INFORME EVALUACIÓN INDEPENDIENTE A LA GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES – TIC PARA LA VIGENCIA 2016
CONTRALORÍA GENERAL DE MEDELLÍN

PATRICIA BONILLA SANDOVAL
Contralora General de Medellín

EFIGENIA SUESCÚN VEGA
Jefe Oficina Asesora de Control Interno
Coordinador General del Informe

CARLOS ANDRÉS ARBELÁEZ VELÁSQUEZ
Profesional Universitario 1

OFICINA ASESORA DE CONTROL INTERNO

MEDELLÍN, FEBRERO DE 2017

Contraloría General de Medellín
¡Con tu participación, Medellín crece!

1. RESUMEN EJECUTIVO

Como resultado de la aplicación de la auditoría independiente a la gestión de las tecnologías de la información y las comunicaciones -TIC- para la vigencia 2016, en lo relativo a la evaluación de desarrollo, adquisición y las operación de las soluciones, además de evaluación la gestión de la seguridad informática se encontraron: 6 aspectos positivos, 2 observaciones y se plantearon 4 recomendaciones. Los aspectos positivos se relacionan fundamentalmente con el desarrollo y la prueba de las soluciones, además de la forma en que se atienden las solicitudes y requerimientos en el sistema Mercurio. Una de las observaciones se relaciona con la ausencia de un mecanismo formal de atención de solicitudes y requerimientos para el sistema Gestión Transparente y la otra con la existencia de algunas vulnerabilidades de seguridad informática en los dos sistemas de información citados. Las recomendaciones planteadas se relacionan con: aprovechar la fortaleza del mecanismo ya establecido para atención de solicitudes y requerimientos del sistema Mercurio, además de implementación de un mecanismo similar para el caso del sistema Gestión Transparente, la mejora el proceso de gestión de la seguridad de la información y la seguridad informática en la organización, y por último la revisión de la documentación existente para la gestión de las TIC.

2. ANTECEDENTES

La Contraloría General de Medellín como resultado del continuo interés por garantizar el logro de los objetivos institucionales, ha tenido a bien realizar una evaluación independiente sobre la gestión de la tecnología de la información -TIC- realizada en la institución, para lo cual la Oficina de Control Interno incluyó en su Plan de Actividades, la realización de la evaluación teniendo como criterios lo dispuesto normativamente al respecto y las buenas prácticas internacionalmente aceptadas para la gestión TIC como lo son COBIT 5, ITIL V3 e ISO 2700.

Cabe anotar que antes de la realización de esta auditoría no se tiene registro de la aplicación de una evaluación independiente a la gestión de la tecnología de la información y la comunicación en la Contraloría General de Medellín, por lo que este esfuerzo se desarrolla como resultado de incremento del interés en la administración en las TIC como un catalizador para el logro de los objetivos institucionales, situación que fue tenida en cuenta para abordar la evaluación desde un nivel macro que aporte valor desde el punto de vista estratégico a la organización.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Evaluar la eficiencia, eficacia y confiabilidad en la gestión de tecnología de la información y las comunicaciones -TIC- de la Contraloría General de Medellín mediante la aplicación de procedimientos que permitan conceptuar sobre el nivel de adopción de las buenas prácticas aceptadas internacionalmente en la materia, el cumplimiento de la ley general de archivo 1581 de 2012, la ley de habeas data 1581 de 2012 y el Procedimiento de Administración y Mantenimiento de las TIC P-GI-I-001 definido en el sistema de gestión de la calidad.

3.2 OBJETIVOS ESPECÍFICOS

- Evaluar el desarrollo y adquisición de soluciones TIC.
  - Evaluar la forma en que se controlan los proyectos de TIC.
  - Evaluar la forma en que se prueban las soluciones TIC.

- Evaluar la operación de las soluciones TIC.
  - Evaluar la forma en que establecen y monitorean los acuerdos de nivel de servicio -SLA-.
  - Evaluar la forma en que se gestión los incidentes y los problemas.

- Evaluar la gestión de la seguridad informática.
  - Evaluar la forma en que se identifican los riesgos de seguridad informática.
  - Evaluar la forma en que se mitigan los riesgos de seguridad informática.
  - Evaluar la forma en que definen y asignan los roles en la gestión de la seguridad informática.
  - Evaluar la forma en que se entrena al personal en seguridad informática.

Contraloría General de Medellín
¡Con tu participación, Medellín crece!

4. ALCANCE

La evaluación independiente considerará para su ejecución la vigencia 2016, además se circunscribe a la evaluación de la infraestructura informática crítica y los sistemas de información Mercurio y Gestión Transparente.

5. CRITERIOS

- ITIL V3: Es un marco de mejores prácticas que se ha elaborado por los sectores público y privado a nivel internacional. En él se describe cómo los recursos de TI deben ser organizados para ofrecer un valor empresarial documentando los procesos, funciones y roles en la administración de servicios de tecnología informática.

