma ISO27002:2013 que no se encuentran implementados en la Entidad o que su implementación es parcial.

Valoración

Para conocer el nivel de implementación de los 114 controles evaluados, la herramienta Diagnóstico GAP ofrece las siguientes seis (6) posibles valoraciones:

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

Nivel de cumplimiento de los controles de seguridad de la información en la Entidad:

La norma ISO27001:2013 cuenta con 14 dominios, 35 objetivos de control y 114 controles para los que puede asignarse un valor de cumplimiento en porcentaje. Para el caso de TRANSMILENIO S.A., el resultado arrojado en el seguimiento al nivel de implementación de cada dominio de la norma es el siguiente:

ISO	DOMINIO	NIVEL DE CUMPLIMIENTO
A.5	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	90%
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	50%
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	72%
A.8	GESTIÓN DE ACTIVOS	51%
A.9	CONTROL DE ACCESO	65%
A.10	CRIPTOGRAFÍA	40%
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	69%
A.12	SEGURIDAD DE LAS OPERACIONES	61%
A.13	SEGURIDAD DE LAS COMUNICACIONES	56%
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	24%
A.15	RELACIONES CON LOS PROVEEDORES	40%
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	57%

A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	57%
A.18	CUMPLIMIENTO	64%
NIVEL DE CUMPLIMIENTO GENERAL		**58%**

Fuente: Tabla construida por la Oficina de Control Interno basada en la evidencia suministrada por la Dirección de TIC (nivel de cumplimiento validado con la Dirección de TIC)

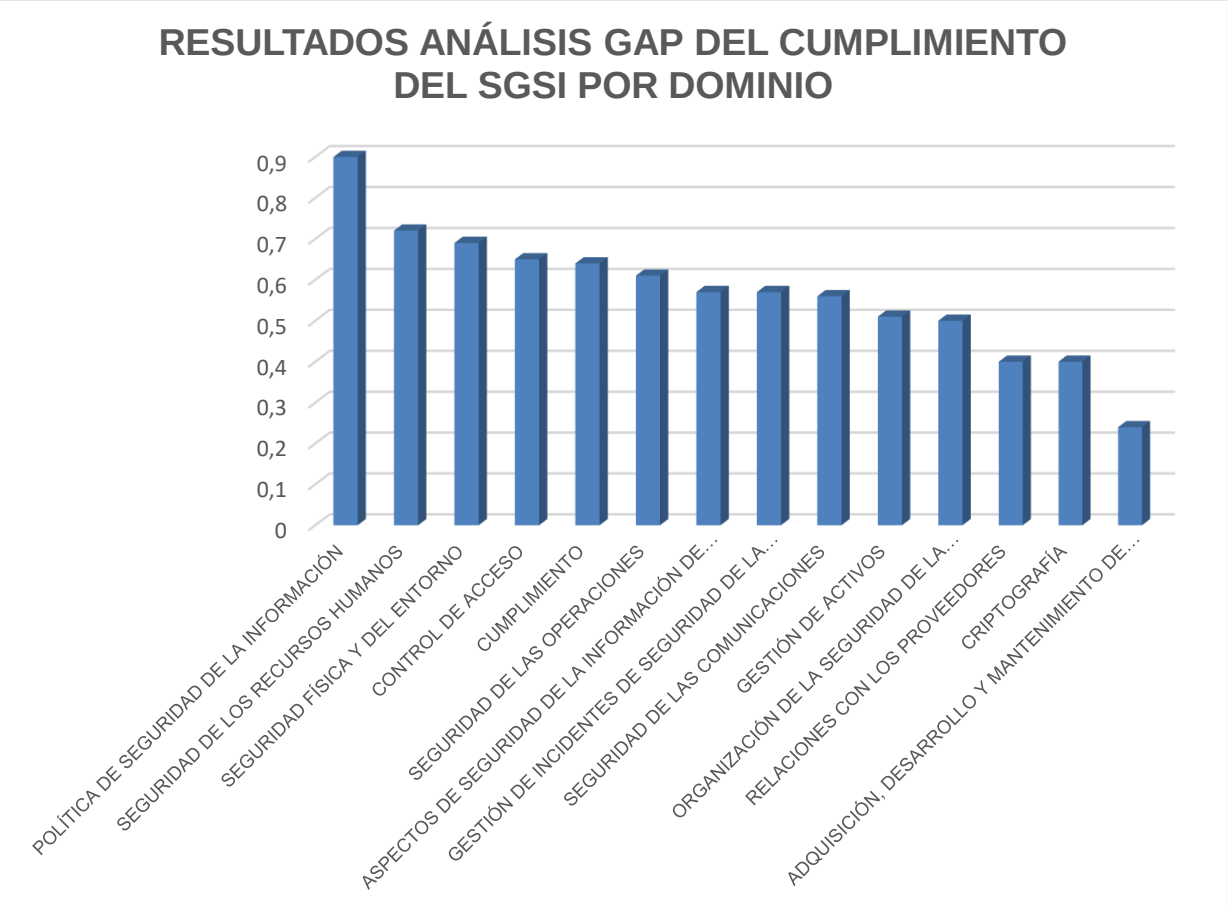
Durante el proceso de validación de resultados al análisis GAP del nivel de implementación de la norma NTC ISO27001:2013 por parte de la Dirección de TIC, la Oficina de Control Interno identificó los siguientes controles para los cuales, la calificación de su nivel de implementación coincide con la calificación presentada por la Dirección de TIC:

