Auditoría Interna

AL PROCESO DE GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC'S) EN LA:

Presentado por: Rubiel Navarro Ch.
rubiel.navarro@hotmail.com

Medellín, julio de 2019

Control del Documento

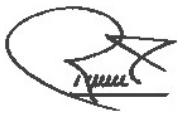
INFORMACIÓN DEL DOCUMENTO

Identificación del Doc.:	RNC-Informe Final Auditoria
Dueño del Documento:	Ing. Rubiel Navarro Ch.
Fecha de Actualización:	22 de julio 2019
Nombre del Archivo:	RNC-Informe Final de Auditoria Contrato 046-2019 vF

HISTORIA DEL DOCUMENTO

Fecha	Versión	Realizado por	Revisado por	Comentario a las modificaciones
22/07/2019	1.0	Equipo del Proyecto		Documento Final

APROBACIÓN DEL DOCUMENTO

Rol/Nombre	Firma	Fecha (dd/mm/aaaa)
Supervisor del Contrato – Lotería de Medellín Luz Adriana Jaramillo		22/07/2019
Contratista Rubiel Navarro Ch.		22/07/2019

Contenido

Introducción

La Auditoría de las Tecnologías de Información es una actividad de control que comprende la evaluación de las Tecnologías de Información y las comunicaciones (TIC), así como de la Seguridad de la Información (SI), dentro de una organización. Está basada en buenas prácticas y normas nacionales e internacionales, que son utilizadas para revisar y calificar el diseño, desempeño y cumplimiento de los controles implementados en el ambiente de TI.

Permite contar con una evaluación objetiva e independiente respecto a los procesos, servicios, aplicaciones, infraestructura e información, identificando los principales riesgos de negocio relacionados con TI, resultado de posibles debilidades de control.

Beneficios de la Auditoría de TIC's

- Verificar que los servicios TIC's se encuentran al nivel que la organización necesita para habilitar, potenciar y soportar de manera efectiva y eficiente sus funciones sustantivas.
- Determinar si el ambiente de control en TI, cumple con las regulaciones y requerimientos normativos.
- Contar con las recomendaciones necesarias para mitigar posibles riesgos que pongan en peligro a los activos de información y a la continuidad del negocio.

Propósito de la Auditoría de TIC's

El propósito de la auditoría es promover el aprovechamiento en el uso de las Tecnologías de Información y las comunicaciones, constatando que se lleven a cabo las mejores prácticas y se siguen los procedimientos que aseguran la veracidad, confidencialidad, confiabilidad y disponibilidad de la información, garantizando de esta manera la prevención ante posibles contingencias que puedan impedir la continuidad del uso de los recursos informáticos.

Realizar las actividades correspondientes a la verificación de los controles internos establecidos en la Oficina de TIC's, así como el estudio de la seguridad, el análisis de los riesgos a que está expuesta la información, la infraestructura de hardware, software y comunicaciones.

1. Objetivos

El presente informe tiene como propósito, presentar a la Lotería de Medellín, los resultados de la verificación que, a través de procedimientos, registros, comunicaciones, revisión documental, entrevistas e inspección ocular, evidencia el cumplimiento y la efectividad del proceso de gestión de tecnología de la información y las comunicaciones (TIC'S) en la consecución de los objetivos de la entidad, produciendo recomendaciones para la búsqueda del mejoramiento de la gestión como soporte corporativo.

2. Alcance

El alcance de la auditoría fue valuar el proceso, riesgos y controles para la Gestión de Tecnología de la Información y las Comunicaciones (TIC's), y en detalle lo relacionado con la gestión de soluciones y sistemas de información, gestión de la seguridad de la información, administración de infraestructura, administración de las comunicaciones, entre otros subprocesos, conforme al Plan Estratégico de Tecnologías de la Información (PETI) vigente para la Lotería de Medellín.

El presente informe se presenta a la Lotería de Medellín, de conformidad con las obligaciones consignadas en el Contrato 046 de 2019:

a) Verificar que los servicios TIC's se encuentran al nivel que la organización necesita para habilitar, potenciar y soportar de manera efectiva y eficiente sus funciones sustantivas.

b) Determinar si el ambiente de control en TI, cumple con las regulaciones y requerimientos normativos.

c) Contar con las recomendaciones necesarias para mitigar posibles riesgos que pongan en peligro a los activos de información y a la continuidad del negocio.

d) Determinar los recursos tecnológicos de la **Lotería de Medellín** y la estructura organizacional de ésta y del área de TIC's.

e) Evaluar la importancia del sistema de información para los procesos de negocio objeto de la auditoria y el soporte que los recursos tecnológicos dan a éstos.

f) Conocer de manera global la gestión sobre el cual se llevará a cabo la auditoria, identificando los elementos que apoyan la seguridad y administración y conocimiento detallado de los servicios de información.

g) Solicitar información al área de informática y validación de la misma.

h) Estudiar y evaluar el control interno en las áreas de tecnologías de información de la Lotería de Medellín.

i) Solicitar información del contenido tecnológico mediante instrumentos de recopilación como son: cuestionarios, entrevistas, inspección.

j) Coordinar con las demás áreas de la **Lotería de Medellín** con el fin de conocer información del tipo informática que éstas hayan considerado en sus procedimientos de revisión.

k) Solicitar Bases de datos de los sistemas a revisar.

l) Revisar y actualizar de ser necesario los procesos definidos y/o pendientes y actualmente en operación con el acompañamiento del personal de Planeación.

m) Coordinar con Auditoría Interna el desarrollo de procedimientos técnicas e inspecciones de auditoría de tecnologías de información.

2.1 Área Auditada

Oficina de Tecnologías de la Información y las Comunicaciones de la Lotería de Medellín.

2.2 Temporalidad de la Auditoria

Fecha de la auditoría: 22/05/2019 al 22/07/2019

2.3 Lugar de la Auditoría

Oficina TIC's en la sede principal de la Lotería de Medellín

2.4 Criterios de la Auditoría

2.4.1 Contrato 046 de 2019

Prestación de servicios profesionales para realizar la Auditoría Interna al proceso de Gestión de Tecnología de la Información y las comunicaciones TIC.

2.5 Documentación Objeto de Revisión

- Documentación estratégica corporativa
- Plan Estratégico de Tecnologías de la Información vigente.
- Documentación de Procesos y Procedimientos de la Entidad.
- Manual de funciones
- Documentación de proyectos y ejecución los mismos.
- Estructura organizacional de la entidad y de la oficina de informática
- Documentación de riesgos y controles para la gestión de información
- Proyecto de la Seguridad Integral
- Información de servicios contratados y proveedores de los mismos
- Documentación de procesos ITIL (estrategia, diseño, transición, operación y mejora continua de servicios), si existen y si están implementados o en proceso de implementación.
- Último Plan de Mejoramiento realizado, conforme a los hallazgos, con la respuesta de los mismos según la última auditoría.
- Indicadores de gestión para TIC's
- Catálogo de servicios TIC's, sistemas de información, bases de datos y demás activos
- Documentación técnica y de usuario de los sistemas de información.
- Relación de documentación técnica de elementos tecnológicos
- Contratos de soporte y mantenimiento, licenciamiento de hardware y software

3. Metodología

La labor de revisión y verificación de que trató la auditoría en cuestión se efectuó con base en las siguientes fases metodológicas:

a) Fase Planeación

1 Inspección: comprensión de la organización, procesos de negocio y sistemas, así como los controles en el proceso de negocio

2 Análisis de Requerimientos: organización y verificación de la información obtenida con el fin de identificar estados y comportamientos, así como comparaciones con referencias establecidas de acuerdo a las buenas prácticas.

b) Fase Ejecución

1 Diseño y ejecución de pruebas: definición y ejecución de pruebas de cumplimiento para los controles clave de la gestión.

