N° INFORME: Informe OCI-2020-059 Consultoría a control de interfaces de sistemas de información

PROCESO/SUBPROCESO/ACTIVIDAD:

Todos los procesos - Evaluación a los controles implementados en la información de las interfaces que provienen de los sistemas origen, hacia los sistemas destino de la Entidad.

RESPONSABLE DEL PROCESO/SUBPROCESO/ACTIVIDAD

Aunque la definición de los controles que deben implementarse en las interfaces de los sistemas de información con que cuenta la entidad, es definida por los líderes de las áreas funcionales respectivas (directores, subgerentes, etc.) que gestionan dichos sistemas, su implementación está a cargo de la Dirección de TIC, la cual, por tanto, se constituye en el área responsable de los procesos evaluados.

EQUIPO CONSULTOR: Néstor Orlando Velandia Sosa, Auditor, Contratista.

OBJETIVO(S):

Llevar a cabo un diagnóstico al diseño y a la efectividad de los controles implementados por la Entidad en la información de las interfaces entre los diferentes sistemas de información existentes en TRANSMILENIO S.A.

ALCANCE:

El trabajo comprende el levantamiento de la arquitectura tecnológica que soporta los sistemas de información de TMSA, el inventario de dichos sistemas y la información de las interfaces entre ellos, identificando eventuales oportunidades de mejora en los controles clave de generación y/o cargue de la información en los

sistemas destino, para evitar la materialización de riesgos relacionados con la calidad, integridad y seguridad de la información.

Como parte de la actividad realizada, se incorporan los resultados de una encuesta desarrollada por la OCI para ser respondida por los responsables de asegurar la calidad, integridad y seguridad de las interfaces de los sistemas de información, en la cual se indaga acerca de los diferentes controles existentes a nivel de interfaz.

El corte de la presente consultoría comprende el período comprendido entre el 1 de enero de 2020 y el 30 de noviembre de 2020.

LIMITACIONES AL ALCANCE:

Dentro de los resultados del trabajo de la consultoría realizada no fue posible identificar los riesgos ni los controles implementados en lo relativo a la arquitectura tecnológica que soporta los sistemas de información, debido a que, al momento de la evaluación, la Dirección de TIC no contaba con el diagrama arquitectónico de la red de cómputo que identifique su estructura, componentes, organización funcional, sistemas de información subyacentes, ubicación, dispositivos de seguridad implementados, entre otros.

La información existente en la Dirección de TIC relacionada con la caracterización de las interfaces de los sistemas de información se encontraba en proceso de elaboración, y por tanto no estaba completa (únicamente se contaba con la información de las interfaces de aquellos sistemas cuya responsabilidad de soporte está a cargo de la Dirección de TIC); por lo anterior, los resultados de la presente consultoría no incluyen conclusiones relacionadas con las interfaces para las que la Dirección de TIC no se contaba con dicha información. Se recalca no obstante que, por control, la mencionada Dirección es responsable de disponer de un catálogo actualizado de los sistemas de información existentes en la Entidad, de implementar

los controles de aplicación en conjunto con las áreas líderes responsables de dichos sistemas, así como de establecer las condiciones técnicas y de protección requeridas para asegurar el intercambio seguro de información entre los sistemas.

Por último y en consideración a que la Dirección de TIC suministró a la OCI tres (3) archivos con versiones diferentes con el inventario de los sistemas de información existentes en la entidad, se aclara que los resultados del trabajo toman como base la última versión del catálogo de sistemas de información que fue aportado por la Dirección de TIC mediante correo electrónico del día 17 de noviembre de 2020 y que se encontraba en una hoja del archivo MS-Excel “TMSA_20201103_Validación de la información aportada sobre SI (version 1).xlsx”.

DECLARACIÓN:

Esta consultoría fue realizada con base en el análisis de una muestra de las interfaces existentes (seleccionada conforme al criterio profesional de la Oficina de Control Interno) y no de la revisión de su totalidad, por lo que subsiste el riesgo de que las conclusiones basadas en dicha muestra no coincidan con aquellas que se habrían obtenido en caso de haber examinado la totalidad de las interfaces.

Por otra parte, se presentan conclusiones basadas en la encuesta realizada que puede tener el riesgo de pérdida de sinceridad (se responda lo que no se está ejecutando) y dificultad para entender la pregunta.

RIESGOS CUBIERTOS:

Con base en el análisis de la anterior información, el diagnóstico busca validar el diseño y la efectividad de los controles implementados en las interfaces de los sistemas de información implica establecer si fueron adecuadamente gestionados o mitigados los siguientes riesgos:

- Errores en la información generada por las aplicaciones,
- Información indebidamente modificada,
- Errores en la estructura o formato de la información generada
- Acceso no autorizado a la información generada, procesada y/o cargada,
- Diferencias entre la información generada y la información cargada,
- Información débilmente validada
- Información cargada múltiples veces al sistema destino.

FORTALEZAS:

El personal de la Dirección de TIC que atendió la consultoría prestó toda su colaboración, aportando la información existente y participando en las reuniones convocadas conforme a su disponibilidad.

CRITERIOS:

1. Constitución Política de Colombia de 1991:
   - Artículo 15. Derecho a la Intimidad. Hábeas Data.
   - Artículo 20. Derecho a la Información.
   - Artículo 284. Acceso a Información Reservada.

2. Ley 1273 de 2009: por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones, el cual establece en su “Capítulo I De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” así:

- Artículo 269A: Acceso abusivo a un Sistema Informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático
- Artículo 269B: Obstaculización Ilegítima de Sistema Informático o Red de Telecomunicación.
- Artículo 269C: Interceptación de Datos Informáticos.
- Artículo 269D: Daño Informático.
- Artículo 269E: Uso de Software Malicioso.
- Artículo 269F: Violación de Datos Personales.
- Artículo 269G: Suplantación de Sitios Web para capturar datos personales.

3. Ley 527 de 1999: por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones.

4. Ley 1266 de 2008: por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contendida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

5. Ley 1341 de 2009: por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones acerca de la protección de los derechos de los usuarios.

6. Ley 1581 de 2012: por la cual se dictan disposiciones generales para la protección de datos personales, habeas data

7. ISO/IEC 27001:2013 Norma técnica que describe los requerimientos del Sistema de Seguridad de la Información aprobado y publicado por la ISO (International Organization for Standardization) y por la IEC (International Electrotechnical Commission).

8. ISO/IEC 27002:2013 Documento que recopila el código de práctica y los controles para la gestión de la seguridad de la información aprobado y publicado por la ISO (International Organization for Standardization) y por la IEC (International Electrotechnical Commission).

9. Documento G-SIS.03 de la Guía para la construcción del catálogo de Sistemas de Información del MINTIC

10. Reglamento Interno de trabajo de TRANSMILENIO S.A. Norma reguladora de las relaciones internas de TMSA con sus trabajadores.