ISO	ITEM	NIVEL DE CUMPLIMIENTO DIRECCIÓN DE TIC	NIVEL DE CUMPLIMIENTO OCI
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**	**72**	**72**
A.7.3	**Terminación y cambio de empleo**	**60**	**60**
A.7.3.1	Terminación o cambio de responsabilidades de empleo	60	60
A.8	**GESTIÓN DE ACTIVOS**	**51**	**51**
A.8.1	**Responsabilidad de los activos**	**60**	**60**
A.8.2	**Clasificación de información**	**53**	**53**
A.9	**CONTROL DE ACCESO**	**65**	**65**
A.9.1	**REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO**	**80**	**80**
A.9.2	**GESTIÓN DE ACCESO DE USUARIOS**	**57**	**57**
A.9.3	**RESPONSABILIDADES DE LOS USUARIOS**	**60**	**60**
A.9.4	**CONTROL DE ACCESO A SISTEMAS Y APLICACIONES**	**64**	**64**
A.10	**CRIPTOGRAFÍA**	**40**	**40**
A.10.1	**CONTROLES CRIPTOGRÁFICOS**	**40**	**40**
A.13	**SEGURIDAD DE LAS COMUNICACIONES**	**56**	**56**
A.13.1	**GESTIÓN DE LA SEGURIDAD DE LAS REDES**	**47**	**47**
A.13.2	**TRANSFERENCIA DE INFORMACIÓN**	**65**	**65**
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**	**24**	**24**
A.14.1	**REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**	**33**	**33**
A.14.2	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE**	38	38
A.14.3	**DATOS DE PRUEBA**	**0**	**0**
A.15	**RELACIONES CON LOS PROVEEDORES**	**40**	**40**
A.15.1	Seguridad de la información en las relaciones con los proveedores	100	100
A.15.2	Gestión de la prestación de servicios de proveedores	0	**0**
A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		
A.16.1	**GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN**	**57**	**57**

ISO	ITEM	NIVEL DE CUMPLIMIENTO DIRECCIÓN DE TIC	NIVEL DE CUMPLIMIENTO OCI
A.16.1.7	Recolección de evidencia	0	0
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		
A.17.1	**Continuidad de la seguridad de la información**	**53**	**53**
A.17.2	**Redundancias**	**60**	**60**
A.18	**CUMPLIMIENTO**	**60**	**60**
A.18.1	**Cumplimiento de requisitos legales y contractuales**	**90**	**75**
A.18.2	**Revisiones de seguridad de la información**		

Fuente: Tabla construida por la Oficina de Control Interno basada en la evidencia suministrada por la Dirección de TIC respecto del nivel de implementación de cada uno de los 114 controles de la norma NTC ISO 27001:2013

A continuación, se presentan de manera gráfica, los controles de la norma en los cuales se presentó diferencia en la calificación de su nivel de implementación, entre la Dirección de TIC y la Oficina de Control Interno:



Fuente: Archivo Excel denominado Instrumento de diagnóstico del Modelo de Seguridad y Privacidad de la Información diligenciado por la Dirección de TIC al 31 de mayo de 2021, y validado por la Oficina de Control Interno en el seguimiento realizado

Análisis de cumplimiento de los controles por cada dominio de la norma:

A continuación, se presenta en forma gráfica, un resumen del nivel de cumplimiento de los controles por cada dominio de la norma (descomponiendo cada dominio por sus diferentes aspectos o temáticas que lo componen). Los gráficos presentados también dan a conocer las diferencias entre la valoración de los controles de la norma realizada por la Dirección de TIC y por la Oficina de Control Interno respectivamente. En las reuniones de presentación de las diferencias mencionadas ante la Dirección de TIC se concertó el porcentaje finalmente aceptado por la Entidad para el cumplimiento de dichos controles (en cada caso, la Oficina de Control Interno presentó ante la Dirección de TIC las correspondientes justificaciones de valoración de estos porcentajes y dio a conocer las recomendaciones que permitirían incrementar el nivel de cumplimiento de dichos controles). Tanto las diferencias identificadas, como las recomendaciones del caso se dan a conocer a continuación:

A.5. Política de seguridad de la información

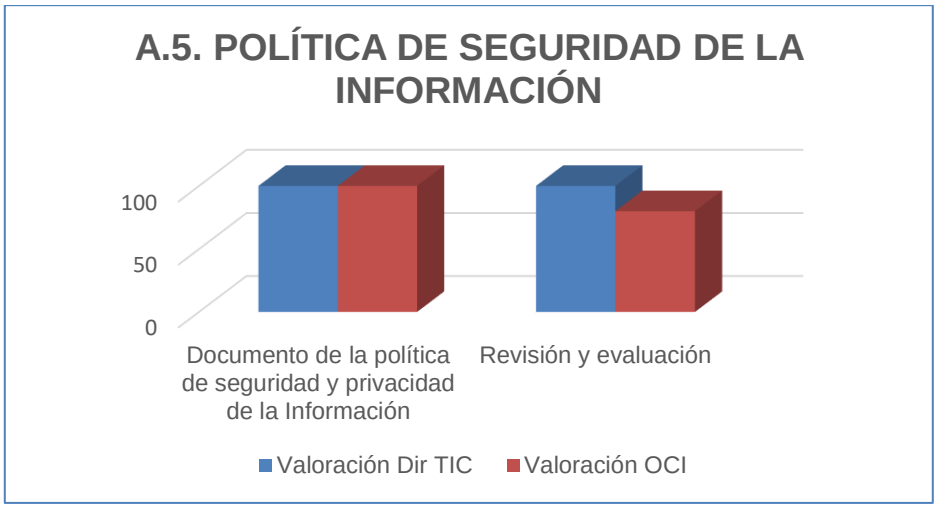
Implementar controles dirigidos a asegurar la actualización de las políticas de seguridad de la información y dejar registro de la revisión anual de las políticas de seguridad de la información en la sección de control de cambios. / evaluar la posibilidad de dejar acta de la revisión efectuada y de su socialización con la Oficina Asesora de Planeación

- Aunque la calificación del control A.5.1.2 “Revisión y evaluación” fue establecida por la Dirección de TIC en 100%, se advierte que en el año 2020 dicha dependencia no adelantó el proceso de revisión anual del Manual de Políticas de Seguridad de la Información, tal como lo establece el numeral 10.3 del citado Manual (desde el año 2017 hasta el año 2019 la Entidad ha venido realizando sin falta las revisiones y actualizaciones anuales). A continuación, se describe la política mencionada:

  "La definición, actualización y mantenimiento del documento de Políticas de Seguridad de la Información de TRANSMILENIO S.A es responsabilidad del Líder u oficial de seguridad de la información, quien debe revisar las políticas de seguridad de la información al menos una vez al año o cuando ocurran cambios

significativos, para asegurar su conveniencia, adecuación y eficacia continua, con la debida aprobación del comité de seguridad de la información y/o Comité Integrado de Gestión y deberá seguir los lineamientos definidos en el procedimiento de control de documentos".

Se presentó diferencia en la calificación del aspecto "Revisión y evaluación" entre la Dirección de TIC (100%) y la Oficina de Control Interno (80%) afectando el resultado final del dominio "Políticas de seguridad de la información" tal como se muestra en la siguiente gráfica:



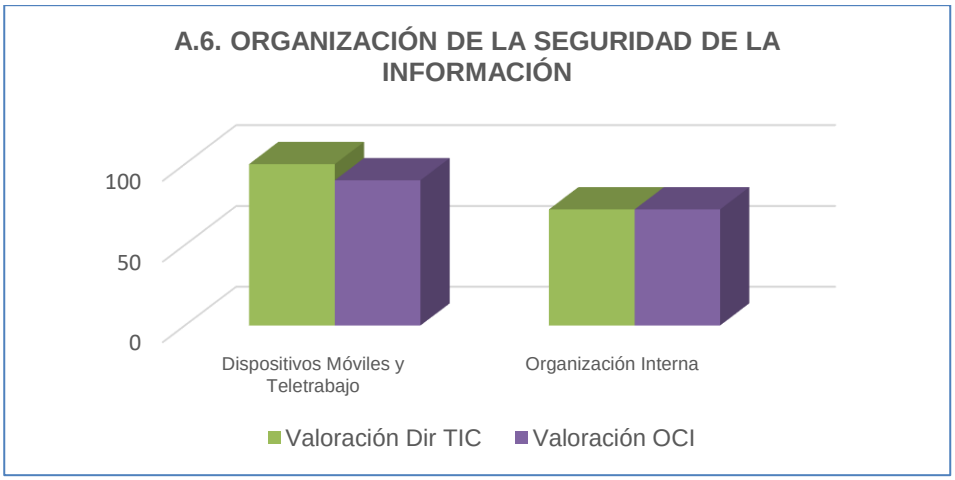
Fuente: construcción propia basada en la documentación aportada por la Dirección de TIC sobre cumplimiento de los controles que componen el dominio A.5. con corte al 31 de mayo de 2021

A.6. Organización de la seguridad de la información

Acelerar el proceso de ajuste de las políticas de teletrabajo y definir e implementar procedimientos de supervisión del cumplimiento de dichas políticas. Alinear dichas políticas con la nueva normatividad establecida.