- COBIT 5: **COBIT** (Control Objectives Control Objectives for Information and related Technology) es el marco aceptado internacionalmente como una buena práctica para el control de la información, Gestión de tecnología Informática -IT- y los riesgos que conllevan. **COBIT** se utiliza para implementar el gobierno de IT y mejorar los controles de IT.

- Incidente: Cualquier evento que no forma parte del desarrollo habitual del servicio de TIC y que causa, o puede causar una interrupción del mismo o una reducción de la calidad de dicho servicio. *(incluye los requerimientos, dudas, solicitudes y dificultades que son reportadas por los usuarios de un sistema informático).*

- Ley 594 de 2000 y decretos reglamentarios 4124 de 2004 y 1100 de 2014.

- Ley 1581 de 2012 y decreto reglamentario 1377 de 2013.

- Procedimiento P-GI-I-001 Administración y Mantenimiento de las TIC.

6. METODOLOGÍA

Cada etapa de la evaluación independiente, se realizó conjuntamente con los dueños del proceso y el personal de la Entidad involucrado en el mismo, mediante entrevistas y ejecución de pruebas para el desarrollo de la auditoría.

7. RESULTADOS DE LA EVALUACIÓN

7.1 EVALUACIÓN DEL DESARROLLO Y ADQUISICIÓN DE SOLUCIONES TIC

Por desarrollo de soluciones TIC, se entienden los esfuerzos que la organización realiza para obtener soluciones informáticas que se deben construir o ajustar según sus necesidades, es decir de alguna forma son soluciones personalizadas. De otro lado, por adquisición de soluciones TIC, se entiende la compra de soluciones que ya existen en el mercado como un estándar y que no tienen que ser construidas o ajustadas a la medida de la organización. La evaluación de la forma en que se adquieren dichas soluciones se hace importante dentro de la auditoría ya que la construcción, ajuste o implementación inadecuada de las mismas puede llevar a situaciones que reducen la eficiencia y/o la eficacia del uso de las TIC en la institución, como ocurre cuando se adquiere una aplicación de software que no puede integrarse con aplicaciones existes y luego obliga que los funcionarios realicen una parte del trabajo o ingreso de datos en un sistema y luego tengan que repetirlo en otro que se usa con una finalidad diferente.

Para evaluar el desarrollo y adquisición de soluciones TIC se revisó la forma que se controlan los proyectos de TIC y la forma en que se prueban las soluciones TIC antes de ponerlas a disposición de los usuarios finales.

Con respecto al control de los proyectos TIC, se analizaron las actas de supervisión y seguimiento aportadas por los funcionarios de la Contraloría Auxiliar de Desarrollo Tecnológico y se encontró que para el caso de los sistemas de información Mercurio y gestión transparente, cuya implementación y soporte se ha tercerizado mediante los contratos No. 002 de 2016 y contrato No. 20 de 2016 respectivamente, se realiza seguimiento adecuado a través de los mecanismos que ofrece la normativa en este sentido incluyendo controles al cumplimiento de las obligaciones que han adquirido los contratistas (principalmente actas de seguimiento).

En lo relativo a la forma en se prueban las soluciones de TIC, se analizó la documentación de los contratos mencionados, las actas de seguimiento a los mismos además de la información aportada en reunión con el personal de la C.A de Desarrollo Tecnológico el 10 de febrero de 2017, encontrándose lo siguiente:

Para el sistema de información Mercurio se tienen implementados ambientes de pruebas y producción

Pruebas en el sitio (http://10.6.201.36:8080/mercurio/index.jsp)

Producción en el sitio (http://10.6.201.37:8080/mercurio/index.jsp)

Los cuales se utilizan para probar los cambios y nuevas funcionalidades tanto desde el punto de vista técnico por parte del contratista en su rol desarrollador, el cual supervisado por el personal de la C.A de Desarrollo Tecnológico, y también por el usuario final que hará uso de la nueva funcionalidad. Una vez realizadas las pruebas y con la respectivas aprobaciones se procede a autorizar al contratista a para transportar los cambios a al ambiente de producción.

Para el sistema de información Gestión Transparente se analizó la documentación de los contratos mencionados, las actas de seguimiento a los mismos además de la información aportada en reunión con el personal de la C.A de Desarrollo Tecnológico el 10 de febrero de 2017, encontrándose que cuenta con ambientes de prueba y producción separados para la funcionalidad de rendición y la funcionalidad misional o de auditor.

Pruebas para rendición:
http://pruebasmedellin.gestiontransparente.com/Rendicion/Inicio.aspx

Pruebas para lo misional (Auditor):
http://pruebasmedellin.gestiontransparente.com/Misional/InicioContraloria.aspx

Producción para rendición:
http://medellin.gestiontransparente.com:8050/Rendicion/Inicio.aspx

Producción para lo misional (Auditor)
http://10.6.201.30:4042/SitePages/Gesti%c3%b3n%20transparente.aspx

Estos ambientes se utilizan para probar los cambios mayores antes de transportarlos al ambiente de producción del aplicativo. No obstante según se informó en reunión realizada el 10 de febrero de 2017, debido a la complejidad de la aplicación y su infraestructura además de las limitaciones presupuestales, no siempre es posible mantener sincronizados los ambientes de prueba como fiel copia de los ambientes de producción lo que puede eventualmente afectar la calidad de algunas pruebas.