11. Manual de Políticas de seguridad de la información de TRANSMILENIO S.A versión 3 (código M-DT-001)

12. Anexo 5. Plan Tratamiento Riesgos Seguridad Informacion.xlsx, versión 0 de julio de 2018.

13. P-DT-012 Procedimiento para el intercambio seguro de información electrónica Versión 1 de abril de 2019.

14. I-DT-001 "Instructivo para la identificación, valoración y clasificación de activos de información" versión 0 de abril de 2019

15. P-DT-017 Procedimiento de control de cambios de infraestructura tecnológica V.0.pdf

16. P-DT-018 Procedimiento de Gestión de Vulnerabilidades Tecnológicas V.0.pdf

17. P-DT-019 Procedimiento de copias de respaldo V.0.pdf

DESCRIPCIÓN DEL TRABAJO REALIZADO:

a. **Reunión de Apertura:** El día 27 de octubre se llevó a cabo la reunión de apertura de la consultoría ante el Director de TIC, en la que fueron presentados los objetivos, alcance, duración y metodología general del trabajo.

b. **Entendimiento:** Se realizaron reuniones de entendimiento con el personal de la Dirección de Tecnología responsable de asegurar la calidad, integridad y seguridad de la información contenida en las interfaces de los sistemas de información de la entidad, así como con la Dirección Técnica de Buses con el fin de conocer los sistemas de información desarrollados y operados por dicha dependencia, así como las interfaces vinculadas a dichos sistemas.

c. **Revisión documentación:** Una vez solicitada a la Dirección de TIC la información listada en el presente literal, se llevó a cabo un análisis de la misma, aclarando que, conforme a lo manifestado por la Dirección de TIC, ésta se encontraba en proceso de construcción:

- Diagrama arquitectónico de la red de cómputo con que cuenta TMSA al máximo nivel de detalle y una explicación del mismo.
- Copia del inventario actualizado de aplicaciones y demás herramientas informáticas utilizadas en los diferentes procesos de la entidad

- Identificación de las aplicaciones origen y destino desde el punto de vista de flujo de información, descripción de la información cruzada entre aplicaciones, frecuencias o fechas de envío y cargue de información, identificación, cargo y dependencia de los responsables del envío y de la recepción de información entre aplicaciones, identificación del proceso o procesos usuarios del sistema
- Presentación detallada del tipo de información que se comparte entre las aplicaciones
- Controles establecidos en el cruce de información entre aplicativos para prevenir los tipos de riesgo vinculados a las interfaces de los sistemas de información:
- Copia de las políticas y procedimientos de TIC formalmente establecidos por TMSA para la adquisición, el desarrollo, la parametrización, la administración, la operación, el mantenimiento y la documentación de aplicaciones y de sus bases de datos.
- Presentación de los proyectos de TMSA que se encuentran en curso, relacionados con la gestión de la información existente en las diferentes aplicaciones, o con el fortalecimiento de los controles en dichas aplicaciones

d. Obtención de información: Para cada sistema de información se identificó su objetivo, los módulos que los componen, el nombre del sistema o sistemas destino (es decir, aquel o aquellos con los que se interrelaciona), características de la información de la interfaz, estructura del archivo, medio de envío, frecuencia de generación, nombre de la dependencia que genera la información y de la que la recibe, nombre del proceso que genera la información y del proceso que la recibe, nombre del documento corporativo que describe los controles de validación de la interfaz y el procedimiento para reportar y corregir información cargada con error, descripción de la validación técnica y/o manual

realizada con esta información y nivel de madurez de la interfaz (porcentaje de confiabilidad de la información con base en registros históricos).

Se efectuó una revisión al documento “Anexo 5. Plan Tratamiento Riesgos Seguridad Informacion.xlsx” con el fin de validar si éste incorporaba la identificación y gestión de los riesgos clave sobre las interfaces de los sistemas de información, y se llevaron a cabo pruebas de validación a los controles de las interfaces de los siguientes sistemas:

- FCSCenter - sistema estadístico
- Sistema estadístico - sistema de apoyo a interventoría, y
- Sistema SAE - sistema espacial

A partir del entendimiento mencionado se evaluó el catálogo de sistemas de información suministrado, validando su conformidad contra el documento “WG.SIS.03 Guía para la construcción del catálogo de Sistemas de Información" del Ministerio de Tecnologías de la Información y las Comunicaciones Versión 1.1 octubre de 2019 y evaluando su completitud y nivel de actualización. Se identificaron oportunidades de mejora en el examen mencionado.

Se llevó a cabo una selección de la muestra de las interfaces de sistemas de información que serían sujetas a la revisión del diseño y efectividad de los controles, las cuales fueron ejecutadas de conformidad, e identificadas oportunidades de mejoramiento.

Se diseñó y aplicó una encuesta a los responsables de asegurar la calidad, integridad y seguridad de la información contenida en las interfaces de los sistemas de información en la entidad; sus resultados fueron tabulados e incorporados en el presente informe.

d) Análisis de resultados y conclusiones: A partir de las anteriores actividades, se identificaron oportunidades de mejora en los controles clave de los procesos de generación y/o cargue de las diferentes interfaces, dirigidas a evitar la materialización de los riesgos descritos. Los resultados de la evaluación realizada por la OCI se presentan en el informe bajo los siguientes títulos:

1. Arquitectura tecnológica que soporta los sistemas de información:
2. Catálogo de sistemas de información:

    a. Evaluación al cumplimiento del documento G-SIS.03 de la Guía para la construcción del catálogo de Sistemas de Información del MINTIC.

    b. Alineación entre el catálogo de sistemas de información y el inventario de activos de información:

3. Interfaces entre los sistemas de información

    a. Documentación existente
    b. Observaciones a la información de interfaces suministrada en el catálogo de sistemas de información
    c. Diferencias en la información de interfaces suministrada por la Dirección de TIC:

4. Evaluación a los controles de las interfaces

    a. sistema FCS Center - sistema estadístico
    b. sistema estadístico - sistema de apoyo a interventoría
    c. Sistema SAE - sistema espacial

5. Resultados de la encuesta realizada a los responsables de asegurar la calidad, integridad y seguridad de la información existente en las interfaces de los sistemas de información.

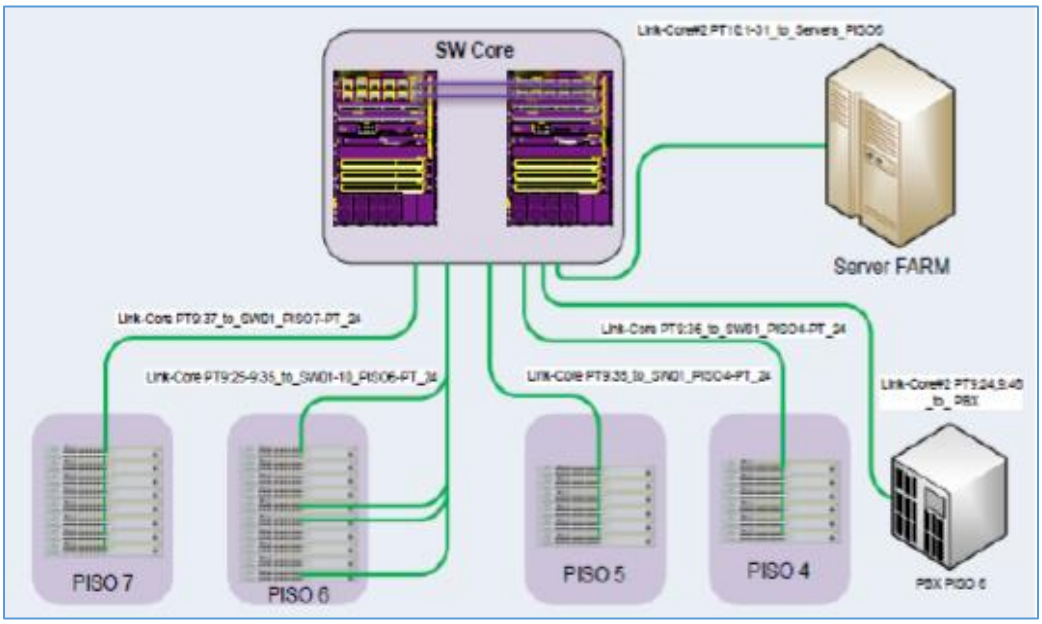
RESULTADOS OBTENIDOS EN LA CONSULTORÍA:

Dentro del contexto del presente informe, se denomina “interfaz” como aquella información de TMSA que es generada por un sistema de información origen y que debe ser cargada en otro sistema llamado sistema destino. Se aclara así mismo que la información generada por el sistema origen puede o no, estar contenida en archivos foráneos al sistema denominados “archivos de interfaz”.

Con el siguiente diagrama se da a conocer la metodología utilizada por la consultoría para el desarrollo del diagnóstico

Con base en la anterior metodología, a continuación, se presentan los resultados de la evaluación realizada:

1. **Arquitectura tecnológica que soporta los sistemas de información:** Mediante correo electrónico enviado por la Oficina de Control Interno a la dirección de TIC el 27 de octubre de 2020, la OCI solicitó copia del diagrama arquitectónico de la red de cómputo existente en la entidad, desplegado al máximo nivel de detalle y una explicación del mismo; en respuesta, el día 6 de noviembre la Dirección de TIC copió en el repositorio de OneDrive dispuesto para la consultoría, el documento "Topología Transmilenio_830063506.pdf", el cual contenía el siguiente diseño de la solución de red Tipo Dispositivo:



Fuente: Correo electrónico del 6 de noviembre, enviado por la Dirección de TIC

Como se pude apreciar en la anterior imagen, el documento contiene dos cuadros: uno con el tipo de dispositivo, la dirección MAC el número de serial y ubicación de los equipos de la red LAN, y otro con la ubicación, el modelo de switch, el número de unidad, la dirección IP y máscara de los equipos rack

existentes. Dado que el documento suministrado no contiene el diagrama arquitectónico de red solicitado, es decir, una representación visual de la red LAN y WAN que incluya entre otros los diferentes componentes de la red (servidores, enrutadores, hubs, subredes alámbricas e inalámbricas, conectividad con redes externas, cortafuegos, etc.), la OCI advierte que su carencia podría llegar a limitar la adecuada gestión de esta clase de activos tecnológicos, la identificación de posibles mejoras en el diseño de la red, facilitar la gestión de soporte técnico requerido, con lo cual podría favorecerse el diagnóstico del desempeño y la seguridad de la red.

2. Catálogo de sistemas de información:

a. **Evaluación al cumplimiento del documento G-SIS.03 de la Guía para la construcción del catálogo de Sistemas de Información del MINTIC:** En el Anexo1 del presente informe se presentan los resultados de la verificación realizada por la OCI al cumplimiento del documento “G-SIS.03 de la Guía para la construcción del catálogo de Sistemas de Información del MINTIC” por parte de TMSA. Con base en dichos resultados, se concluye que existen brechas entre los lineamientos de la guía frente a lo establecido en el catálogo de sistemas de información de la entidad; particularmente lo señalado en el numeral 3.1.2 relacionado con "Documentación del catálogo de sistemas de información", sub numeral 2: “Verificar que hayan sido ingresados todos los sistemas de información en la herramienta o instrumento definido por la entidad."

b. **Alineación entre el catálogo de sistemas de información y el inventario de activos de información:** La OCI llevó a cabo una verificación dirigida a validar si los sistemas de información registrados en el catálogo de SI figuraban en el inventario de activos de información de la Entidad (el cruce

fue realizado contra la columna “sistemas de información” de la hoja “Hw-Sw-Servicios” y filtrando la información por el tipo de activo “Software”). A continuación, se dan a conocer las estadísticas de las observaciones identificadas, cuyo detalle se muestra en el Anexo 2 del presente informe:

TIPO DE OBSERVACIÒN	CANT	%
El sistema de información que figura en el catálogo de SI también está en el inventario de activos de información (sin observaciones por parte de la OCI)	14	31%
No corresponde a un sistema de información; no figura en el catálogo de SI	1	2%
Sistema de información que no figura en el inventario de activos de información	23	51%
Sistema del inventario de activos no corresponde a un sistema de información	1	2%
Sistema del inventario de activos no corresponde a un sistema de información; no figura en el catálogo de sistemas de información	4	9%
Sistema del inventario de activos no corresponde a un sistema de información; No figura en el inventario de activos de información	1	2%
Sistema del inventario no figura en el catálogo de activos de información	1	2%
TOTAL GENERAL	**45**	**100%**

Fuente: construcción de la OCI con base en la información suministrada por la Dirección de TIC durante el ejercicio.

Con base en los resultados anteriores, se concluye que el catálogo de sistemas de información no se encuentra debidamente alineado con el inventario de activos de información de la Entidad, en lo relacionado con la identificación de sistemas de información.

Por otro lado y aunque la Guía para la construcción del catálogo de Sistemas de Información del MINTIC no es de obligatorio cumplimiento, sino que establece lineamientos orientadores para su construcción, la OCI identificó brechas contra esta buena práctica; particularmente contra lo señalado en el numeral 3.1.2 "Documentación del catálogo de sistemas de información", sub numeral 2 que define: "*Verificar que hayan sido ingresados todos los sistemas de información en la herramienta o instrumento definido por la entidad*.".

También se presenta una brecha con lo establecido en el documento I-DT-001 denominado "instructivo para la identificación, valoración y clasificación de activos de información" versión 0 de abril de 2019, en lo relacionado con el numeral 7.1. "Instrucciones a seguir para la identificación y registro de activos de información" literal a. "Identificar los activos de información" el cual indica que:

> *"Los líderes de proceso realizarán la identificación y actualización del Inventario de Activos de Información (subrayado fuera de texto) diligenciando el formato R-DT-010 Inventario de Activos de Información. El Profesional Especializado Grado 06 - Seguridad Informática (o quien cumpla el rol de Oficial de Seguridad de la información) supervisará la ejecución de dichas actividades, así como la implementación de las actividades establecidas en el presente documento.".*

La OCI considera así mismo que la falta de alineación entre el catálogo de sistemas de información y el inventario de activos de información podría afectar negativamente la gestión administrativa, técnica y operativa de los

activos de la entidad y en la gestión de seguridad de los mismos por parte de la Dirección de TIC.