Este control, que tuvo un nivel de cumplimiento del 50%, presentó diferencia en la calificación del aspecto "Dispositivos móviles y teletrabajo" entre la Dirección de TIC (100%) y la Oficina de Control Interno (90%). Por otro lado, aunque la calificación del control A.6.2.2 "Teletrabajo" estaba al 100% por parte de la Dirección de TIC, en la fecha de elaboración del presente informe dicha dependencia se encontraba ajustando las políticas de teletrabajo, haciéndolas aplicables a las diferentes modalidades de trabajo en casa, por lo

que el nivel de cumplimiento del control fue ajustado al 80%. La anterior diferencia de porcentaje afectó el resultado final del aspecto "Dispositivos móviles y teletrabajo" tal como se muestra en la siguiente gráfica:



Fuente: construcción propia basada en la documentación aportada por la Dirección de TIC sobre cumplimiento de los controles que componen el dominio A.6. con corte al 31 de mayo de 2021

A.7. Seguridad de los recursos humanos:

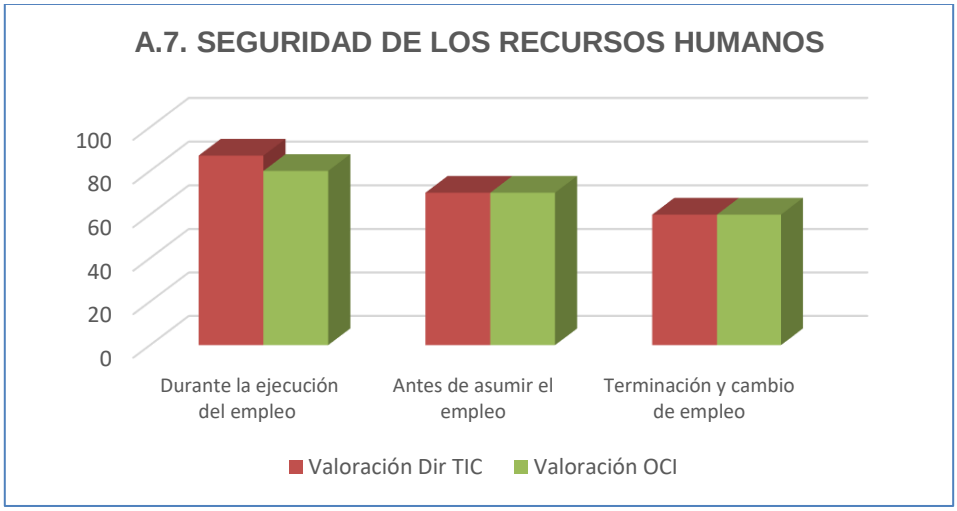
1. Llevar a cabo revisiones y actualizaciones anuales del Plan de Cultura y Sensibilización del SGSI establecido conforme lo menciona el propio Plan de Cultura y Sensibilización del Sistema de Gestión de Seguridad de la Información SGSI (T-DT-007) que se encuentra vigente en la actualidad.

2. Establecer e implementar instancias de supervisión anual del cumplimiento de la política de actualización anual del Plan de Cultura y Sensibilización del SGSI.

    - Aunque la calificación del control A.7.2.2 *"Toma de conciencia, educación y formación en la seguridad de la información"* estaba al 100% por parte de la Dirección de TIC, se advierte que el "Plan de Cultura y Sensibilización en Seguridad de la Información V1 fechado en septiembre de 2020, no se encontraba publicado en la Intranet, ni se aportó evidencia de su aprobación por parte del comité Institucional de Gestión y Desempeño tal como lo establece el literal b de la política de cultura y sensibilización en seguridad de la información, contenida en el Manual de Políticas de Seguridad de la Información V4 (M-DT-001), Dado lo anterior, el nivel de cumplimiento del control fue ajustado al 80%.

La anterior diferencia de porcentaje afectó el resultado final del aspecto *"Toma de conciencia, educación y formación en la seguridad de la información"* tal como se advierte en el párrafo anterior.

Este control, que tuvo un nivel de cumplimiento del 72%, presentó diferencia en la calificación del aspecto "Durante la ejecución del empleo" entre la Dirección de TIC (87%) y la Oficina de Control Interno (80%), tal como se muestra en la siguiente gráfica:



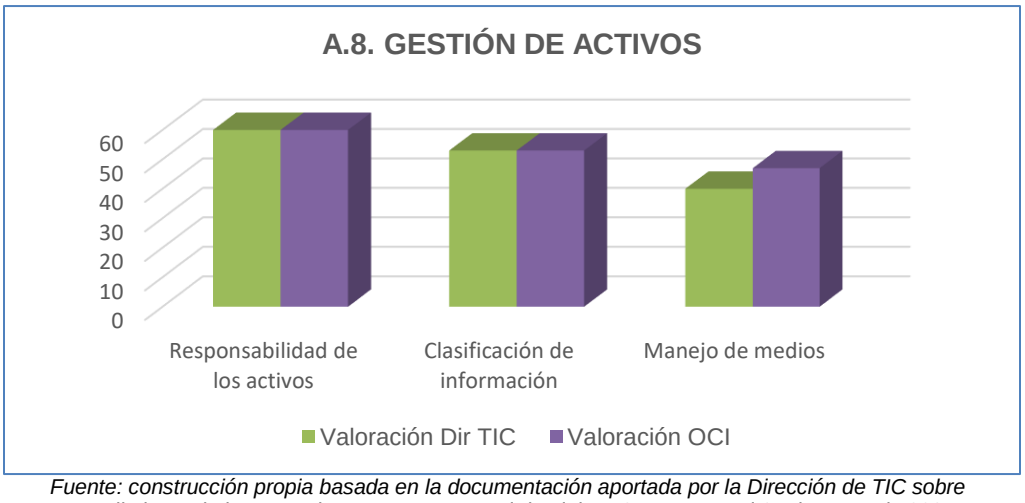
Fuente: construcción propia basada en la documentación aportada por la Dirección de TIC sobre cumplimiento de los controles que componen el dominio A.7. con corte al 31 de mayo de 2021

A.8. Gestión de activos:

Definir e implementar un procedimiento formalmente establecido para proteger los medios que contienen información contra acceso no autorizado, uso indebido o corrupción durante el transporte

Para el control A.8.3.3 "Transferencia de medios físicos", cuya descripción es: "Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte" fue calificada en CERO por parte de la Dirección de TIC, la Entidad tiene implementado como control realizar transferencia de medios físicos a través de embalaje y sello con el fin de proteger la información contra acceso no autorizado. Aunque la Entidad no cuenta con un procedimiento formalmente establecido para fortalecer el control de transferencia de los medios físicos, la Oficina de Control Interno considera que la calificación del control no puede estar en CERO y le asigna un porcentaje de 20%.

Este control, que tuvo un nivel de cumplimiento del 51%, presentó diferencia en la calificación del aspecto "Manejo de medios" entre la Dirección de TIC (40%) y la Oficina de Control Interno (47%). En este caso, es superior la calificación del nivel de implementación del control realizada por la Oficina de Control Interno frente a la calificación del control realizada por la Dirección de TIC, tal como se muestra en la siguiente gráfica:



Fuente: construcción propia basada en la documentación aportada por la Dirección de TIC sobre cumplimiento de los controles que componen el dominio A.8. con corte al 31 de mayo de 2021

A.11. Seguridad física y del entorno:

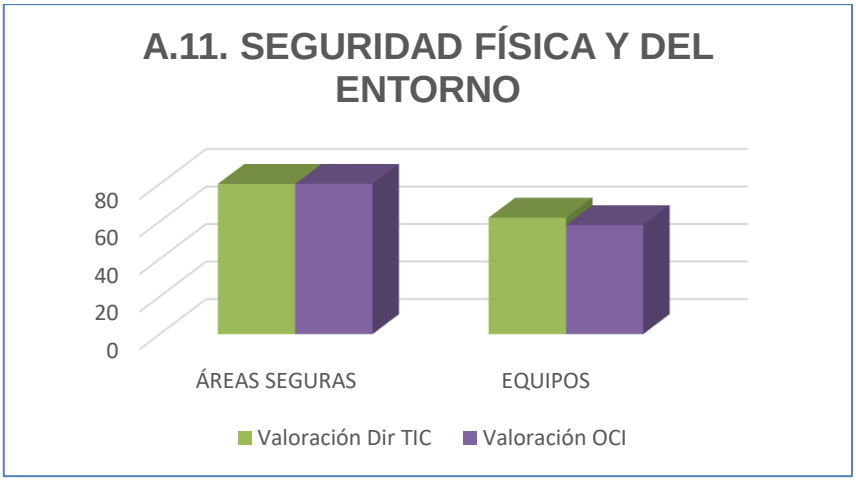
Durante los procesos de sensibilización de las políticas de seguridad de la información se recomienda reforzar el cumplimiento de la política de equipos desatendidos y la política de escritorio limpio, y llevar a cabo acciones de verificación periódicas en las diferentes dependencias de la Entidad, dirigidas a validar su cumplimiento. Evaluar la posibilidad de adelantar conversaciones con los líderes de las dependencias que generaron observaciones durante la revisión con el fin de sensibilizar a los usuarios de la misma en el cumplimiento de la política.