2 Visitas: asistencia presencial a las instalaciones de la Lotería de Medellín, principalmente a la Oficina de Tecnología de Información y Comunicaciones TIC's.

3 Observación: verificación de la gestión que realiza la Oficina de Tecnología de Información y Comunicaciones TIC's.

4 Revisión analítica: evaluación de los resultados de la ejecución de las pruebas y revisiones de auditoría.

5 Seguimiento de mejoras: verificación de los planes de mejoramiento ejecutados por la Oficina TIC's y en general por la Lotería de Medellín, en atención a las observaciones y recomendaciones de las anteriores auditorías.

c) Fase Entregables

1 Informes: elaboración de informes con los resultados de la auditoría.

4. Avance en este Informe

De acuerdo con el avance de las actividades de auditoría y el desarrollo del presente informe, el porcentaje de ejecución es de **100%**, como se muestra en la siguiente ilustración:

Auditoría Interna al Proceso de Gestión de Tecnología de la Información y las Comunicaciones (TIC's) en la Lotería de Medellín

	ACTIVIDAD	Mayo 2019			Junio 2019				jul-19		
		20-24		27-31	4-7	10-14	17-21	25-28	2-5	8-12	15-19
1	**Inicio del Contrato**										
	• Firma de contrato y acta de inicio										
	• Reunión de apertura										
	• Reunión preliminar con Oficina TIC's										
	• Plan de auditoría y cronograma de ejecución										
2	**Investigación preliminar:**										
	• Revisión de información y de documentos										
	• Conocimiento global de la entidad										
	• Conocimiento del sistema operacional y del sistema de información y todos sus componentes										
	• Documentación										
3	**Planeación de la Auditoría:**										
	• Análisis de información de contenido tecnológico (entrevistas, cuestionarios, inspección etc.)										
	• Análisis de información en otras áreas de la Lotería (entrevistas, cuestionarios, inspección etc.)										
	• Análisis de escenarios y grupos de riesgo										
	• Documentación										
4	**Ejecución de la auditoría:**										
	• Desarrollo de procedimientos										
	• Formulación de posibles observaciones y/o recomendaciones										
	• Comunicación de posibles observaciones y/o recomendaciones										
	• Archivo de papeles de trabajo										
	• Cierre de auditoría										
5	**Elaboración y entrega de informe de resultados**										
6	**Socialización de resultados**										

5. Informe del Resultado de la Auditoría

Como parte del desarrollo de cada fase, se realiza evaluación de los resultados obtenidos, y con base en esto se emite el informe final respectivo. A continuación un resumen ejecutivo de las debilidades de control interno identificadas y que están descritas en el informe detallado del resultado de la auditoría (numeral 5.4).

5.1 Aspectos destacables

En la etapa de ejecución de la auditoria se identificaron diversos aspectos que pueden dejarse de mencionar:

- La actitud positiva y disponibilidad de los auditados, así como la entrega oportuna de la documentación requerida por el auditor.

- La excelente disposición y la actitud inmejorable que mostraron cuando se les solicitó a los funcionarios de la Oficina de TIC's y a su Director, la colaboración para indagar acerca de la gestión de servicios de tecnología y las labores que desarrollan.
- Profesionalismo y compromiso evidente en todos los funcionarios de la Oficina de TIC's.
- Dedicación permanente a las labores encomendadas.
- Se destaca la estructura organizacional implementada y la infraestructura tecnológica que está en proceso de mejoramiento para seguir soportando la operación de la Lotería.

5.2 Síntesis del Resultado

A continuación se presenta una síntesis de las observaciones y/o recomendaciones que resultaron del proceso de auditoría realizado:

E2.	Realizar un análisis y evaluación del área de TIC, con el fin de obtener una definición clara de las funciones, líderes del proceso y la responsabilidad de las diferentes personas que conforman la Oficina de Tecnología de Información y Comunicaciones.
El personal no tiene un conocimiento pleno de las funciones esenciales consignadas para cada persona en el correspondiente cargo que está definido en el "*Manual Específico de Funciones y Competencias Laborales*", y algunos funcionarios (agentes de mesa de ayuda y soporte) dudan al identificar el área a la cual pertenecen.	
Observación (requiere acción de mejora)	N/A
Recomendación (opcional: acción de mejora)	• Incentivar en los funcionarios de la Oficina de Tecnologías de Información y Comunicaciones un conocimiento pleno de las funciones consignadas para cada uno en el "*Manual Específico de Funciones y Competencias Laborales*". • Motivar a todos los funcionarios para que conozcan con suficiencia la estructura del área de TIC's (misión, visión, principios y valores, organigrama y las áreas internas).

F1.	Conocer la información requerida por otras áreas de la Oficina de TIC's.
1. Falta de oportunidad en la respuesta a una solicitud que Réditos Empresariales hizo a la Lotería el 31 de enero de 2018 y que después de múltiples dificultades la Oficina de TIC's dio respuesta después de 16 meses, el 22 de mayo de 2019. 2. Solicitud de capacitación para la reparación de los dispositivos Spectra T-1000, que a la fecha aún no tiene respuesta de la Oficina de TIC's.	
Observación (requiere acción de mejora)	• Dar respuesta a la solicitud de capacitación para la reparación de los dispositivos Spectra T-1000. • Generar un plan de mejoramiento que conduzca a garantizar una respuesta oportuna a todas las solicitudes que las demás áreas de la Lotería le hagan la Oficina de TIC's. • Definir ANS's (acuerdos de niveles de servicio) para toda la gama de

	solicitudes
Recomendación (opcional: acción de mejora)	N/A

H1.	Revisar los procesos definidos y en operación.
Existen documentados en el PLAN DE SEGURIDAD YPRIVACIDAD DE LA INFORMACIÓN tres (3) procesos definidos y descritos: 1. Gestión de soluciones TIC's 2. Gestión de servicios de soporte 3. Administración de la infraestructura y seguridad de la información Estos procesos, aunque contienen la definición y la descripción necesarias, deberían tener una caracterización más amplia y más formal en concordancia con los lineamientos del Modelo Integrado de Planeación y Gestión (Plan de Acción Integral de la Lotería) y teniendo en cuenta las buenas prácticas del Modelo de gestión estratégica de TI que se recomienda en las instituciones del estado.	
Observación (requiere acción de mejora)	• Hacer una caracterización más detallada de los procesos mencionados.
Recomendación (opcional: acción de mejora)	N/A

I1.	Determinar que el ambiente de control de TI esté alineado con la estrategia de gestión.
Se hizo la revisión de la definición y contenido del "*Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI*" incluido en "*Plan de Acción Integral de la Lotería de Medellín*". El PETI está definido para el período 2016-2019 e incluye la planeación estratégica de gestión de TI, gobierno de TI, políticas de TI en cuanto a seguridad, información, acceso y uso, etc., portafolio de servicios, gestión financiera y plan de continuidad de TI.	
Observación (requiere acción de mejora)	N/A
Recomendación (opcional: acción de mejora)	• Proveer evidencia del mecanismo de aprobación del PETI por la alta gerencia de la Lotería. • Definir el "Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI" para el periodo 2020-2023 teniendo en cuenta el Marco de Referencia de Arquitectura Empresarial para la gestión de TI en el país, el cual debe ser liderado conjuntamente por la alta dirección de la Lotería y la Dirección de Tecnologías de la Información y las comunicaciones. • Para ello, se sugiere utilizar el esquema (o marco de trabajo) de Arquitectura Empresarial TOGAF que proporciona un enfoque para el diseño, planificación, implementación y gobierno de una arquitectura empresarial de información.