Durante la validación de la presente observación, la Dirección de Tecnología indicó que el catálogo de sistemas de información se encuentra en proceso de construcción y que se están adelantando las labores de actualización respectivas.

3. Interfaces entre los sistemas de información

a. **Documentación existente:** Como resultado del cruce realizado entre la información del catálogo de sistemas de información que fue suministrado para nuestra evaluación, y la relacionada en el archivo "SistemasInformacionTICOrigenDestinoV.0.xlsx" (el cual incluye información sobre la caracterización de las interfaces de los sistemas de información de la entidad), se pudo establecer que para los siguientes 30 sistemas de información, de los 39 existentes (correspondiente al 77% de los sistemas de información existentes en el catálogo), el archivo "SistemasInformacionTICOrigenDestinoV.0.xlsx" no contiene la información de detalle de las interfaces, no obstante que en el catálogo, estos sistemas contienen información de interoperabilidad:

- ALCAPITAL
- APLICACIÓN TECNOLÓGICA DE VIGILANCIA
- CENTRO DE CONTROL OPERACIONAL (CCO) - TransMiCable S.A.
- CENTRO DE GESTIÓN CDEG
- CICLOPARK
- CORDIS
- CRM
- DatosSAE

- ERP - JSP7 (SIAF)
- GOAL BUS
- Herramienta seguimiento Otro Si a los Operadores del Sistema Zonal
- INDICADORES
- INTRANET
- PLATAFORMA EIC
- PROACTIVANET
- ReportSAE
- ROYAL
- SOFTWARE ISS SECUROS
- STPGUI
- SUITE VISION EMPRESARIAL
- SUPERVISIÓN OFFLINE
- TABLA MAESTRA SIRCI
- T-DOC
- TIEMPO PROMEDIO DE ESPERA DE USUARIOS
- TRANSMIAPP
- TRANSMISURVEY
- VEHICULOS
- VEHICULOSQUERY
- VIHANET
- VISION BRT

Fuente: construcción de la OCI

Por otro lado, el archivo "SistemasInformacionTICOrigenDestinoV.0.xlsx" incluye información de las interfaces de los sistemas "*GTFS Dinamicos" y "Outlook*" los cuales no figuran en el catálogo de sistemas de información.

Así mismo, aunque el catálogo de sistemas de información incluye los sistemas de información FCS Center y SAE de propiedad de Recaudo Bogotá (los cuales generan información de interfaz hacia sistemas de información de TRANSMILENIO S.A.), el catálogo no precisa que la propiedad de los mismos es de Recaudo Bogotá y no de TMSA. Con base

en lo anterior y para los sistemas de información que no cuentan con esta información, la OCI advierte que:

a. La Dirección de TIC podría llegar a tener limitaciones para establecer si las medidas de seguridad y control que han sido implementadas por las dependencias responsables de las interfaces de dichos sistemas, son o no efectivas.

b. Para los sistemas de información sin detalle de interfaz en el catálogo de sistemas, se desconoce si en la práctica la entidad está dando cumplimiento a las políticas de intercambio seguro de información descritas en el documento P-DT-012 denominado “procedimiento para el intercambio seguro de información electrónica” (se resalta que aunque el documento se denomina “procedimiento”, éste no contiene procedimientos, sino un conjunto de políticas y responsables para que el intercambio seguro de información entre sistemas).

b. **Observaciones a la información de interfaces suministrada en el catálogo de sistemas de información:** Como resultado de la revisión efectuada a la información de interfaces suministrada por la Dirección de TIC en el catálogo de sistemas de información, la OCI identificó las siguientes situaciones (en el Anexo 3 del presente informe se presenta el detalle de las observaciones a la información de interfaces suministrada):

OBSERVACIÓN OCI	CANTIDAD	PORCENTAJE
Sistemas que generan interfaz y se determina el tipo de integración, pero no se estipula el sistema destino	10	53%
Sistemas que generan interfaz pero no se estipula el sistema destino	5	26%
Sistemas que generan interfaz pero no se estipula el sistema destino ni el tipo de integración	1	5%

OBSERVACIÓN OCI	CANTIDAD	PORCENTAJE
Casos para los que no se estipuló el tipo de integración de la interfaz	1	5%
No se estipuló el tipo de integración entre "Contratista" y "TMSA", los cuales a juicio de la OCI tampoco corresponden a sistemas de información	1	5%
Se define tipo de integración pero no se estipula nombre de la interfaz ni sistema que consume el servicio	1	5%
TOTAL	**19**	**100%**

c. **Diferencias en la información de interfaces suministrada por la dirección de TIC:** La información sobre las interfaces de los sistemas de información fue suministrada por la Dirección de TIC en 3 archivos así:

   c. Mediante correo electrónico del día 30-oct-2020 se reciben los documentos "SistemasInformacionTICOrigenDestinoV.0.xlsx" e IntegracionSistemasInformacionTicV.1.pptx"

   d. Mediante correo electrónico del día 17-nov-2020 se recibe el documento "TMSA_20201103_Validación de la información aportada sobre SI (version 1).xlsx"

   Como parte de la revisión efectuada a la documentación mencionada fueron identificadas las siguientes observaciones:

SistemasInformacionTICOrigenDestinoV.0.xlsx		Presentación PowerPoint: Integración Sistemas de Información		OBSERVACIONES DE OCI
Aplicación Origen	**Aplicación Destino**	**Aplicación Origen**	**Aplicación Destino**	
Espacial	Portal de Datos Abiertos			Interfaces en "SistemasInformacionTICOrigenDestinoV.0.xlsx" no existentes en la presentación PowerPoint "Integración Sistemas de Información.pptx"
SAE	Espacial			
		SAE	GTFS Estático	Interfaces en la presentación PowerPoint "Integración Sistemas de Información.pptx" no existentes en el archivo "SistemasInformacionTICOrigenDestinoV.0.xlsx"
		DOC T	Sistema de Apoyo a Interventoria	

Fuente: Construcción de la OCI con base en la información suministrada por la Dirección de TIC durante el ejercicio

d. **Evaluación a los controles de las interfaces:** Mediante reunión virtual realizada el día 10 de noviembre de 2020 con los ingenieros de la Dirección de TIC: Angela Patricia Umaña Muñoz, Cristian David Santiago Gutierrez Gil, Jorge Iván Flórez Franco, José Luis Garnica Quiroz, David Monroy Machado, fue realizada la validación de los controles implementados a las interfaces entre los sistemas FCSCenter y sistema estadístico, entre el sistema estadístico y el sistema de apoyo a interventoría y entre el sistema SAE y el sistema espacial. Como resultado se identificaron las siguientes observaciones:

Sistema FCSCenter - sistema estadístico

Aunque fue suministrado el documento “20201115 InfromacionOCI.docx” a la OCI, el día 20 de noviembre de 2020, con detalles del proceso de validación adelantado por la Dirección de TIC a la información proveniente del sistema FCSCenter con destino al sistema estadístico, se advierte que la Entidad no dispone de procedimientos formalmente establecidos para asegurar la calidad, integridad y seguridad de la información que fluye entre ambos sistemas.