- Se presentó diferencia en la calificación del aspecto "Equipos" entre la Dirección de TIC (62%) y la Oficina de Control Interno (58%). Aunque la calificación de los controles A.11.2.8 "Equipos de usuario desatendidos" y A.11.2.9 "Política de escritorio limpio y pantalla limpia" estaban al 100% y al 80% respectivamente por parte de la Dirección de TIC, se advierte que:

- Para el caso del control "Equipos de usuario desatendidos", aunque la calificación del control estaba al 100% por parte de la Dirección de TIC, se advierte que como parte del CONTRATO NO. 772 de 2019 con la empresa Password SAS, ésta llevó a cabo una revisión al cumplimiento de la política de equipos desatendidos identificando 15 hallazgos de equipos desatendidos y adjuntando al informe (fechado en febrero de 2020) la evidencia fotográfica respectiva, situación que evidencia el incumplimiento de la política mencionada. Dado lo anterior, el nivel de cumplimiento del control fue ajustado al 80%

- Para el caso del control "Política de escritorio limpio y pantalla limpia", aunque la calificación del control estaba al 80% por parte de la Dirección de TIC, se advierte que como parte del CONTRATO NO. 772 de 2019 con la empresa Password SAS, ésta llevó a cabo una revisión al cumplimiento de la política de escritorio limpio identificando 11 hallazgos, las cuales dio a conocer el en informe de febrero de 2020 adjuntando las evidencias fotográficas respectivas. Dado lo anterior, el nivel de cumplimiento del control fue ajustado al 60%

Este control tuvo un nivel de cumplimiento del 69%, tal como se muestra en la siguiente gráfica:



Fuente: construcción propia basada en la documentación aportada por la Dirección de TIC sobre cumplimiento de los controles que componen el dominio A.11. con corte al 31 de mayo de 2021

A.12. Seguridad de las operaciones:

1. Con posterioridad a la ejecución de las pruebas de análisis de vulnerabilidades y hacking ético realizadas anualmente por parte de la Entidad se recomienda planear y ejecutar planes de remediación para el cierre de las brechas identificadas. Confirmar el cierre de las brechas identificadas con la ejecución de pruebas de re-testeo y hacking ético adicionales, y procedimiento de igual manera con el diseño y ejecución de planes de remediación dejando evidencia de las acciones ejecutadas.

2. Implementar las recomendaciones presentadas en el informe OCI-2021-028 de evaluación al cumplimiento de la normativa de Derechos de Autor en materia de software en lo relativo a la instalación de software por parte de los usuarios.

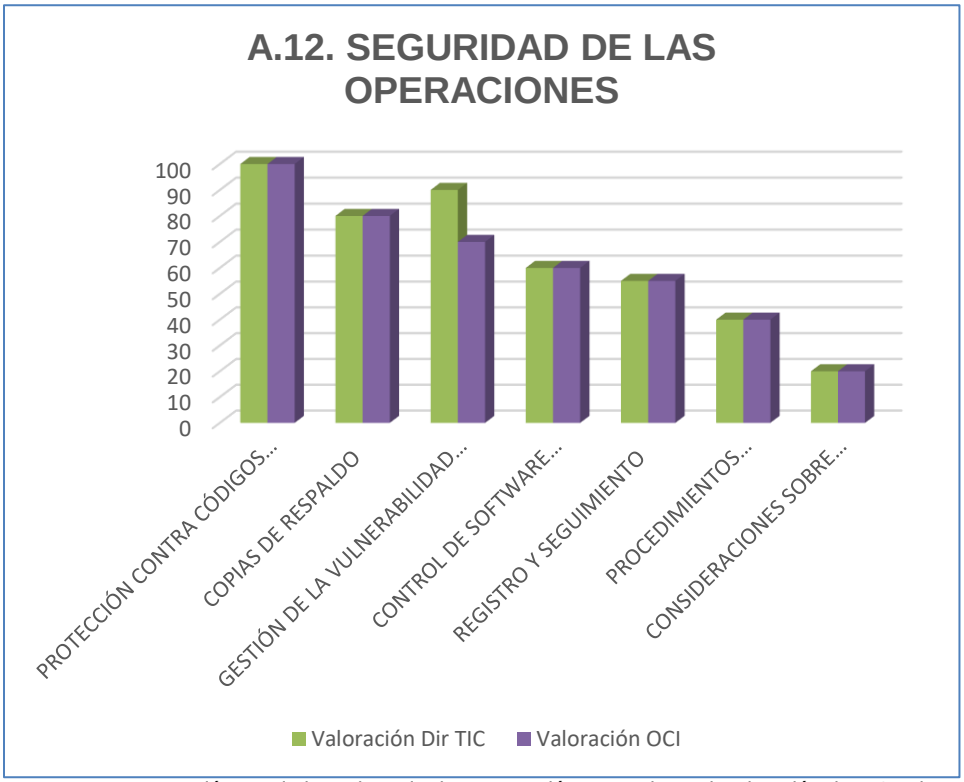
   - Se presentó diferencia en la calificación del aspecto "Gestión de la vulnerabilidad técnica" entre la Dirección de TIC (90%) y la Oficina de Control Interno (70%). Aunque la calificación de los controles A.12.6.1 "Gestión de las vulnerabilidades técnicas" y A.12.6.2 "Restricciones sobre la instalación de software" estaban al 80% y al 100% respectivamente por parte de la Dirección de TIC, se advierte que:

     - Para el caso del control "Gestión de las vulnerabilidades técnicas", aunque la calificación del control estaba al 80% por parte de la Dirección de TIC, se advierte que en el 2020 la Dirección de TIC programó con apoyo del proveedor Password la realización de análisis de vulnerabilidades a la plataforma central de cómputo de la Entidad (testeo y re-testeo); sin embargo, no diseñó un plan de remediación de las vulnerabilidades identificadas en el testeo inicial. Tampoco se cuenta con un comparativo entre las brechas inicialmente identificadas frente a las brechas resultantes en el re-testing (en enero y febrero de 2020 hubo escaneo y otro a diciembre que fue reportado en marzo). Dado lo anterior, el nivel de cumplimiento del control fue ajustado al 60%

     - Para el caso del control "Restricciones sobre la instalación de software", aunque la calificación del control estaba al 100% por parte de la Dirección de TIC, se advierte que conforme a los resultados de una evaluación al

cumplimiento de la Ley de Derechos de Autor en materia de software por parte de la OCI mencionados en el informe en el informe OCI-2021-028, se identificó en algunos equipos software no licenciado. Dado lo anterior, el nivel de cumplimiento del control fue ajustado al 80%

El control tuvo un nivel de cumplimiento del 61%, como se muestra en la siguiente gráfica:



Fuente: construcción propia basada en la documentación aportada por la Dirección de TIC sobre cumplimiento de los controles que componen el dominio A.12. con corte al 31 de mayo de 2021

A.18. Cumplimiento:

1. Diseñar y ejecutar planes de remediación para el cierre de las brechas identificadas, con posterioridad a la ejecución de las pruebas de análisis de vulnerabilidades y hacking ético realizadas anualmente por parte de la Entidad se recomienda, dejando evidencia de las acciones adelantadas. Confirmar el cierre de las brechas identificadas con la ejecución de pruebas de re-testeo y hacking ético adicionales, y procedimiento de igual manera con el diseño y ejecución de planes de remediación dejando evidencia de las acciones ejecutadas.

2. Implementar las recomendaciones presentadas en el informe OCI-2021-028 de evaluación al cumplimiento de la normativa de Derechos de Autor en materia de software en lo relativo a la instalación de software por parte de los usuarios.

3. Establecer e implementar un plan de revisión del cumplimiento de las políticas de seguridad de la información con las diferentes dependencias, relacionadas con los log de los sistemas de información que éstas gestionan.

Se presentó diferencia en la calificación de los aspectos "Cumplimiento de requisitos legales y contractuales" y "Revisiones de seguridad de la información" del dominio A.18 "Cumplimiento" entre la Dirección de TIC y la Oficina de Control Interno así:

ASPECTO	CONTROL	DESCRIPCIÓN	CALIFICACIÓN DIRECCIÓN DE TIC	CALIFICACIÓN OFICINA DE CONTROL INTERNO
Cumplimiento de requisitos legales y contractuales	A.18.1.2	Derechos de propiedad intelectual.	100%	80%
	A.18.1.3	Protección de registros	100%	80%
	A.18.1.4	Protección de los datos y privacidad de la información relacionada con los datos personales.	100%	80%
Revisiones de seguridad de la información	A.18.2.3	Revisión de cumplimiento técnico	80%	60%

Fuente: Construcción Oficina de Control Interno. Diferencia en la calificación de los aspectos "Cumplimiento de requisitos legales y contractuales" y "Revisiones de seguridad de la información" del dominio A.18 "Cumplimiento" entre la Dirección de TIC y la Oficina de Control Interno

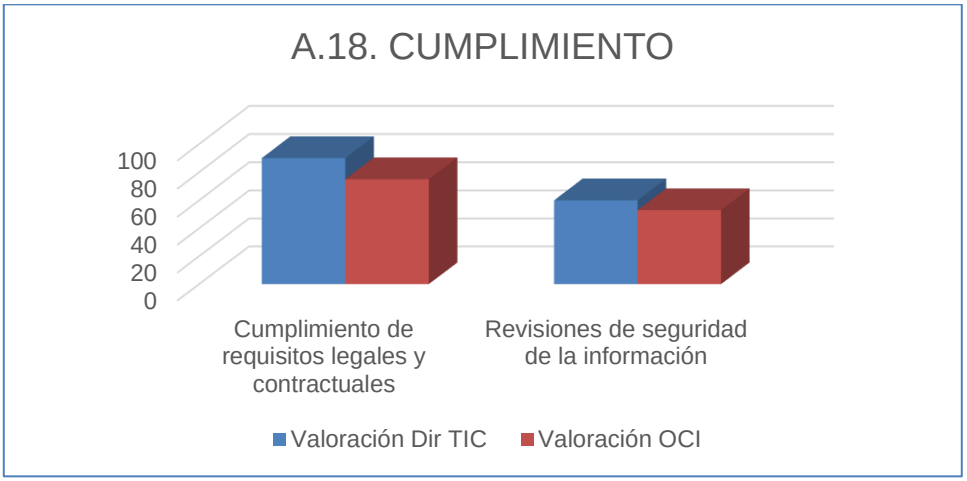
- Para el control A.18.1.2. "CUMPLIMIENTO (Derechos de propiedad intelectual)": Aunque la calificación del control estaba al 100% por parte de la Dirección de TIC, se advierte que conforme a los resultados de una evaluación al cumplimiento de la Ley de Derechos de Autor en materia de software por parte de la OCI mencionados en el informe en el informe OCI-2021-028, se identificó en algunos equipos software no licenciado. Dado lo anterior, el nivel de cumplimiento del control fue ajustado al 80%