I2.	Determinar que el ambiente de control de TI esté alineado con el gobierno de TI.
Se hizo la revisión de la definición del gobierno de TI en el "*Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI*", el cual contiene la estructura organizacional de TI, la definición de procesos y el modelo de operación. Sin embargo, para que las TIC's cumplan su papel es necesario contar con un modelo de gobierno de TI que contemple los siguientes aspectos:Marco legal y normativo, Estructura de TI y procesos (ya definidos), Toma de decisiones, Gestión de relaciones con otras áreas y	

entidades, Gestión de proveedores, Acuerdos de servicios y de desarrollos, Alineación con los procesos.	
Observación (requiere acción de mejora)	N/A
Recomendación (opcional: acción de mejora)	Aplicar el modelo **COBIT**, estándar internacional para los temas de **Gobierno de TI**, e **ITIL** para la gestión de proveedores y la gestión de niveles de servicio. El modelo **COBIT** define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro "dominios" principales: Planificación y organización; Adquisición e implantación; Soporte y servicios; y, Monitoreo. Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. Estos dominios y objetivos de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

I3.	Determinar que el ambiente de control de TI esté alineado con la gestión de información y los sistemas de información.
Durante las entrevistas a las ingenieras del área de negocio y aplicaciones empresariales, se evidencia que se están desarrollando adecuaciones para hacer que las aplicaciones sean cada vez más operativas y útiles en el manejo de información y provean funciones ajustadas a las necesidades de la organización. Sin embargo, se han identificado algunos sistemas, como CYGNUS, que están desarrollados con herramientas muy antiguas y que requieren una renovación completa. Para lo cual la Oficina de TIC's ha venido estructurando proyectos de renovación de nuevas soluciones.	
Observación (requiere acción de mejora)	N/A
Recomendación (opcional: acción de mejora)	Tener en cuenta que MINTIC proporciona el "*Esquema para contratar proyectos de desarrollo de sistemas de información*" y las "*Mejores prácticas para la transformación de las entidades del Estado en el desarrollo de sistemas de información*", con el propósito de facilitarle a las entidades estatales la implementación de planes de re-ingeniería, desarrollo o compra de sistemas de información. Ver el siguiente link: https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6799.html

I4.	Determinar que el ambiente de control de TI esté alineado con la administración de la seguridad.
Se hizo la revisión del "*Plan de Seguridad y Privacidad de la Información*", ubicado en el portal web corporativo, en donde se define que la Lotería de Medellín, a través de la Dirección de Tecnologías de la Información y la Comunicación, impulsa la implementación del Modelo de Seguridad y Privacidad de la Información MSPI, basándose en el modelo PHVA, sin embargo, no se tuvo evidencia de la existencia de la definición de este modelo que debe estar acorde con las buenas prácticas de seguridad, incluyendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública. También se revisó el documento "*MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION.pdf*", que tiene un contenido acorde con lo requerido, pero que está desactualizado, pues su revisión y la aprobación fue en diciembre de 2016. De la misma manera, se evidenció que el contenido del documento "*Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información*" ubicado en el portal web de la Lotería (https://www.loteriademedellin.com.co/gestion-y-control/informes-de-gestion) no tiene el contenido correspondiente con el título de este documento y no trata los riesgos de seguridad y privacidad de la información. Por tal motivo, no fue posible revisar el "*Plan de tratamiento de riesgos de seguridad*".	
Observación (requiere acción de mejora)	• Realizar la definición e implementación del Modelo de Seguridad y Privacidad de la Información. • Actualizar y someter a aprobación el documento "*MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION.pdf*" • Proveer para revisión el "*Plan de tratamiento de riesgos de seguridad*". • Tener en cuenta la norma ISO 17799:2005 que establece los diez (10) dominios de control que cubren por completo la Gestión de la Seguridad de la Información.
Recomendación (opcional: acción de mejora)	• Utilizar el "*Instrumento de Evaluación MSPI*", herramienta del Ministerio de Tecnologías de la Información y las Comunicaciones de uso libre sin fines lucrativos, creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea (hoy Gobierno Digital) en su cuarto componente "*Seguridad y Privacidad de la Información*". • Generar el documento de Continuidad de Negocio y el Análisis de Impacto de Negocio (BIA).

J1.	Determinar que el ambiente de control de TI esté alineado con los servicios tecnológicos (administración y operación de infraestructura tecnológica y de sistemas de información).
Se realizaron en dos (2) oportunidades, sendas inspecciones al centro de cómputo, se realizó una entrevista con el administrador de la plataforma tecnológica, Ing. Camilo Aristizábal, y se utilizó un cuestionario de revisión de servicios e infraestructura del área de TIC's. Como resultados de estas acciones se evidencia que el centro de cómputo principal, tiene las características tecnológicas apropiadas para soportar la operación de la Lotería, no obstante, se identifican algunas características que requieren revisión.	

Observación (requiere acción de mejora)	• Adiestrar al personal en el uso de extintores. • Crear mecanismos de divulgación para que los usuarios de las otras áreas conozcan las políticas y los procedimientos para el ingreso y la permanencia en el centro de cómputo, y las normas de seguridad. • Implementar controles regulares para verificar la efectividad de las políticas de seguridad.
Recomendación (opcional: acción de mejora)	• Implementar completamente la gestión de cambios de **ITIL**. • Iniciar la implementación de **ITIL** en la gestión de niveles de servicio, seguridad, disponibilidad, capacidad, continuidad de servicios y gestión de problemas.

J2.	Determinar que el ambiente de control de TI esté alineado con los servicios tecnológicos (Servicios de soporte técnico y mesa de ayuda).
Se evidencia que los casos de soporte interno no se registran al 100%, debido a la premura del servicio, a la urgencia del mismo o la actitud de colaboración que muestran los funcionarios de soporte.	
Observación (requiere acción de mejora)	• Crear el mecanismo y propender por la disciplina en el registro de la totalidad de los casos de soporte interno.
Recomendación (opcional: acción de mejora)	• Iniciar la implementación de ITIL en la gestión de eventos, incidencias, solicitudes o requerimientos, service desk.

K1.	Verificación de la definición y tratamiento de los riesgos.
Se hizo la revisión de la definición de los riesgos incluidos en el "*Plan de Seguridad y Privacidad de la Información*" y la documentación y tratamiento, para determinar su completitud. Haciendo un análisis exhaustivo, se sugiere incluir en la caracterización y tratamiento, algunos riesgos.	
Observación (requiere acción de mejora)	N/A
Recomendación (opcional: acción de mejora)	• Se recomienda evaluar la lista de riesgos sugerida, encontrar otros aún no identificados e incluirlos en el análisis y la caracterización.