Por medio de procesos ETL ("Extract, Transform and Load", es un tipo de integración de datos referidos a las acciones de: extraer, transformar, cargar, que se utilizan para procesar datos provenientes de múltiples fuentes), los cuales son ejecutados diariamente, la Dirección de TIC toma la información almacenada en el FTP (Protocolo de transferencia de archivos, en inglés File Transfer Protocol o FTP) suministrado por Recaudo Bogotá relacionada con validaciones zonales, troncales, duales, venta y recarga de tarjeta y de la página de datos abiertos de TMSA; posteriormente, se lleva dicha información al sistema estadístico. Dado que en este proceso no se ejecutan rutinas de validación a la calidad e integridad de la información, la información tomada para el cargue en el sistema Estadístico podría contener errores o inconsistencias.

sistema estadístico - sistema de apoyo a interventoría

Aunque fue suministrado a la Oficina de Control Interno el documento “InfromacionOCI12112020.docx” por correo electrónico el día 13 de noviembre de 2020 con los detalles del proceso de lectura y cargue de información adelantado por la Dirección de TIC a la información proveniente del sistema estadístico con destino al sistema de apoyo a interventoría, se advierte que,

para esta interfaz, la Entidad no cuenta con procedimientos formalmente establecidos para asegurar la calidad y integridad y seguridad de la información que fluye entre este sistema y el sistema de apoyo a interventoría.

Previo al proceso de cargue de información al sistema de apoyo a interventoría, la Dirección de TIC no adelanta procesos de validación o verificación de la calidad de la información generada por el sistema estadístico (la información se toma mediante web service del Sistema Estadístico y Sistema Espacial según corresponda); por lo que el procedimiento establecido para identificar eventuales inconsistencias en la información de la interfaz es el reporte por parte de cualquier usuario de que no se visualiza algún vehículo, conductor o ruta (lo anterior debido a que la información de la interfaz depende de la información existente en el sistema fuente), la cual corresponde a una medida correctiva y no preventiva.

En la reunión de socialización de la presente observación ante la Dirección de TIC (10 de noviembre de 2020), los ingenieros asistentes a la reunión manifestaron que durante el proceso de construcción de los sistemas estadístico y de apoyo a interventoría se tomó información de muestra con la cual se validó el correcto cargue de información; así mismo se mencionó, que en caso de que un usuario reporte la carencia de un determinado dato en la interfaz, esto usualmente obedece a que en el sistema origen no existe dicho dato y que por lo tanto es necesario que el área responsable lo registre en el sistema origen con el fin de que el sistema de apoyo a interventoría pueda visualizarlo. Al respecto la OCI advierte que el mecanismo de detección de errores existente es correctivo y no preventivo, y se detecta porque tiene impacto sobre la funcionalidad del sistema de apoyo a la interventoría (es decir que la carencia de otro tipo de información podría no ser detectada por el sistema destino).

Sistema SAE - sistema espacial

Aunque la Dirección de TIC suministró a la OCI por correo electrónico el documento “solicituInterfaces.docx” el día 20 de noviembre de 2020 con los detalles del proceso de lectura de la información de interfaz proveniente del sistema SAE y su cargue al sistema espacial, elaborado por la dirección de TIC, la entidad no cuenta con procedimientos formalmente establecidos para asegurar la calidad, integridad y seguridad de la información que fluye entre este sistema y el sistema espacial, es decir que no han sido estipulados de manera formal los controles y protecciones que deben aplicarse entre la generación de datos del sistema origen y el cargue de los mismos en el sistema destino. Cabe mencionar que dentro del sistema no se cargan archivos interfaz.

4. Resultados de la encuesta realizada a los responsables de asegurar la calidad, integridad y seguridad de la información existente en las interfaces de los sistemas de información.

Objetivo de la encuesta: Obtener información de las diferentes dependencias de TMSA acerca de los controles implementados en los procesos de generación, validación y cargue de la información de las interfaces entre los diferentes sistemas de la entidad.

Fecha de realización: 24 de noviembre de 2020

Descripción de la encuesta: La encuesta consta de 37 preguntas (ver detalle de las mismas en el Anexo 4 del presente informe), de las cuales, 6 corresponden a datos del encuestado, 2 a la identificación del sistema origen y sistema destino respectivamente, y las 29 preguntas restantes buscan

identificar los controles implementados por la entidad a nivel de cada una de las interfaces entre los sistemas de información. Dado que el elemento de información clave en la encuesta es "la interfaz" y que ésta se identifica a partir de las relaciones entre los sistemas origen y los sistemas destino de la entidad, las respuestas de los encuestados requeridas para el análisis son las 29 preguntas restantes.

De esta forma, y conforme a las respuestas presentadas en la encuesta, existen 18 interfaces para las cuales se validan las 29 preguntas de control que fueron diseñadas por la Oficina de Control Interno, se aclara así mismo que conforme al formato de la encuesta, de este universo de 29 preguntas, los encuestados debieron contestar un número menor debido a que la mayoría de las preguntas estaban condicionadas a las respuestas de preguntas previas. En el siguiente ejemplo, si el encuestado responde sí a la pregunta 1, se habilitarán las preguntas desde a hasta d, en caso contrario, deberá contestar la pregunta e.

1. ¿Emplea herramientas informáticas de apoyo para verificar la calidad de la información?
   Sí:
   a. Por favor indique las características de la herramienta utilizada para a cabo la verificación de la información de la interfaz.
   b. ¿Considera que son suficientes las herramientas existentes para llevar a cabo las validaciones a la información de la interfaz?
   c. Por favor explique qué otras herramientas considera necesarias para fortalecer el proceso de validación de la interfaz
   d. ¿Considera necesario fortalecer el domino sobre las herramientas informáticas que utiliza para verificar la calidad de la información de la interfaz?

   No:
   e. Por favor indique las razones por las cuales no considera necesario el uso de herramientas tecnológicas para verificarla información de la interfaz

Conforme a lo mencionado, los análisis realizados en el presente informe corresponden a las respuestas presentadas para cada una de las 18 interfaces referidas en la encuesta.

Personal objetivo: Todas las personas que son responsables de asegurar la calidad, integridad y seguridad de la información existente en las interfaces de los diferentes sistemas de información de TMSA.

En cumplimiento de este objetivo, la Dirección de TIC indicó a la Oficina de Control Interno el nombre de las dependencias que gestionan interfaces de sistemas de información en la entidad. La Oficina de Control Interno remitió un correo electrónico a los directores de dichas áreas solicitándoles remitir la encuesta a los responsables de gestionar dicha información.

Notas aclaratorias para la interpretación de los resultados de la encuesta:

Nota 1. Las respuestas para las interfaces "Sistema Estadístico" - "Transmiapp", "Sistema Espacial" - "Transmiapp", "MiZonal" - "Transmiapp" y "Extra-digital" - "Transmiapp" fueron contestados en un solo registro. Para efectos de nuestros análisis, esta información fue separada en 4 registros así:

f. "Sistema Estadístico" - "Transmiapp",
g. "Sistema Espacial" - "Transmiapp",
h. "MiZonal" - "Transmiapp", y
i. "Extra-digital" - "Transmiapp"

Nota 2. Las respuestas presentadas por la Oficina de Control Interno relacionadas con el sistema "ACL" no se tienen en cuenta dentro de

los análisis que se presentan, toda vez que dicha herramienta no corresponde a un sistema de información, sino un software de análisis de datos.