En general, la gestión de las pruebas en las soluciones TIC conserva el espíritu de las buenas prácticas internacionales en la materia, especialmente en lo relativo a la gestión de cambios, como es el caso del proceso COBIT BAI06 cuyo propósito es: *"Posibilitar una entrega de los cambios rápida y fiable para el negocio, a la vez que se mitiga cualquier riesgo que impacte negativamente en la estabilidad e integridad del entorno en que se aplica el cambio"* y el proceso de gestión de cambios definido en ITIL, cuyo propósito es *"Controlar el ciclo de vida de todos los*

Cambios. El objetivo primordial de la Gestión de Cambios es viabilizar los cambios beneficiosos con un mínimo de interrupciones en la prestación de servicios de TI".

7.2 EVALUACIÓN LA OPERACIÓN DE LAS SOLUCIONES TIC

Por operación de las TIC se entiende todo el conjunto de actividades que se realizan en una solución TIC desde que se dispone para el uso de los usuarios a los que está destinada, hasta que se retira de circulación, pasando por la atención de todas fallas que presente y la atención de todos los requerimientos, preguntas, o consultas que realicen los usuarios que hacen uso de ella. La evaluación de la operación de la soluciones TIC se hace importante dentro de la auditoría ya que la operación inadecuada de las mismas puede llevar a situaciones en las que se reduce la eficiencia y/o la eficacia en el uso de las TIC en la institución, como ocurre cuando se adquiere y pone en funcionamiento una aplicación de software que, aunque técnicamente opera bien, es poco utilizada por las personas a las que está destinada porque no obtienen respuestas oportunas a las inquietudes, dudas o problemas que se les presentan al hacer uso el software.

Para evaluar este asunto de auditoría se revisó la forma en que se establecen y monitorean los acuerdos de nivel de servicio tanto entre la Contraloría General de Medellín y los contratistas, como entre la Contraloría General de Medellín y sus usuarios. Adicionalmente se evaluó la forma en que se atienden las solicitudes, requerimientos, dudas, inquietudes o problemas que los usuarios realizan a la C.A de Desarrollo Tecnológico, lo que técnicamente se conoce la gestión de incidentes y problemas.

Con respecto al establecimiento de acuerdos de nivel de servicio entre la Contraloría general de Medellín y sus contratistas se evaluaron los contratos asociados a cada sistema de información y la información aportada en reunión realizada con el personal encargado el 10 de febrero de 2017, y se encontró lo siguiente:

Para el sistema Mercurio que estos acuerdos se encuentran establecidos como parte de los estudios previos y propuesta que hacen parte integral del contrato No. 002 de 2016, los cuales definen los tipos de mantenimiento del que será objeto el software, la tabla de criticidad que servirá para clasificar la magnitud de los incidentes, además de los tiempos de respuesta convenidos, ver Cuadro 1:

Cuadro 1: Acuerdo de nivel de servicio establecido para el sistema de información Mercurio

Sistema de Información Mercurio	
Criticidad del incidente	**Tiempo máximo de respuesta**
Prioridad Alta (CRÍTICOS):	DOS HORAS (2) con atención inicial telefónica antes de los QUINCE (15) Minutos
Prioridad Media (PRIORITARIO)	DOCE HORAS (12), siempre y cuando el Cliente permita la disponibilidad tanto de conexión remota como de recurso humano con el perfil adecuado para el apoyo al soporte, con atención inicial telefónica antes de las DOS (2) Horas
Prioridad Baja (ESTÁNDAR)	VEINTICUATRO (24) HORAS con atención inicial telefónica antes de CUATRO (4) horas

Fuente: construcción propia a partir de los datos incluidos en el contrato No. 002 de 2016

Cabe anotar que estos mismos acuerdos de nivel de servicio se trasladan directamente hacia el usuario final ya que el soporte técnico para el sistema de información Mercurio se encuentra tercerizado.

Para el sistema de información Gestión Transparente, si bien en el contrato No. 20 de 2016 y sus estudios previos se definen claramente los productos y servicios que debe entregar el contratista a la Contraloría General de Medellín, no se encontró evidencia del establecimiento de acuerdos con respecto a los tiempos de respuesta que tendrá el contratista para atender las incidencias levantadas por la Contraloría. Adicionalmente, tampoco se encontró evidencia del establecimiento de acuerdos de nivel de servicio entre la Contraloría General de Medellín y los diversos usuarios que hacen uso del sistema Gestión Transparente, situación que es razonable en virtud de que no se establecieron acuerdos de nivel de servicio con el contratista correspondiente.