M1.	Verificar la gestión interna que realiza el área de TIC's para gestionar todas las iniciativas y proyectos de TI.
Con base en la información recolectada en las entrevistas con los funcionarios de la Oficina de TIC's que lideran proyectos y supervisan la ejecución de proyectos de los diversos proveedores, se identifica que no se apoyan en las buenas prácticas de gestión de proyectos y no tienen el conocimiento detallado de las condiciones contractuales y las obligaciones que debe cumplir cada contratista o proveedor.	
Observación (requiere acción de mejora)	• La Oficina de TIC's debe propender por la gestión de todas las iniciativas y proyectos de TI, utilizando una metodología formal de gestión de proyectos y de seguimiento a la ejecución de los mismos, utilizando mecanismos apropiados.
Recomendación (opcional: acción de mejora)	• Utilizar las buenas prácticas de gestión de proyectos como PMI o Scrum, según aplique al tipo de proyecto que se esté administrando o supervisando.

5.3 Seguimiento a Observaciones en Auditorías Anteriores

Se relacionan a continuación los planes de mejoramiento que surgieron como resultado de las auditorías realizada en noviembre de 2016 y al final del año 2017. Se describe la observación, la información de seguimiento suministrada por el Director de la Oficina de TIC's y el estado de la correspondiente observación:

PLAN DE MEJORAMIENTO POR AUDITORÍA DE NOVIEMBRE 2016

OBSERVACIÓN	**1. PLANEACIÓN ESTRATÉGICA DE TECNOLOGÍA E INFORMACIÓN** La Dirección de Informática no cuenta con un Plan Estratégico Corporativo de Tecnología e Informática (PETI) que muestre la ruta que oriente el camino de la Entidad en un periodo determinado. **Acción de mejora**: BENEDAN deberá implementar un Plan estratégico Corporativo de Tecnologías de la Información (PETI) con el fin de direccionar la entidad a mejores prácticas con estrategias de innovación y desarrollo tecnológico como respuesta a la competitividad y logro de los objetivos Corporativos.	√
SEGUIMIENTO	Se desarrolló. Es el documento que funciona como hoja de ruta para la planeación y seguimiento de los proyectos del Área de TIC's.	

OBSERVACIÓN	**2. POLÍTICAS DE SEGURIDAD** No se tiene aprobadas las políticas de seguridad de la información, se cuenta con un primer borrador el cual consideramos que está bien concebido, en cuanto al propósito legal y de cumplimiento. Dentro del documento no se encontró la inclusión de la Responsabilidad Demostrada, el cual es una exigencia de la Superintendencia de Industria y Comercio (SIC). **Acción de mejora**: BENEDAN debería establecer una política de seguridad de la información basado en la estrategia Corporativa con el fin de generar directrices empresariales en torno a la gestión de la información con sus componentes estratégicos, de gestión, legal y procedimental.	√
SEGUIMIENTO	Se desarrollaron los documentos de políticas de seguridad de información y de tratamiento de datos personales.	

OBSERVACIÓN	**3. SEGURIDAD DE LOS RECURSOS HUMANOS** Se cuenta con un formato de entrega del cargo llamado *lista de chequeo de paz y salvo y devolutivos para el retiro del cargo*, en el cual la Dirección de Informática debe verificar todo lo pertinente a la parte informática y firma el cumplimiento de la entrega. **Acción de mejora**: Es importante que la coordinación de gestión humana incluya este formato en el Sistema de Gestión de la Calidad y sea socializado al interior de la entidad.	√

SEGUIMIENTO	Se elaboró y se integró al SIGC	

OBSERVACIÓN	**4. GOBIERNO EN LÍNEA** En cuanto a la implementación de Gobierno en línea no son muy significativos los avances, se debe definir un comité de Gobierno el Línea, donde se deben definir las actividades, responsables, metas y recursos presupuestales, a fin de satisfacer oportunamente mediante los servicios y/o productos del GIT de TIC's, las necesidades y requerimientos de los grupos internos de trabajo de la Entidad en cuanto a las tecnologías disponibles, enmarcando los elementos de Sistemas de Información, Comunicaciones y Servicios Tecnológicos (Infraestructura TI). **Acción de mejora**: Es importante que la alta Dirección conforme un comité de Gobierno en Línea donde se dejan claramente las funciones y responsabilidades. Con el fin de cumplir con la estrategia de gobierno en línea.	√
SEGUIMIENTO	Comité de Gobierno en línea formalmente establecido y Plan de Acción elaborado. Actualmente, existe el decreto, pero se debe retomar su implementación (Funcionario de TIC encargado: Gloria Pérez).	

OBSERVACIÓN	**5. SEGURIDAD FÍSICA Y DEL ENTORNO** Se evidencia que no existe un adecuado control de los equipos de cómputo, de tal forma que se evite un riesgo de pérdida o daño. **Acción de mejora**: Es importante que la Dirección Financiera y administrativa en conjunto con la Dirección de Informática implementen una metodología para llevar el control e inventario de los equipos de cómputo, con el fin de contar en tiempo real con inventario actualizado y las condiciones técnicas de los equipos.	√
SEGUIMIENTO	Documento de inventario consolidado.	

OBSERVACIÓN	**6. CONTROL DE ACCESO** Se implementó por parte de la entidad un sistema biométrico para el acceso de los funcionarios y visitantes. Se encontró que no se reporta a la Dirección de informática las novedades en cuanto al personal. No se hace un control efectivo de las tarjetas de acceso a la compañía, ya que cuando se hace un retiro de un empleado, no se hace la descarga de datos del retiro en el sistema, solo se hace el cambio del nombre y la foto. Se cuenta con una directriz para el acceso al templo de los millones la cual se viene cumpliendo. **Acción de mejora**: La Dirección de Informática debe brindar capacitación sobre los accesos a la Dirección Financiera y Administrativa con el fin de mantener la seguridad en la entidad y para efectos de bloqueo de accesos y el manejo integral de información. Se debe implementar una política para el control de acceso a las áreas de. (Almacén, Tesorería, Data Center etc.)	**Por Verificar**

SEGUIMIENTO		

OBSERVACIÓN	**7. DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN** No existe una responsabilidad específica del circuito cerrado de televisión en lo que tiene que ver con la capacidad de almacenamiento, copia de seguridad, manuales de funcionamiento, revisión y monitoreo de las grabaciones, mantenimiento de cámaras, capacitación etc. Que permita elaborar un informe periódico para dirección de la compañía. **Acción de mejora**: Es importante que se responsabilice a un funcionario de la Dirección Financiera y Administrativa sobre la administración y manejo de las cámaras de seguridad. La Dirección de Informática debe brindar una capacitación al Funcionario que se designe por parte de la dirección Financiera y Administrativa para la administración y manejo de las cámaras de seguridad.	Por Verificar
SEGUIMIENTO		

OBSERVACIÓN	**8. ADMINISTRACIÓN DE INCIDENTES** Una vez revisado los casos MABE, se puede determinar que aún continúan casos abiertos con más de un mes de solicitado. En el sistema los casos MABE, se evidencio que a la fecha existen 22 casos que fueron asignados y aún continúan abiertos. **Acción de mejora**: La Dirección de Informática debe realizar un mayor control a los casos que aún continúan abiertos y brindar capacitación a todo el personal para el manejo de la Herramienta. Se debe realizar una revisión a los niveles de servicios con el fin de determinar los tiempos de atención.	En ejecución
SEGUIMIENTO	Se han efectuado acciones para disminuir el número de casos asignados aún abiertos, sin embargo se siguen presentando aunque con menor frecuencia. No se ha definido ANS que permitan mitigar esta situación.	