Número de respuestas obtenidas: 18 (correspondientes a las 18 interfaces mencionadas en la encuesta, cada una de las cuales se identifica mediante las columnas “nombre sistema origen” y “nombre sistema destino”).

Número de personas que contestaron la encuesta: 7 (es decir, que las 18 interfaces son gestionadas por 7 personas, las cuales son responsables de la lectura de información del sistema origen, validación y cargue en el sistema destino).

Dependencias que contestaron la encuesta: Las 7 personas responsables de las interfaces pertenecen a las siguientes dependencias:

j. Dirección Corporativa
k. Dirección de TIC
l. Dirección Técnica de BRT
m. Oficina de Control Interno

RESULTADOS DE LA ENCUESTA

4.1. Sistemas origen - Destino:

Conforme a los resultados de la encuesta, en la siguiente tabla se identifican los sistemas origen (generadores de información de interfaz) y destino (consumidores de la información existente en las interfaces):

SISTEMA ORIGEN	SISTEMA DESTINO
Sistema Estadistico	Sistema Apoyo a Interventoría
Sistema de Apoyo a Interventoría	TDOC
Geoportal	Sistema de Apoyo a Interventoria
OUTLOOK	TDOC
SAE	Sistema Espacial
MiZonal	Transmiapp
jsp7 modulo facturación	Carvajal facturacion electrónica
jsp7	mi planilla
SAE	VisionBRT
FcsCenter	Bodega de Datos
Sistema Estadístico	Transmiapp
Sistema Espacial	Transmiapp
Sistema Extra-digital	Transmiapp
SAE	MiZonal (TICS-DTB)
Tabla Maestra SIRCI: Captura de información por interfaz gráfica	Tabla Maestra SIRCI: Almacenamiento en base de Datos
Indicadores de Programación: Interfaz gráfica de cargue	Indicadores de Programación: Almacenamiento en la base de datos
Tabla Maestra SIRCI: Interfaz web de cargue	Tabla Maestra SIRCI: Almacenamiento en la base de datos
TransmiSuevey (App movil)	TransmiSuevey API

Fuente: Resultados de la encuesta realizada a los responsables de gestionar la información de las interfaces de los sistemas de información de la entidad.

Respecto de la anterior información, la OCI advierte que las interfaces generadas entre los sistemas origen y destino que se encuentran en color gris, no figuran en el catálogo de sistemas de información de la Entidad.

4.2. Existencia de políticas y procedimientos de control formalmente establecidos para la transferencia de información entre sistemas de información

En atención a la siguiente pregunta: “(Solo para ser diligenciada por la dirección de TIC): En cumplimiento del numeral 6.1.2. del procedimiento para el intercambio seguro de información electrónica (P-DT-012), agradezco confirmar si la entidad dispone de políticas, procedimientos y controles de transferencia formales dirigidos a proteger la transferencia de información, mediante todo tipo de instalaciones de comunicaciones.”, el 100% de los encuestados manifestaron que la entidad dispone de políticas y procedimientos formalmente establecidos para el control de la transferencia de información entre sistemas. Del mismo modo, a la pregunta: “¿En la práctica se siguen las políticas y los procedimientos establecidos?”, el 100% manifestó que en la práctica sí se siguen (ver detalle de las respuestas presentadas en el Anexo 5 del presente informe).

En relación con las anteriores respuestas, y teniendo en cuenta que los resultados de la consultoría anteriores a la realización de la esta pregunta difieren de los análisis que pueden obtenerse con las respuestas presentadas para esta pregunta, la OCI advierte que si bien, el documento “P-DT-012 Procedimiento para el intercambio seguro de información electrónica Versión 1 de abril de 2019” establece un conjunto de políticas para la transferencia de información entre sistemas de información, éste no define los procedimientos de lectura, validación ni cargue de información entre sistemas de manera general, ni para interfaces específicas.

4.3. Existencia de registros que evidencien el cumplimiento de los procedimientos de verificación definidos para la interfaz

A la pregunta: "¿Se mantienen registros que evidencien el cumplimiento de los procedimientos de verificación definidos para la interfaz?", los 7 responsables de las 18 interfaces de los sistemas de información respondieron negativamente, es decir, que no se llevan registros que evidencien el cumplimiento de los procedimientos de verificación definidos para la interfaz

Al respecto, la Oficina de Control Interno advierte la importancia de mantener registros que permitan evidenciar el cumplimiento cabal de las políticas y procedimientos corporativos establecidos, incluyendo los relacionados con el aseguramiento de la calidad, integridad y seguridad de la información contenida en las interfaces de los sistemas de información.

4.4. Preguntas no contestadas por un número representativo de encuestados:

Las siguientes preguntas, fueron contestadas solo para 3 interfaces de las 18 existentes (para 15 interfaces restantes la pregunta no fue contestada); por lo anterior, no es posible presentar un análisis concluyente de las respuestas presentadas:

- ¿Cuál es el tiempo promedio requerido en los procesos de validación adelantados sobre la interfaz? (ver detalle de las respuestas presentadas a esta pregunta en el Anexo 12 del presente informe)
- ¿Considera suficiente el tiempo establecido para llevar a cabo las validaciones a la calidad de la información, transformar (de ser el caso) y cargar la información en el sistema destino?
- ¿En general, cómo considera el nivel de calidad de la información generada en el archivo de interfaz?

- Por favor identifique el nivel de confidencialidad de la información contenida en la interfaz
- ¿Cuenta el repositorio que almacena la interfaz, con restricciones que limiten el acceso a la información únicamente al personal autorizado?
- Por favor indique las características de los controles implementados por la entidad para asegurar la calidad, confiabilidad y seguridad de la información de la interfaz (ver detalle de las respuestas presentadas a esta pregunta en el Anexo 13 del presente informe).
- ¿Con qué frecuencia es rechazada la información generada en el archivo de interfaz por no cumplir los criterios mínimos de calidad?
- Cuando la interfaz es rechazada por deficiencias en la calidad de la información, ¿qué tan oportuna es la corrección y reenvío de la misma?
- ¿Se mantiene una copia de respaldo de las interfaces generadas?
- Por favor indique el período de retención de la información respaldada

Igual situación se presenta para la pregunta: "¿Generan las acciones de supervisión informes de resultados, que son socializados con los responsables y demás niveles pertinentes?", la cual solo fue respondida para 8 interfaces de las 18 existentes (ver detalle de las respuestas presentadas en el Anexo 9 del presente informe).

4.5. Conclusiones de la encuesta, afectadas por las preguntas no contestadas

Las preguntas que se listan a continuación, no fueron contestadas por el 33% de los encuestados (es decir, para 6 interfaces de las 18 existentes), por lo que las conclusiones obtenidas se basan en las respuestas del 67% restante:

- ¿Cuenta la entidad con un documento que describa las condiciones mínimas de calidad que debe cumplir la información de la interfaz para ser aceptada por el sistema destino?