Con respecto a la gestión de incidentes y problemas, se analizaron los 4 informes de comportamiento de la mesa de ayuda producidos por la C.A de Desarrollo Tecnológico en 2016, además del reporte detallado de los casos atendidos mediante la aplicación mesa de ayuda en 2016 y la información aportada en reunión con personal de la C.A de Desarrollo Tecnológico el 10 de febrero de 2017, encontrándose lo siguiente:

Para el sistema de información Mercurio se cuenta con un esquema definido de atención de incidentes y problemas que se apoya fundamentalmente en el sitio Web de la mesa de ayuda, a través del cual se gestionaron en 2016, un total de

1.588 casos relacionados con el sistema mercurio, lo que representa el 37.16% de los casos atendidos, siendo de esta forma el servicio con el mayor número de casos, según datos reportados en el informe "Informe Comportamiento Mesa De Ayuda 4 Trimestre 2016" publicado por la C.A de Desarrollo Tecnológico.

En general la gestión de operaciones de TIC para los asuntos auditados, conserva parcialmente el espíritu de las buenas prácticas internacionales en la materia, como es el caso de:

- El proceso de Gestión del Nivel de Servicio (SLM) según ITIL, cuyo propósito es: "*Negociar Acuerdos de Nivel de Servicio (SLA) con los clientes y diseñar servicios de acuerdo con los objetivos propuestos, además de asegurar que todos los Acuerdos de Nivel Operacional (OLA) y Contratos de Apoyo (UC) sean apropiados, y de monitorear e informar acerca de los niveles de servicio.*"

- El proceso de gestión de incidentes según ITIL, cuyo propósito es: "*Manejar el ciclo de vida de todos los Incidentes con el fin de devolver el servicio de TI a los usuarios lo antes posible*."

- El proceso COBIT DSS02 Gestionar Peticiones e Incidentes de Servicio, cuyo propósito es: "Lograr **una mayor productividad** y minimizar las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.

Ya que según se evidencio, si bien el sistema de información Mercurio cuenta con acuerdos de nivel de servicio definidos, no ocurre lo mismo para el sistema Gestión Transparente. Adicionalmente, con respecto a la gestión de incidentes, se evidencio la existencia de mecanismos formalmente establecidos para tal efecto en el caso del sistema de información Mercurio, pero no el sistema Gestión Transparente, situación que es observada.

7.3 EVALUAR LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA

Para abordar adecuadamente la evaluación de este asunto de auditoría es importante primero diferenciar entre la seguridad de la información y la seguridad informática. La seguridad de la información se ocupa de la protección de ésta sin importar su medio de almacenamiento o transmisión, sean documentos físicos o las conversaciones de las personas; mientras que la seguridad informática se ocupa de la protección de la información sólo mientras es almacenada o transmitida mediante dispositivos informáticos. Por lo tanto la seguridad informática se considera sólo una parte de la seguridad de la información. La evaluación de la gestión de la seguridad informática se hace importante dentro de

la auditoría ya que se asocia directamente a la confiabilidad de la información que se gestiona a través de los sistemas de información evaluados, Mercurio y Gestión Transparente los cuales soportan procesos misionales.

Para evaluar la gestión de la seguridad informática se analizó la forma en que se identifican y mitigan los riesgos de seguridad informática, además de la asignación de roles en esta materia y el plan de capacitación que posee la entidad para mejorar las competencias de sus funcionarios en seguridad informática.

Con respecto a la forma en que se identifican los riesgos de seguridad informática, se analizó la información de identificación de riesgo consignada en el registro F-ES-I-013 dispuesto en la plataforma Isolución, el plan de contingencia de tecnología de la información 2016, y la información aportada por el personal de la C.A de Desarrollo Tecnológico en reunión realizada el 10 de febrero de 2017, además de los resultados de la aplicación de pruebas de seguridad no intrusivas realizadas por la Oficina de Control Interno encontrándose lo siguiente.

Existe evidencia de una identificación de riesgos en seguridad informática a través del diligenciamiento del formato con código F-ES-I-013 el cual se encuentran a acorde con la política de administración de riesgos establecida en documento código D-GE-PL-002, y con la norma NTC 27005. El Cuadro 2, presenta la identificación de algunos riesgos en seguridad informática contenida en el formato F-ES-I-013.

Adicionalmente, se encontró también evidencia de una identificación de riesgos en seguridad informática en el plan de contingencia de tecnología de la información 2016, el cual incluye entre sus objetivos los siguientes:

- Efectuar análisis de riesgos realizando una identificación y evaluación del hardware y software crítico a ser protegido.

- Realizar análisis de vulnerabilidades y riesgos que afectan a la información.

- Desarrollar una lista con las posibles medidas de seguridad la cual permita reducir los riesgos para el centro de datos de la Contraloría General de Medellín.

Y presenta además una identificación de 27 riesgos que podrían afectar el centro de datos principal, entre los que se cuenta incendio, explosión, sabotaje y pérdida del suministro de servicios esenciales como la energía eléctrica y el agua (el agua es necesario para refrigerar el centro de cómputo) entre otros.