OBSERVACIÓN	**9. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO** La Dirección de informática cuenta con un Plan de Continuidad del negocio desde el punto de vista informático, es necesario que este plan sea articulado con el plan de continuidad de la entidad. **Acción de mejora**: Se debe diseñar un solo Plan de Continuidad del Negocio de Benedan (hoy Lotería de Medellín), para garantizar el cumplimiento de los objetivos prioritarios del negocio en caso de contingencia. Seguridad y confianza a las partes interesadas, Identificar amenazas y vulnerabilidades sobre las operaciones críticas de la compañía, para su tratamiento y control de manera proactiva, Integrar la estandarización, innovación y el liderazgo en la gestión del riesgo operativo.	Por Verificar

SEGUIMIENTO	Documento del Plan de continuidad de negocio y documento soporte de los simulacros realizados. **OBSERVACIÓN DE LA PRESENTE AUDITORÍA**: Estos documentos no se encuentran dentro de la documentación recibida.	

OBSERVACIÓN	**10. SEGURIDAD FÍSICA EN INSTALACIONES** No se encontraron los manuales de las UPS nuevas. Los sistema de alimentación interrumpida (UPS) no son monitoreadas para verificar su correcto funcionamiento, ya que si sucede algún evento se debe hacer uso de la garantía del proveedor. **Acción de mejora**: Se debe contar con los manuales de las UPS y designar un funcionario que permanentemente realice monitoreo a las UPS.	√
SEGUIMIENTO	Se instalaron dos (2) circuitos de UPS y se generó el documento soporte del mantenimiento preventivo sobre los componentes UPS.	

OBSERVACIÓN	**11. PROTECCIÓN DE DATOS** La entidad debe darle aplicación al Decreto No. 1377 de 2013, en su artículo 23 "*Medios para el ejercicio de los derechos. Todo Responsable y Encargado deberá designar a una persona o área que asuma la Función de protección de datos personales, que dará tramite a las solicitudes de los titulares para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el presente Decreto*".. **Acción de mejora**: Se debe realizar una Resolución donde esta función esté en cabeza de alguna de las Direcciones de Informática o Comercial.	**En ejecución**
SEGUIMIENTO	Están definidas las políticas; pendiente la resolución para iniciar publicación de las políticas. Se debe tratar el tema de normatividad de protección de datos en Comité de Gerencia.	

PLAN DE MEJORAMIENTO POR AUDITORÍA DE 2017

OBSERVACIÓN	**1. MAPA DE RIESGOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES** Se cuenta con el mapa de riesgos del Proceso, en el Sistema de Gestión de la Calidad, el cual no se encuentra actualizado a la fecha de la auditoria. En la revisión realizada al mapa de riesgos se encuentra que no existe monitoreo periódico al comportamiento de los mismos, ya que como se puede determinar en el análisis no es visto como una herramienta de control para mitigar los riesgos en el cumplimiento de los objetivos trazados en el proceso. • Acceso o uso indebido de Internet • Desviación en los resultados de auditorias • No implementación de la acciones correctivas • Fallas en el funcionamiento de los equipos • Perdida de información • Acceso inapropiado al entorno de programas e información • Uso inadecuado de derechos de autor • Daños físicos de los equipos. **Acción de mejora**: Actualizar el mapa de riesgos.	√
SEGUIMIENTO	Se actualiza el mapa y se incorpora al Sistema de Gestión de la Calidad. A la fecha (julio de 2019) no se han actualizado **OBSERVACIÓN DE LA PRESENTE AUDITORÍA**: La matriz y el mapa de riesgos se deben actualizar periódicamente y no esperar que ocurran otros eventos para hacerlo.	

OBSERVACIÓN	**2. PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN** Una vez revisado el PETI, se encuentra que no está aprobado por la alta dirección y no se le ha realizado seguimiento al cumplimiento de las acciones allí planteadas. De acuerdo con el decreto 415 del 7 de marzo del 2016 en su artículo 2.2.35.3, como objetivos del fortalecimiento institucional la entidad deben liderar la gestión estratégica a través del PETI. Desde el 6 de marzo fue enviado por la Oficina de Tecnologías de la información el PETI, para los aportes de cada una de las direcciones y a la fecha no ha sido posible el documento definitivo. Los Objetivos planteados en el PETI son difíciles de medir y en la planeación los objetivos deben ser medibles y que se puedan alcanzar. En cuanto a los indicadores hace falta indicadores de infraestructura, aplicativos, información, servicios de TI y recurso humano. Se deben definir las estrategias e iniciativas en tecnología y Procesos basado en los estándares internacionales para tecnologías de la Información, con el fin de generar valor en la entidad. **Acción de mejora**: • Realizar los ajustes al plan de acuerdo a las recomendaciones. • Volver a presentar a la alta gerencia el PETI para su aprobación.	√
SEGUIMIENTO	Según información de la matriz de seguimiento, se hicieron los ajustes y se aprobó el PETI. **OBSERVACIÓN DE LA PRESENTE AUDITORÍA**: proveer la evidencia de la aprobación del PETI.	

OBSERVACIÓN	**3. INDICADORES DE GESTIÓN** La oficina de tecnologías de la información cuenta con tres indicadores así: • % Cumplimiento del cronograma proyectos TI. • % Disponibilidad servicios comerciales. • Efectividad a la atención a solicitudes de soporte. **Acción de mejora**: Se deben revisar los indicadores del sistema de gestión de la Calidad y actualizarlos con el fin de determinar si es necesario el cambio o diseño de otros indicadores que apunten al Plan Estratégico de Informática, para que permitan una toma de decisiones oportunas.	√
SEGUIMIENTO	Según información del Director de la Oficina de TIC's, los indicadores se actualizaron pero falta que la Oficina de Planeación los integre en el Sistema de Calidad.	

OBSERVACIÓN	**4. PLAN DE CONTINUIDAD DEL NEGOCIO** En la revisión realizada se encuentra que la Oficina de Tecnologías de la Información cuenta con un Plan de Continuidad de Negocio para el área. **Acción de mejora**: Conciliar con el almacén el inventario que se tiene registrado en la dirección de Informática versus el inventario que se lleva en almacén, una vez consolidado se enviara un informe a la dirección de control Interno. Para que este complementado con la competencia desde la dirección de cada área involucrada en el proceso.	√
SEGUIMIENTO	Según información del Director de la Oficina de TIC's, el plan de continuidad de TIC's está definido, se debe actualizar con la nueva infraestructura tecnología y gestionar la aprobación de la Alta Dirección. **OBSERVACIÓN DE LA PRESENTE AUDITORÍA**: proveer la evidencia de la aprobación del Plan de Continuidad.	