- ¿Dispone la entidad de instancias responsables de supervisar periódicamente los resultados de la validación realizada a la información de la interfaz?
- ¿Emplea herramientas informáticas de apoyo para verificar la calidad de la información?
- ¿Considera que son suficientes las herramientas existentes para llevar a cabo las validaciones a la información de la interfaz?
- ¿Considera necesario fortalecer el domino sobre las herramientas informáticas que utiliza para verificar la calidad de la información de la interfaz?

A continuación, se presentan las conclusiones de cada una de las anteriores preguntas, las cuales, como se mencionó, están afectadas por las respuestas no contestadas, las cuales corresponden a un 33%:

a. ¿Cuenta la entidad con un documento que describa las condiciones mínimas de calidad que debe cumplir la información de la interfaz para ser aceptada por el sistema destino?

Dos (2) de las 18 respuestas (es decir, el 11%) fueron contestadas afirmativamente, 10 fueron contestadas negativamente (es decir, el 56%), (ver detalle en el anexo 6 del presente informe). La OCI advierte la importancia de la entidad formalice en el corto plazo las condiciones mínimas de calidad que debe cumplir la información de las interfaces, para asegurar su aceptabilidad en los sistemas consumidores de dicha información; así como la necesidad de dar a conocer a los responsables de gestionar esta información, la existencia o no de las condiciones mínimas de calidad descritas anteriormente.

b. ¿Dispone la entidad de instancias responsables de supervisar periódicamente los resultados de la validación realizada a la información de la interfaz?

Para los responsables de 8 interfaces de las 18 existentes (correspondiente al 44%), la Entidad contestó que cuenta con instancias responsables de supervisar periódicamente los resultados de validación de la información de la interfaz, mientras que para 4 responsables (correspondiente al 22%) la entidad no se cuenta con dichas instancias, (ver detalle en el anexo 7 del presente informe). La OCI resalta la importancia de definir e implementar mecanismos o instancias de supervisión y control de los resultados de la validación realizada a la información de la interfaz, así como de dar a conocer dichas medidas (en caso de existir) a los responsables que no contestaron la pregunta.

c. ¿Emplea herramientas informáticas de apoyo para verificar la calidad de la información?

Para 1 responsable de las 18 interfaces existentes (correspondiente al 6%) la Entidad contestó que emplea herramientas informáticas de apoyo para verificar la calidad de la información de las interfaces, mientras que para 11 responsables de interfaces (correspondiente al 61%) no se emplean dichas herramientas (ver detalle en el anexo 8 del presente informe). La OCI recomienda el uso de herramientas informáticas de apoyo al proceso de lectura, validación y cargue de información de las interfaces en los sistemas destino debido a que favorecen no solo la efectividad y el desempeño de estos procesos de control descritos, sino el aseguramiento de la calidad, integridad y seguridad de la información de las interfaces.

d. ¿Considera que son suficientes las herramientas existentes para llevar a cabo las validaciones a la información de la interfaz?

Doce (12) responsables de interfaces de las 18 existentes (correspondiente al 67%) contestaron que son suficientes las herramientas existentes para llevar a cabo las validaciones a la información de la interfaz (ver detalle en el anexo 10 del presente informe). La OCI resalta la importancia de que la Entidad defina e implemente instancias de supervisión y control sobre los resultados del proceso de validación y cargue de la interfaz en los sistemas destino, así como de dar a conocer dichas medidas (en caso de existir) a los responsables que no contestaron la pregunta. La supervisión del cumplimiento de las medidas de control descritas, reducen la posibilidad de que se presenten errores o manejos indebidos sobre la calidad, integridad y seguridad de la información que contienen las interfaces.

e. ¿Considera necesario fortalecer el domino sobre las herramientas informáticas que utiliza para verificar la calidad de la información de la interfaz?

Un (1) encuestado manifestó emplear herramientas informáticas de apoyo para verificar la calidad de la información de las interfaces; sin embargo, en la pregunta subsecuente, 9 de los 18 responsables de las interfaces (correspondiente al 50%) consideran necesario fortalecer el domino de las herramientas informáticas para verificar la calidad de la información de las interfaces; tres (3) responsables de gestionar las interfaces (correspondiente al 17%) consideran que no es necesario fortalecer dicho domino (ver detalle en el Anexo 11 del presente

informe), El personal encuestado destaca la necesidad de fortalecer el domino de las herramientas informáticas para apoyar el aseguramiento de la calidad, integridad y seguridad de la información contenida en las interfaces, lo cual supone además la necesidad de disponer de tales herramientas como parte de su labor.

CONCLUSIONES:

Como resultado del trabajo de consultoría realizado por la Oficina de Control Interno, se presentan las siguientes conclusiones:

1. Al momento de realización de la consultoría, la dirección de TIC se encontraba actualizando el catálogo de sistemas de información, por lo cual no existe certeza acerca del número total de sistemas de información con que cuenta la Entidad, ni por tanto del número de interfaces que permiten su interrelación.

2. La información contenida en el catálogo de sistemas de información no se encuentra debidamente alineada con aquella contenida en el inventario de activos de información en lo relacionado con los sistemas de información existentes.

3. La información aportada por la Dirección de TIC a la OCI, en relación con las interfaces de los sistemas de información existentes presentó diferencias, situación que genera incertidumbre en la confiabilidad de dicha información.

4. Teniendo en cuenta que la entidad no dispone de procedimientos formalmente establecidos para validar la información de las interfaces de los sistemas origen, ni para procesar dicha información en los sistemas destino, no resulta factible emitir una conclusión respecto de si es adecuado el diseño de los controles existentes, ni por tanto, poder calificar su efectividad.

5. Para las tres interfaces evaluadas: sistemas FCSCenter - sistema estadístico; sistema estadístico - el sistema de apoyo a interventoría; y sistema SAE - el sistema espacial, se concluye que ninguno de ellos cuenta con rutinas de validación de la información, que se ejecuten previas al proceso de cargue al sistema destino.

6. La Entidad no cuenta con información de detalle para la totalidad de las interfaces de los sistemas de información

7. Con base en los resultados de la encuesta realizada y en el análisis de los resultados obtenidos por la Oficina de Control Interno previos a la realización de la misma, se presentan las siguientes conclusiones:

   a. La información de los sistemas origen y destino resultante de la consultoría (y la cual determina el número de interfaces existentes) difiere de la obtenida a través de la encuesta (12 de las interfaces mencionadas en la encuesta no figuran en el catálogo de sistemas de información).

   b. Con base en la encuesta, el 100% de los encuestados que pertenecen a la Dirección de Tic manifiestan que la entidad dispone de políticas y procedimientos formalmente establecidos para el control de la transferencia de información entre sistemas; sin embargo, la entidad no aportó copia de las mismas a la OCI en atención a las solicitudes de información realizadas.