Con respecto a la forma en que se mitigan los riesgos en seguridad informática, se analizó la misma información que se tuvo en cuenta para evaluar la forma en que

se identifican los riesgos, además de los informes mensuales del centro de datos, el memorando 037502-201600010741 dirigido a la Oficina Asesora de Control interno el 10 de junio de 2016 y el documento "Atención de Incidentes informáticos" aportado por la C.A Desarrollo Tecnológico encontrándose lo siguiente.

Cuadro 2: Riesgos de seguridad de la información identificados en el registro correspondiente al formato F-ES-I-013.

Código: F-ES-I-013 Versión:09	IDENTIFICACIÓN DEL RIESGO		
Nivel:	Apoyo		
Proceso:	Gestión Tecnología de la Información		
Objetivo:	Proceso: Innovar y mantener el desarrollo de las tecnologías de la información y las comunicaciones TIC de la entidad.		
Causas	**Riesgo**	**Descripción**	**Consecuencias potenciales**
Amenazas provenientes de fuentes externas: (virus, hacker, etc.) e internas: (los funcionarios de la entidad)	Vulnerabilidad en la seguridad interna y externa de las TIC	Es la incapacidad de resistencia cuando se presenta una amenaza cibernética o la incapacidad para reponerse después de que ha ocurrido.	Perdida de información. Violación de la privacidad. Sobrecostos administrativos y operativos.
Daños en los servidores ó en la Red. Fallas en los programas o en las bases de datos, suspensión del servicio eléctrico al centro de computo.	Errores en Hardware y Software	Mal funcionamiento de servidores ó red.	Suspensión del servicio. Pérdida de imagen. Perdida de información.

Fuente: Registro correspondiente al formato F-ES-I-013 extraído de Isolución

Existe evidencia de la definición de un tratamiento de los riesgos identificados en el registro del formato F-ES-I-03, especialmente en lo relacionado al implementación de controles de seguridad informática como son un sistema de control de tráfico en la red de datos (Firewall), un sistema de control de virus informáticos y mecanismos para gestionar las copias de seguridad de la información. El Cuadro 3 presenta las opciones de tratamiento para algunos riesgos identificados en el registro F-ES-I-013.

Cuadro 3: Tratamiento de riesgos de seguridad de la informática definidos en el registro correspondiente al formato F-ES-I-013.

Código: F-ES-I-013 Versión: 09	MAPA DE RIESGOS	
Nivel:	Apoyo	
Proceso:	Gestión Tecnología de la Información	
Objetivo:	Proceso: Innovar y mantener el desarrollo de las tecnologías de la información y las comunicaciones TIC de la entidad.	

Riesgo	Calificación		Evaluación Riesgo	Controles	Nueva Calificación		Nueva Evaluación	Opciones de manejo	Acción	Responsable	Indicador
	Probabilidad	Impacto			Probabilidad	Impacto					
Vulnerabilidad en la seguridad interna y externa de las TIC	5	4	Zona de riesgo extrema	Verificar que se hayan implementado los firewall, swit antivirus y back up internos y externos.	3	2	Zona de riesgo baja	Asumir el riesgo	Monitorear la implentación firewall, swit antivirus y back up internos y externos.	C.A Desarrollo Tecnológico	Informe Data Center y Red de Datos
Errores en Hardware y Software	3	4	Zona de riesgo extremo	Verificar el soporte y mantenimiento de las TIC	1	2	Zona de riesgo baja	Asumir el riesgo	Revisar los tiempos respuesta desde la mesa de ayuda Revisar que se haya realizado el soporte y mantenimiento de acuerdo al Plan de Mantenimiento	C.A Desarrollo Tecnológico	No. requerimientos solucionados/ total requerimientos

Fuente: Mapa de Riesgos Isolucion

Si bien los controles de seguridad informática que se encuentran implementados son necesarios y prestan un servicio a la organización, éstos corresponden fundamentalmente al área de infraestructura informática, y aunque funcionen correctamente su efectividad debe ser potencializada mediante la complementación con controles propios en los sistemas de información y el mejoramiento de la concienciación en seguridad informática de los funcionarios.

A parte de lo relativo a los controles de seguridad informática como tales, y según se indica en el memorando 037502-201600010741 dirigido por la C.A de Desarrollo Tecnológico a la Oficina de Control interno el 10 de junio de 2016; durante el mes de Marzo de mismo año se presentó la materialización de un incidente que afectó el funcionamiento de un dispositivo de almacenamiento masivo y que coincide con la descripción de uno de los riesgos identificados para el proceso de gestión de las TIC: “Mal funcionamiento de servidores o red” *(ver Cuadro 2)*, el cual, si bien no se originó en debilidades informáticas propiamente dichas, sino en la falta de oportunidad en la contratación de los servicios de administración y monitoreo, muestra una debilidad organizacional para gestionar este tipo de riesgos de forma integral.