- Para el control A.18.1.3 "CUMPLIMIENTO (Protección de registros)": Aunque la calificación del control estaba al 100% por parte de la Dirección de TIC, se advierte que dicha dependencia no tiene definidas ni implementadas actividades periódicas de monitoreo del cumplimiento de las políticas de copias de respaldo y restauración de

datos para aquellos sistemas de información cuyo soporte técnico se encuentra a cargo directo de las dependencias; por esta razón se desconoce si las dependencias que son responsables técnicos de los sistemas de información protegen adecuadamente los registros de las copias de respaldo y restauraciones realizadas. Dado lo anterior, el nivel de cumplimiento del control fue ajustado al 80%

Las anteriores diferencias de porcentaje afectaron el resultado final de los aspectos "Cumplimiento de requisitos legales y contractuales" y "Revisiones de seguridad de la información" del dominio A.18 "Cumplimiento".

Este control tuvo un nivel de cumplimiento del 64%, desagregado como se muestra en la siguiente gráfica:



Fuente: construcción propia basada en la documentación aportada por la Dirección de TIC sobre cumplimiento de los controles que componen el dominio A.18. con corte al 31 de mayo de 2021

RESUMEN DE HALLAZGOS:

No.	Título de Hallazgo	Repetitivo
1	Debilidad en la gestión y administración del riesgo del proceso Gestión de TIC	No
2	Alcance insuficiente del SGSI en la Entidad	No
3	Desactualización del Plan de Cultura y sensibilización en seguridad de la información y debilidades en la cobertura de las sesiones de	No

No.	Título de Hallazgo	Repetitivo
	sensibilización de éste.	
4	Debilidades en el Plan de Recuperación de Desastres en cuanto pruebas, cobertura, tiempos de restauración y formalización de los roles.	No
5	Debilidades en la aplicación normas de seguridad en el Data Center y en el cuarto de suministro UPS	No
6	Carencia de un Plan de Servicios Ciudadanos Digitales al interior de la Entidad	No
7	Diseño deficiente de indicadores de gestión de TIC	No

CONCLUSIÓN

Aunque como parte del seguimiento realizado al nivel de implementación de la norma NTC ISO27001:2013 la Oficina de Control Interno dio a conocer en el presente informe las diferencias en las ponderaciones realizadas por la Dirección de TIC a cada uno de sus 114 controles, sus justificaciones y las recomendaciones que permiten incrementar la calificación de dichos controles, es importante señalar que la Dirección de TIC también debe adelantar gestiones dirigidas a cerrar las brechas de aquellos controles con calificación menor del 100% y para las cuales hubo coincidencia en la calificación entre la Dirección de TIC y la Oficina de Control Interno.

El presente informe fue socializado con el enlace de la Dirección de TIC y su equipo de trabajo los días 21 y 26 de mayo, y 1 de junio de 2021.

Los hallazgos y observaciones relacionados en el presente informe corresponden a la evaluación realizada a muestras tomadas, conforme a la Planeación del trabajo de Auditoría dentro del alcance establecido, por lo tanto, es responsabilidad del área auditada, efectuar una revisión de carácter general sobre los aspectos evaluados.

En virtud a lo definido en el procedimiento P-CI-010 Formulación y seguimiento a los planes de mejoramiento, la oficina de Control Interno solicita los mismos sean enviados en un plazo no

mayor a ocho (8) días hábiles posteriores a la radiación del presente informe. De igual forma, se indica que, si la Dirección de TIC lo considera, la oficina de Control Interno está en disposición de asesora en la formulación de los planes de mejoramiento

Cualquier información adicional, con gusto será suministrada.

Bogotá D.C., 30 de junio del 2021.

LUIS ANTONIO RODRÍGUEZ OROZCO

Jefe Oficina de Control Interno

Elaboró: Néstor Orlando Velandia Sosa – Contratista
Revisó: Luz Marina Díaz Ramírez - Contratista