RECOMENDACIONES:

Con base en los resultados obtenidos de la evaluación a los controles establecidos por la Entidad a la información de las interfaces de los diferentes sistemas de

información, a continuación, damos a conocer las oportunidades de mejora respectivas, para que sean evaluadas e implementadas:

1. Elaborar y mantener el diagrama arquitectónico de la red de cómputo existente con la representación visual de la red LAN y WAN como un complemento del diagrama topológico de la red de TMSA, que identifique entre otros los siguientes componentes: subredes alámbricas a inalámbricas, servidores, enrutadores, hubs, conectividad con redes externas, cortafuegos, etc. En criterio de la OCI, la anterior información facilitaría a la dirección de TIC gestionar adecuadamente esta clase de activos tecnológicos, prestarles el soporte técnico requerido, así como diagnosticar y fortalecer su desempeño funcional y de seguridad.

2. Adoptar lo que se considere aplicable y conveniente de la Guía para la construcción del catálogo de Sistemas de Información del MINTIC". Si bien, ésta contiene sugerencias que no son de forzoso cumplimiento por parte de la entidad para la elaboración del catálogo de sistemas de información, su adopción traería múltiples beneficios (los cuales se relacionan en el mismo documento).

3. Asegurar la alineación en contenido de los siguientes documentos, los cuales constituyen la base para llevar a cabo la gestión de activos tecnológicos, la gestión de seguridad de la información, y la gestión del servicio (norma ITIL):

   - El catálogo de sistemas de información,
   - El inventario de activos de información, y
   - La base de datos de elementos de configuración (denominada CMDB).

4. Definir e implementar medidas de control dirigidas a asegurar el cumplimiento de lo establecido en el documento "I-DT-001 instructivo para la identificación,

valoración y clasificación de activos de información versión 0 de abril de 2019" en todos sus numerales. Como punto de partida se recomienda ajustar los siguientes aspectos, los cuales fueron mencionados en el informe:

- Incorporar dentro del catálogo de sistemas de información la totalidad de los sistemas utilizados por TMSA.
- Retirar del catálogo de sistemas de información aquellas herramientas que no sean consideradas sistemas de información (por ejemplo, hojas de cálculo y bases de datos)
- Asignar a los sistemas de información de la entidad un nombre único y emplear siempre dicho nombre en cualquier documento corporativo que lo requiera.
- Desplegar la información de detalle de cada sistema requerida en el catálogo de sistemas de información, evitando las celdas en blanco.
- Describir en forma clara el propósito de cada sistema
- Establecer categorías y tipologías estándar y convenientes para la entidad aplicables a los sistemas de información, evitando el uso de categorías redundantes, duplicadas o ambiguas.
- Separar las categorías "Fabricante" y "Proveedor de soporte", con el fin de facilitar la diferenciación entre el fabricante de los sistemas de información, del agente responsable de su soporte.
- Utilizar la totalidad de los atributos establecidos en la guía para la construcción del catálogo de Sistemas de Información del MINTIC que resulten aplicables en la entidad.
- Definir una estructura estándar de campos (columnas) para la identificación de la arquitectura tecnológica de los sistemas de información, con el uso de categorías únicas para sistema operativo, tipo de sistema, categoría, plataforma, base de datos, etc.

5. Asegurar y mantener una alineación permanente entre la información del catálogo de sistemas de información, la contenida en el inventario de activos de información, así como la de cualquier otro documento corporativo que también emplee información relacionada con sistemas de información, tales como: el catálogo de servicios de tecnología, la base de datos de elementos de configuración requerida en la gestión del servicio, etc.

6. Evaluar la conveniencia de incluir dentro del catálogo de sistemas de información, por cada sistema, la siguiente información clave relacionada con las interfaces de los sistemas:

   - Identificación del sistema que generan información
   - Identificación del sistema que consumen información
   - Nombre de la interfaz
   - Tipo de integración
   - Características y descripción de la información compartida entre sistemas
   - Frecuencia de generación o de cargue
   - Nombre de la dependencia que origina la información
   - Nombre de la dependencia que recibe la información
   - Nombre del proceso que origina la información
   - Nombre del proceso que recibe la información
   - Diccionario y estructura de los datos procesados en la interfaz
   - Medio de envío
   - Descripción de los controles preventivos diseñados para evitar la materialización de riesgos sobre la calidad, integridad y seguridad de la información de la interfaz
   - Descripción de los controles detectivos diseñados para identificar oportunamente la eventual materialización de riesgos sobre la calidad, integridad y seguridad de la información de la interfaz

- Descripción de los controles correctivos diseñados para ajustar la información que fue cargada con errores de calidad, integridad y/o seguridad.
- Nombre del documento corporativo que describe los procedimientos para prevenir, detectar y corregir la materialización de riesgos como los siguientes:

    - Errores en la información generada por las aplicaciones,
    - Información indebidamente modificada,
    - Errores en la estructura o formato de la información generada
    - Acceso no autorizado a la información generada, procesada y/o cargada,
    - Diferencias entre la información generada y la información cargada,
    - Información débilmente validada
    - Información cargada múltiples veces al sistema destino.

- Descripción de las validaciones realizadas a la información generada

7. Complementar la información del catálogo de sistemas de información con la información de interfaces faltante de los sistemas de información. Para el caso de los sistemas de información que son propiedad de Recaudo Bogotá y que se intercomunican con sistemas de información de TMSA, se recomienda identificarlos dentro del catálogo como sistemas que no son propiedad de TMSA o registrarlos de manera separada, pero vinculándolos a los sistemas de información de TMSA con los cuales se intercomunica.

8. Definir e implementar conjuntamente entre las áreas funcionales y la Dirección de TIC, las reglas de validación que resulten aplicables para asegurar la calidad y seguridad del dato, así como los criterios de conciliación de información entre los sistemas origen y destino.

9. Establecer un documento corporativo que defina la estructura, el contenido, frecuencia de actualización y la metodología para el diligenciamiento de la información del catálogo de sistemas de información de la Entidad. Como parte de esos lineamientos y con el fin de evitar el registro de información inconsistente o no homogénea dentro del catálogo, se recomienda que su diligenciamiento se realice de manera conjunta por personal de las diferentes áreas funcionales y de la Dirección de TIC, y por otra parte, como complemento de la medida anterior, designar un responsable de supervisar periódicamente el cumplimiento del documento descrito, quien, para tal efecto, puede elaborar el informe de supervisión respectivo y darlo a conocer a los niveles directivos pertinentes.

El presente documento fue socializado con la Dirección de TIC en reunión virtual realizada el día 10 de noviembre de 2020 y complementada el día 1 de diciembre de 2020, con el envío de un correo electrónico por parte de la Dirección de TIC con sus comentarios a la redacción en borrador, de las diferentes observaciones que fueron identificadas por la Oficina de Control Interno en desarrollo del presente trabajo.

Cualquier información adicional con gusto será suministrada.

Bogotá D.C., 18 de diciembre de 2020,

LUIS ANTONIO RODRÍGUEZ OROZCO
Jefe Oficina de Control Interno

Elaboró: Néstor Orlando Velandia Sosa- Contratista, Oficina de Control Interno
Revisó: Luz Marina Díaz Ramírez - Contratista, Oficina de Control Interno