Con respecto a la forma en que se definen y asignan los roles en la gestión de la seguridad informática, se analizó el Acuerdo 066 de 2012 del Concejo de Medellín

y la información aportada por el personal de la C.A de Desarrollo Tecnológico en reunión realizada el 10 de febrero de 2017, encontrándose lo siguiente:

El citado acuerdo, en su artículo 4 "*Objetivos de los órganos superiores de dirección y administración*", aunque establece los objetivos de la Contraloría Auxiliar de Desarrollo Tecnológico, no hace alusión la seguridad informática. No obstante en su artículo 11 "*Funciones requisitos y competencias laborales*", en la definición de las funciones el cargo "*Contralor Auxiliar*" para la unidad de gestión "*Contraloría Auxiliar de Desarrollo Tecnológico*", en el numeral 4 de la sección "*Descripción de funciones esenciales*" indica: "*4. Adoptar medidas de seguridad orientadas a mantener la integridad de los recurso informáticos* ", lo cual aunque es importante, no cubre las otras propiedades de la información de cuya protección se encarga al seguridad informática: disponibilidad y confidencialidad.

Adicionalmente, se encontró que el mismo artículo 11 del citado acuerdo, indica entre las funciones los profesionales universitarios Grado 02P: "*4. Establecer mecanismos que permitan controlar la seguridad del hardware y el software, los procedimientos y estándares para la utilización de los equipos y el respaldo de las aplicaciones.*", lo cual si bien puede asociarse a una tarea relacionada con la seguridad de informática, no indica una asignación precisa para gestionar riesgos pues no se cita una responsabilidad en proteger la integridad, disponibilidad y confidencialidad la información procesada a través de los sistemas de información de la institución.

No obstante, durante la reunión realizada el 10 de febrero de 2016, se encontró también que pese a la ausencia de asignación normativa de roles, los funcionario de la C.A tienen un nivel alto de concienciación con respecto a la seguridad informática, y propenden por la implementación de los controles estándares de la industria en la materia, como se puede evidenciar en la implementación, y control de soluciones como el sistema de control de tráfico de datos (Firewall), el plan de contingencia de tecnología informática, los mecanismos para la gestión de copias de seguridad y control de virus informáticos.

Con respecto a la evaluación de la forma en que se entrena el personal en seguridad informática, no se encontró evidencia de la existencia de un plan de capacitación de los funcionarios de la C.A de Desarrollo Tecnológico en la materia.

En general, la gestión de la seguridad informática en la organización, aunque cuenta con una buena implementación de controles, no se evidencia un nivel de madurez que lleve a la operación efectiva de un ciclo de mejora continua que gestione de forma integral los riesgos según el espíritu de la familia de estándares ISO 27000. No obstante es importante anotar que la existencia de controles constituye una importante base de mejora, a partir de la cual podría establecerse

un proceso formal de gestión de riesgos en seguridad informática inspirado en los estándares internacionales correspondientes.

7.4 ASPECTOS TRANSVERSALES

Dado que la gestión de las TIC posee aspectos que son transversales a los asuntos cuya evaluación se ha presentado en los numerales anteriores, se hace importante abordarlos de una forma más específica. El aspecto más relevante evaluado corresponde a la documentación del proceso de administración de las TIC que existe en la organización, para lo cual se analizó el Procedimiento P-GI-I-001 Administración y Mantenimiento de las TIC dispuesto en la la plataforma Isolucion, encontrándose lo siguiente.

Al comparar el Procedimiento P-GI-I-001 con la documentación para la gestión de TIC que aportan las buenas prácticas internacionales como ITIL y COBIT, se encuentra que éstas incluyen la descripción de múltiples procesos, actividades y funciones, lo difiere de la forma sucinta en la que se expresan las actividades en el procedimiento con que cuenta la Contraloría (ver Figura 1 y Figura2), el cual si bien cubre todas las etapas de la vida de una solución de TIC, no posee en algunos componentes un alto nivel de detalle alto, lo que podría dificultar el control, seguimiento y medición de la gestión de TIC como tal, y en última instancia desfavorecer la eficacia y la eficiencia del mismo.

Figura 1:Esquema de actividades y procesos de ITIL V3

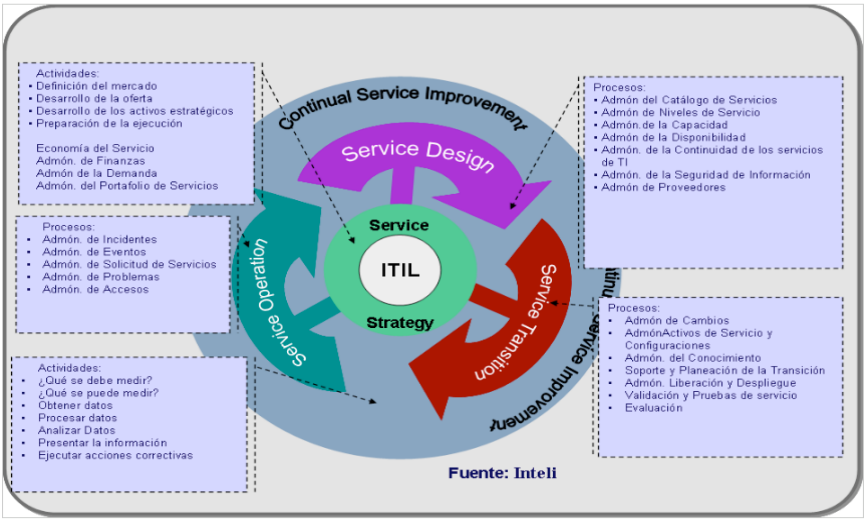

Imagen tomada de: https://sg.com.mx/buzz/las-diferencias-itil-v2-v3#.WK8gNfLSn2U

Figura 2: esquema de procesos en Cobit 5.