OBSERVACIÓN	**5. CASOS MABE** Una vez revisados los casos MABE se presenta el cuadro de los casos que aún continúan pendientes de darle solución. **Acción de mejora**: Se deben revisar los indicadores del sistema de gestión de la Calidad y actualizarlos con el fin de determinar si es necesario el cambio o diseño de otros indicadores que apunten al Plan Estratégico de Informática, para que permitan una toma de decisiones oportunas.	**En ejecución**
SEGUIMIENTO	Se deben implementar los controles e indicadores.	

OBSERVACIÓN	**6. SOFTWARE** Aplicativo "core" de negocio (CYGNUS), desarrollado en herramientas como VISUAL BASIC, donde no existe soporte por la casa matriz por más de 8 años, presenta una obsolescencia significativa. **Acción de mejora**: Realizar el proyecto de actualización del aplicativo que se ajuste a las necesidades actuales y futuras, de acuerdo con las necesidades planteadas por el área comercial, ajustado a una estrategia comercial y de mercadeo.	En ejecución
SEGUIMIENTO	Está en proceso de contratación el desarrollo externo de la nueva herramientas. La entidad reconoce como buena práctica contratar el desarrollo de software externamente y que la Lotería se dedique al negocio, dado que el desarrollo implica conocimiento específico, especialización, experiencia, aplicación de herramientas etc.	

OBSERVACIÓN	**7. GOBIERNO EN LÍNEA** En cuanto a la implementación de Gobierno en línea se creó el comité de Gobierno en Línea y se realizaron reuniones de seguimiento. A la fecha no se ha firmado la Resolución el esquema de publicación. Estrategia Gobierno en Línea- Transparencia y Acceso a la Información: Soportar tecnológicamente las necesidades de desarrollo surgidas en el proceso de implementación de la Estrategia Gel contenidas en el decreto 2693 de 2012 y ley 1712 de 2014. En las actas de reunión existen compromisos que a la fecha no se han logrado cumplir. **Acción de mejora**: Dar traslado al *Comité de Gobierno en Línea* para que lleve el plan de implementación de Gobierno en Línea (Gobierno Digital) de acuerdo a lo descrito en la norma.	En Ejecución
SEGUIMIENTO	Aún no se ha iniciado el proceso de implementación de Gobierno Digital- **OBSERVACIÓN DE LA PRESENTE AUDITORÍA**: iniciar el proceso de implementación, tan pronto se formalice la iniciativa por parte del Gobierno Nacional.	

OBSERVACIÓN	**8. SEGUIMIENTO AL PLAN ESTRATÉGICO** La Oficina de control Interno recomienda que se agilice el diseño del proyecto de informática para el empréstito con el fin de dar cumplimiento a las metas contempladas en el Plan estratégico. **Acción de mejora**: Adelantar el proceso del empréstito para que los proyectos apalancados por estos recursos puedan tener avances	En Ejecución
SEGUIMIENTO	Según información del Director de la Oficina de TIC's, los proyectos de modernización en etapa de aprobación y contratación. Los indicadores están desarrollándose en el tablero de control. **OBSERVACIÓN DE LA PRESENTE AUDITORÍA**: como se especifica en el detalle de la revisión de objetivos de control de TI, se recomienda utilizar buenas prácticas de gestión de proyectos como PMI o Scrum, según aplique al tipo de proyecto que se esté administrando o supervisando.	

OBSERVACIÓN	**9. RELACIÓN CON PROVEEDORES** Evidenciamos proveedores de desarrollo de software, custodia de medios, Telefonía, correo electrónico y otros más con los cuales BENEDAN no tiene establecido los acuerdos de niveles de servicios (ANS), acuerdos de Confidencialidad y/o acuerdos de transferencia de información claramente especificados con cada uno de ellos y de acuerdo al propósito de cada uno de los contratos. Solamente se tienen firmados con DITAR, CADENA y LOTTIRED. **Acción de mejora**: Desarrollar y firmar los acuerdos de nivel de servicio (ANS), acuerdos de confidencialidad y/o acuerdos de transferencia de información.	En Ejecución
SEGUIMIENTO	Los acuerdos de confidencialidad ya existen y los ANS para quienes apliquen. Los acuerdos de confidencialidad para desarrollo de software, deben extenderse para los proveedores de mantenimientos de BD.	

OBSERVACIÓN	**12. PROTECCIÓN DE DATOS** Se han hecho avances en la definición de la política de tratamiento de información beneficencia de Antioquia, la política general para el proceso de gestión del talento humano, el procedimientos para la revisión jurídica contractual y el protocolo para la recolección de datos personales, Se realizó el reporte de la Base de datos. **Acción de mejora**: Es importante que se socialice al interior de la entidad los avances y políticas sobre la protección de datos.	En ejecución
SEGUIMIENTO	Están definidas las políticas; pendiente la resolución para iniciar publicación de las políticas. Se debe tratar el tema de normatividad de protección de datos en Comité de Gerencia.	

5.4 Informe Detallado del Resultado de la Auditoría

El siguiente detalle consolida los resultados de las labores realizadas durante las tres (3) fases metodológicas, para dar cumplimiento a las obligaciones consignadas en el Contrato 046-2019. Para dar cumplimiento a cada una de estas obligaciones, en un orden metodológico adecuado de ejecución de actividades, se desarrollaron las siguientes actividades y acciones de verificación:

A.	**Coordinar con Auditoría Interna el desarrollo de procedimientos técnicas e inspecciones de auditoría de tecnologías de información.**

No.	**Descripción, pregunta o actividad**
A1.	Desarrollar y presentar el plan de auditoría y el cronograma de trabajo, de conformidad con lo especificado en el contrato.
Prueba realizada	
El plan de auditoría y el cronograma de ejecución fueron presentados de conformidad con lo establecido en el contrato 046 de 2019, y fue debidamente aprobado por la LOTERÍA DE MEDELLÍN.	
Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
NA	**SI**
Recomendación	
NA	
Resultado	
Es satisfactoria la evidencia suministrada.	

No.	**Descripción, pregunta o actividad**
A2.	Ejecutar la auditoría y elaborar los respectivos informes, de conformidad con el plan y el cronograma de trabajo definido.
Prueba realizada	
Se dio cumplimiento a la ejecución de la auditoría y elaboración de los respectivos informes (preliminar y final).	
Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
NA	**SI**
Recomendación	
NA	
Resultado	
Es satisfactoria la evidencia suministrada.	

No.	**Descripción, pregunta o actividad**

A3.	Coordinar en forma permanente con el supervisor del contrato, las reuniones que se requieran para verificar el avance, ejecución de actividades y entrega de informes y documentos propios de la ejecución de la auditoría.

Prueba realizada

Durante el periodo de ejecución del contrato, se realizaron reuniones de avance con el supervisor del contrato y con su apoyo se realizaron todas las actividades del plan de auditoría.

Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
N/A	**SI**

Recomendación

N/A

Resultado

Es satisfactoria la evidencia suministrada.

B.	**Solicitar información al área de informática y validación de la misma.**

No.	**Descripción, pregunta o actividad**
B1.	Formalizar la solicitud de documentación e información a la Lotería de Medellín, como insumo inicial para el desarrollo del trabajo de auditoría.