Imagen tomada de: Guía de procesos catalizadores de Cobit 5.

7.5 ASPECTOS POSITIVOS

Durante el desarrollo de la Auditoría se encontraron múltiples aspectos positivos en la gestión de las tecnologías de la información y las comunicaciones en la organización, algunos de los más significativos se presentan a continuación:

- **Aspecto Positivo 1**: Durante el análisis de la forma en que se controlan los proyectos de TIC, se encontró que el control del proyecto de automatización de flujos de trabajo en Mercurio, si bien se realizó por fuera de la vigencia analizada en esta auditoría, fue ejercido utilizando una metodología estructurada y enfocada a lograr la calidad de los entregables.

- **Aspecto Positivo 2**: En la organización se hace uso de ambientes de prueba y producción para los sistemas Mercurio y Gestión Transparente a fin de probar

los cambios en un ambiente de laboratorio antes de aplicarlos en los ambientes de producción, lo cual ayuda controlar los riesgos asociados a la aplicación de cambios que no han sido debidamente probados.

- **Aspecto Positivo 3:** En la organización se cuenta con un acuerdo de nivel de servicio definido para el servicio de soporte sobre el sistema Mercurio, lo cual ayuda a regular una relación sana y productiva con el contratista.

- **Aspecto Positivo 4**: En la organización se lleva un registro de las incidencias reportadas para el sistema Mercurio a través de su sitio Web Mesa de Ayuda, lo cual aporta en la generación de insumos para la toma de decisiones con respecto al servicio de soporte de dicho sistema. Además se encontró que en 2017 se está haciendo de dichos datos para elaborar material instructivo a fin de educar mejor a los usuarios y atacar la causa de las incidencias más frecuentes.

- **Aspecto Positivo 5**: En la organización se cuenta con una metodología documentada de gestión de riesgos que se aplica en el caso de los riesgos de seguridad informática, lo cual constituye la piedra angular de cualquier proceso de gestión del riesgo en seguridad informática o seguridad de la información que la organización desee formalizar.

- **Aspecto Positivo 6**: La organización cuenta con controles de acceso a los expedientes alojados en el sistema Mercurio, los cuales no pudieron ser burlados mediantes las pruebas de seguridad que realizó la Oficina de Control Interno.

7.6 OBSERVACIONES

Observación 1

Se observó que la operación del sistema de información Gestión Transparente en 2016 no incluyó el claro establecimiento de un mecanismo de atención de incidentes para todos sus usuarios objetivo que tuviera como fin brindar una atención oportuna, tanto a los funcionarios de los sujetos de control como a los funcionarios de la Contraloría General de Medellín, lo que desfavorece el proceso de adopción de esta nueva herramienta, ya que no todos sus usuarios se informan claramente sobre los canales a través de los cuales pueden reportar sus consultas, inquietudes y dificultades, ni tampoco los tiempo de respuesta que pueden esperar una vez realizados los reportes, por lo que podrían preferir hacer

uso de las herramientas y mecanismos antiguos que ellos ya conocen y con los que se sienten más cómodos.

En la situación descrita no se aplica la esencia del proceso COBIT DSS02 "*Gestionar Peticiones e Incidentes de Servicio*", cuyo propósito es: *"Lograr **una mayor productividad** y minimizar las interrupciones mediante la rápida resolución de consultas de usuario e incidentes*", ni tampoco se aplica la esencia del proceso de gestión de incidentes según ITIL, cuyo propósito es: "*Manejar el ciclo de vida de todos los Incidentes con el fin de devolver el servicio de TI a los usuarios lo antes posible*."

Evidencia de lo anterior se puede encontrar en el acta de reunión 02 de la auditoría a la gestión de la tecnología de la información 2016.

Observación 2

Se observó que los sistemas Gestión Transparente y Mercurio pueden ser vulnerables a algunos riesgos de seguridad informática específicos, los cuales si bien fueron identificados y valorados, aún no se encuentran completamente controlados. En el caso más notorio la situación se da por una deficiencia en el abordaje integral de la seguridad de la información como un asunto que es responsabilidad toda la institución, y no únicamente responsabilidad de la C.A de Desarrollo Tecnológico. La existencia de las vulnerabilidades encontradas trae como consecuencia una degradación de la propiedad de confiabilidad y validez de la información ya que se demuestra que existen formas en que una persona no autorizada puede acceder o modificar información alojada en los sistemas Gestión Transparente y Mercurio.

La situación anterior se aparta de lo establecido en el **artículo 19 de la ley 594 del 2000**:

"***ARTÍCULO 19**. Soporte documental. Las entidades del Estado podrán incorporar tecnologías de avanzada en la administración y conservación de sus archivos, empleando cualquier medio técnico, electrónico, informático, óptico o telemático, siempre y cuando cumplan con los siguientes requisitos:*

> *a) Organización archivística de los documentos;*
>
> *b) Realización de estudios técnicos para la adecuada decisión, teniendo en cuenta aspectos como la conservación física, las condiciones ambientales y operacionales, la seguridad, perdurabilidad y reproducción de la información contenida en estos soportes, así como el funcionamiento razonable del sistema.*

PARÁGRAFO 1º. Los documentos reproducidos por los citados medios gozarán de la validez y eficacia del documento original, siempre que se cumplan los requisitos exigidos por la leyes procesales y se garantice la autenticidad, integridad e inalterabilidad de la información" subrayado propio

Adicionalmente, la adecuada gestión de las vulnerabilidades encontradas toma relevancia según lo prescrito en el **artículo 2 de la Ley 87 de 1993,** en donde se establece como uno de los objetivos del sistema de control interno:

"e) Asegurar la oportunidad y confiabilidad de la información y de sus registros;"

De otro lado, en lo relativo a los documentos gestionados a través de los sistemas Gestión Transparente y Mercurio que contiene datos personales, como es el caso de los nombres completos y los número de identificación de empleados y/o contratistas, la situación descrita se aparta de la aplicación del principio de seguridad, establecido el artículo **4 literal g de la Ley 1581 de 2012**, que reza:

"*g) **Principio de seguridad**: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; "*

A parte de lo anterior, y desde un punto de vista técnico, la situación descrita se parta de los controles de seguridad sugeridos por la norma NTC 27002, en especial en lo referido al control 10.1.1 *"Política de uso de los controles criptográficos: Se debería desarrollar e implementar una política que regule el uso de controles criptográficos para la protección de la información*", al control "*7.2.2 Concienciación, educación y capacitación en Seguridad de la Información: Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo*."

7.7 RECOMENDACIONES

Recomendación 1	
Descripción	Elementos relacionados
Analizar las formas de aprovechar el mecanismo existente de gestión de incidentes y potencializarlo mediante la adopción de las mejores prácticas en la materia, como el proceso de gestión de incidentes y problemas de ITIL, a modo de fomentar la mejora continua del mismo y el aumento recurrente de su eficiencia y eficacia.	Aspecto Positivo 4

Recomendación 2	
Descripción	Elementos relacionados
Analizar el establecimiento de un servicio de atención de incidentes para el sistema Gestión Transparente que ofrezca a todos los usuarios: horarios de atención, subservicios y tiempos de respuesta claros, de modo que se facilite el uso de dicho sistema por parte de su público objetivo.	Observación 1

Recomendación 3	
Descripción	Elementos relacionados
Analizar las formas de mejorar la aplicación de la política de administración de riesgo D-GE-PL-002 en lo relativo a la seguridad informática, de forma que se logre una mayor profundidad y cubrimiento en el	Observación 2

proceso de gestión de riesgos de seguridad informática y seguridad de la información en general. Se recomienda además tener en cuenta, como parte del análisis, la asignación de roles y capacitación en seguridad informática para los funcionarios.	

Recomendación 4	
Descripción	Elementos relacionados
Analizar los procesos propuestos en las buenas prácticas internacionales para la gestión de TIC, como ITIL y Cobit, para cuáles de ellos generarían beneficios al ser implementados en la organización y establecer una prioridad de adopción.	Observación 1 Observación 2

GLOSARIO DE TÉRMINOS

- ITIL V3: Es un marco de mejores prácticas que se ha elaborado por los sectores público y privado a nivel internacional. En él se describe cómo los recursos de TI deben ser organizados para ofrecer un valor empresarial documentando los procesos, funciones y roles en la administración de servicios de tecnología informática.

- COBIT 5: **COBIT** (Control Objectives for Information and related Technology) es el marco aceptado internacionalmente como una buena práctica para el control de la información, Gestión de tecnología Informática -IT- y los riesgos que conllevan. **COBIT** se utiliza para implementar el gobierno de IT y mejorar los controles de IT.

- Ambiente o entorno de pruebas: Es el conjunto de una aplicación de software y sus elementos asociados, que se usan con el fin de realizar ensayos y pruebas sin comprometer los sistemas que están siendo usado directamente por los funcionarios de la entidad.

- Ambiente o entorno de producción: Es el conjunto de una aplicación de software y sus elementos asociados, que se usan directamente por los funcionarios de la entidad en su diario quehacer.

- Acuerdo de nivel de servicio o ANS: (en inglés Service Level Agreement o SLA), es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. El ANS es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc.

- Cifrar: codificar el contenido de un mensaje de acuerdo con una clave a fin de proteger su contenido, de manera que sólo pueda leerlo quien cuente con la clave adecuada para decodificarlo.