Prueba realizada

Para el inicio del trabajo de auditoría, se procedió en la reunión de apertura a solicitar la siguiente documentación:

- Documentación estratégica corporativa
- Plan Estratégico de Tecnologías de la Información vigente.
- Documentación de Procesos y Procedimientos de la Entidad.
- Manual de funciones
- Documentación de proyectos y ejecución los mismos.
- Estructura organizacional de la entidad y de la oficina de informática
- Documentación de riesgos y controles para la gestión de información
- Proyecto de la Seguridad Integral
- Información de servicios contratados y proveedores de los mismos
- Documentación de procesos ITIL (estrategia, diseño, transición, operación y mejora continua de servicios), si existen y si están implementados o en proceso de implementación.
- Último Plan de Mejoramiento realizado, conforme a los hallazgos, con la respuesta de los mismos según la última auditoría.
- Indicadores de gestión para TIC's
- Catálogo de servicios TIC's, sistemas de información, bases de datos y demás activos
- Documentación técnica y de usuario de los sistemas de información.

- Relación de documentación técnica de elementos tecnológicos.
- Contratos de soporte y mantenimiento, licenciamiento de hardware y software.

De la misma forma, se realizó una revisión de la documentación publicada en el sitio web https://www.loteriademedellin.com.co, específicamente los apartes *Quiénes Somos* y *Estructura Organizacional*.

Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
N/A	**SI**

Recomendación
N/A

Resultado
Se recibió por correo electrónico y mediante memoria USB, la documentación solicitada. La documentación suministrada por Auditoría Interna y la Oficina de TIC permite el cumplimiento satisfactorio a esta actividad.

C.	**Conocer de manera global la gestión sobre el cual se llevará a cabo la auditoria, identificando los elementos que apoyan la seguridad y administración y conocimiento detallado de los servicios de información.**

No.	**Descripción, pregunta o actividad**
C1.	Conocimiento general de la Lotería de Medellín, específicamente el Área de Tecnología de la Información y las Comunicaciones.

Prueba realizada
Para tal efecto, se hace una revisión detallada de la documentación recibida y se inicia el proceso conociendo el entorno de la empresa y del área de Tecnología de la Información y Comunicaciones, cuáles son los procesos sistematizados con los que la empresa cuenta, cuál es la organización del departamento de tecnología de información y comunicaciones, los planes estratégicos que se encuentren documentados de las TIC, los planes de operación, contingencia y/o continuidad de la empresa que se encuentren relacionados con el área de tecnología de la información.

Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
N/A	**SI**

Recomendación
N/A

Resultado
La documentación suministrada por Auditoría Interna y la Oficina de TIC, y la información publicada en el sitio web, fue suficiente para cumplir con el objetivo de la presente actividad.

D.	**Solicitar información del contenido tecnológico mediante instrumentos de recopilación como son: cuestionarios, entrevistas, inspección.**

No.	Descripción, pregunta o actividad
D1.	Realizar la recopilación de información mediante cuestionarios, entrevistas y mecanismos de inspección.

Prueba realizada	
En la ejecución de la auditoría se realizaron entrevistas con el Director y funcionarios de la Oficina TIC's, y con el Coordinador de Apuestas Permanentes de la Dirección de Operaciones, se les solicitó el diligenciamiento de cuestionarios a los funcionarios de la Oficina TIC's, y mediante la inspección y un instrumento de verificación escrita, se revisaron las características del centro de cómputo. Los cuestionarios diligenciados se adjuntan al final del presente informe en el Anexo 3.-Papeles de Trabajo Diligenciados.	
Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
N/A	**SI**
Recomendación	
N/A	
Resultado	
Las entrevistas realizadas, los cuestionarios diligenciados y las labores de inspección son evidencias satisfactorias del cumplimiento de esta actividad.	

E.	**Determinar los recursos tecnológicos de la Lotería de Medellín y la estructura organizacional de ésta y del área de TIC's.**

No.	Descripción, pregunta o actividad
E1.	Determinar los recursos tecnológicos de la Lotería de Medellín.

Prueba realizada	
Mediante la revisión del archivo **Inventario2019.xlsx** suministrado por el Director de la Oficina de TIC's y el cuestionario técnico de las características del centro de cómputo, se pudieron determinar los recursos tecnológicos de la Lotería de Medellín y las características del centro de cómputo.	
Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
N/A	**SI**
Recomendación	
N/A	
Resultado	
La evidencia suministrada es satisfactoria.	

No.	Descripción, pregunta o actividad
E2.	Realizar un análisis y evaluación del área de TIC, con el fin de obtener una definición clara de las

	funciones, líderes del proceso y la responsabilidad de las diferentes personas que conforman la Oficina de Tecnología de Información y Comunicaciones.

Prueba realizada

Mediante los mecanismos de recolección (entrevistas a los funcionarios de la Oficina de TIC's y los cuestionarios por ellos diligenciados), la revisión del organigrama, los acuerdos 11, 12, 13, 19, 20, 21y 25, la resolución 280, la planta de Cargos 2019, el "*Manual Específico de Funciones y Competencias Laborales*" publicados en el sitio web https://www.loteriademedellin.com.co, se obtuvo la definición clara de funciones, líderes de proceso y responsabilidades del personal del área TIC's.

Estas acciones permitieron conocer la Estructura Organizacional de la Oficina de TIC's, conformada esencialmente por tres (3) áreas:

- **Área de Negocio y Aplicaciones Empresariales**: que sirve de puente entre el personal técnico y el personal de negocio y el que se dedica a simular los procesos de negocio en las aplicaciones empresariales.
- **Área de Infraestructura y Telecomunicaciones**: encargada de garantizar la disponibilidad de los servicios, conectividad y seguridad de la información, además de diseñar e implementar los planes de recuperación ante desastres en caso de una eventualidad para mantener la operación.
- **Área de Gestión, Planificación, y estrategias de servicio**: encargada de diagnosticar, diseñar, implementar y evaluar los servicios que presta la dirección, optimizando la adaptación y asimilación de las nuevas tecnologías, y realizando el seguimiento y tratamiento a los riesgos identificados para los procesos de la dirección.

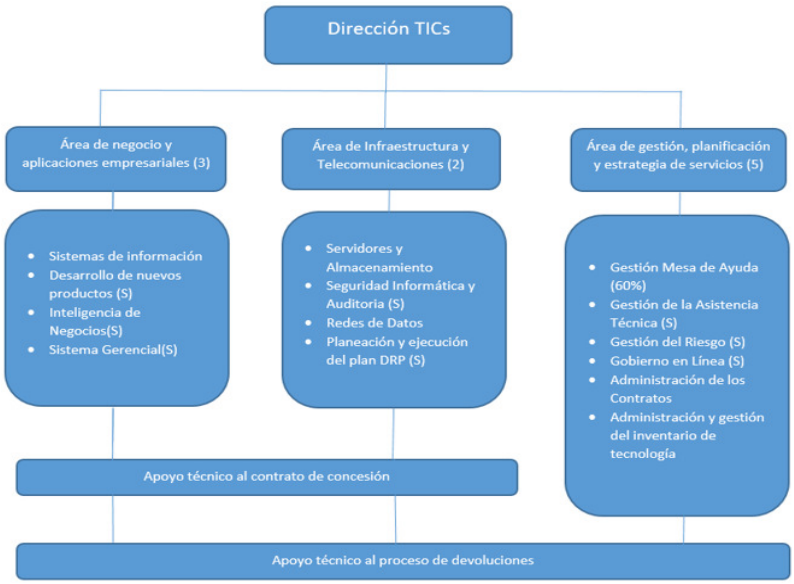


Ilustración 1-Descripciones e imagen tomada del archivo "Estructura Dirección TICs v2.docx", suministrado por el Director de la Oficina de TIC's

Esta actividad permitió establecer que el personal no tiene un conocimiento pleno de las funciones esenciales consignadas para cada persona en el correspondiente cargo que está definido en el "*Manual Específico de Funciones y Competencias Laborales*", y algunos funcionarios (agentes de mesa de ayuda y soporte) dudan al identificar el área a la cual pertenecen.

Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**

N/A	**SI**

Recomendación

- Incentivar en los funcionarios de la Oficina de Tecnologías de Información y Comunicaciones un conocimiento pleno de las funciones consignadas para cada uno en el "*Manual Específico de Funciones y Competencias Laborales*".
- Motivar a todos los funcionarios para que conozcan con suficiencia la estructura del área de TIC's (misión, visión, principios y valores, organigrama y las áreas internas).

Resultado

La evidencia suministrada, los cuestionarios diligenciados y las entrevistas realizadas son satisfactorias.

F.	**Coordinar con las demás áreas de la Lotería de Medellín con el fin de conocer información del tipo informática que éstas hayan considerado en sus procedimientos de revisión.**

No.	**Descripción, pregunta o actividad**
F1.	Conocer la información requerida por otras áreas de la Oficina de TIC's.

Prueba realizada

Se realizó una reunión con Orlando Marín, Coordinador de Apuestas Permanentes de la Dirección de Operaciones. En esta reunión se conocieron las siguientes observaciones:

3. Falta de oportunidad en la respuesta a una solicitud que Réditos Empresariales hizo a la Lotería el 31 de enero de 2018 y que después de múltiples dificultades la Oficina de TIC's dio respuesta después de 16 meses, el 22 de mayo de 2019.
4. Solicitud de capacitación para la reparación de los dispositivos Spectra T-1000, que a la fecha aún no tiene respuesta de la Oficina de TIC's.

Estas observaciones fueron comunicadas al Director de la Oficina de TIC's, quien manifestó que:

1. La primera solicitud se hizo antes de él ser contratado y el proceso de respuesta fue en verdad deficiente por múltiples circunstancias (pérdida de la solicitud, lentitud en el análisis y en la generación de la respuesta, entre otras).
2. A la segunda solicitud se le está dando respuesta en la actualidad.

Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
• Dar respuesta a la solicitud de capacitación para la reparación de los dispositivos Spectra T-1000. • Generar un plan de mejoramiento que conduzca a garantizar una respuesta oportuna a todas las solicitudes que las demás áreas de la Lotería le hagan la Oficina de TIC's • Definir ANS's (acuerdos de niveles de servicio) para toda la gama de solicitudes.	**NO**

Recomendación

N/A

Resultado

Las situaciones presentadas evidencian la necesidad de implementar un plan de mejoramiento que asegure respuestas oportunas bajo tiempos razonables, acordados por ANS's.

G.	**Solicitar Bases de datos de los sistemas a revisar.**

No.	Descripción, pregunta o actividad
G1.	Solicitar Bases de datos de los sistemas a revisar.

Prueba realizada

Mediante las entrevistas se indagó sobre las bases de datos para cada uno de los sistemas de información en funcionamiento en la Lotería de Medellín. Se identificó que las bases de datos están en Oracle 11g para los sistemas CYGNUS y Sistema Financiero SICOF, Oracle 12c para el Sistema Gerencial, MYSQL para el CRM.

Según comenta el ingeniero. Camilo Aristizábal, se está haciendo la migración de las bases de datos Oracle 11g a la versión 12c, siempre y cuando los aplicativos lo soporten.

Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
N/A	**SI**

Recomendación

N/A

Resultado

El motor de bases de datos Oracle es uno de los mejores del mercado y cumple técnicamente con lo que la Lotería de Medellín necesita en este sentido.

H.	**Revisar y actualizar de ser necesario los procesos definidos y/o pendientes y actualmente en operación con el acompañamiento del personal de Planeación.**

No.	Descripción, pregunta o actividad
H1.	Revisar los procesos definidos y en operación.

Prueba realizada

Conforme con la documentación analizada existen documentados en el PLAN DE SEGURIDAD YPRIVACIDAD DE LA INFORMACIÓN tres (3) procesos definidos y descritos:

4. Gestión de soluciones TIC's
5. Gestión de servicios de soporte
6. Administración de la infraestructura y seguridad de la información

Estos procesos, aunque contienen la definición y la descripción necesarias, deberían tener una caracterización más amplia y más formal en concordancia con los lineamientos del Modelo Integrado de Planeación y Gestión (Plan de Acción Integral de la Lotería) y teniendo en cuenta las buenas prácticas del Modelo de gestión estratégica de TI que se recomienda en las instituciones del estado.

Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
• Hacer una caracterización más detallada de los procesos mencionados.	**NO**

Recomendación
N/A
Resultado
La evidencia analizada de la definición y descripción de los procesos existe, pero se requiere completar.

I.	**Determinar si el ambiente de control en TI, cumple con las regulaciones y requerimientos normativos.**

En este ámbito se evalúa el ambiente de control de TI desde la perspectiva de la estrategia de gestión, el gobierno de TI, la gestión de información, los sistemas de información, la administración de la seguridad y los servicios tecnológicos (**ver Obligación J**).

No.	**Descripción, pregunta o actividad**
I1.	Determinar que el ambiente de control de TI esté alineado con la estrategia de gestión.
Prueba realizada	
Se hizo la revisión de la definición y contenido del "*Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI*" incluido en "*Plan de Acción Integral de la Lotería de Medellín*". El PETI está definido para el período 2016-2019 e incluye la planeación estratégica de gestión de TI, gobierno de TI, políticas de TI en cuanto a seguridad, información, acceso y uso, etc., portafolio de servicios, gestión financiera y plan de continuidad de TI.	
Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
N/A	**SI**
Recomendación	
• Proveer evidencia del mecanismo de aprobación del PETI por la alta gerencia de la Lotería. • Definir el "Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI" para el periodo 2020-2023 teniendo en cuenta el Marco de Referencia de Arquitectura Empresarial para la gestión de TI en el país, el cual debe ser liderado conjuntamente por la alta dirección de la Lotería y la Dirección de Tecnologías de la Información y las comunicaciones. • Para ello, se sugiere utilizar el esquema (o marco de trabajo) de Arquitectura Empresarial TOGAF que proporciona un enfoque para el diseño, planificación, implementación y gobierno de una arquitectura empresarial de información.	
Resultado	
La evidencia revisada y analizada es satisfactoria	

No.	**Descripción, pregunta o actividad**
I2.	Determinar que el ambiente de control de TI esté alineado con el gobierno de TI.
Prueba realizada	
Se hizo la revisión de la definición del gobierno de TI en el "*Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI*", el cual contiene la estructura organizacional de TI, la definición	

de procesos y el modelo de operación. Sin embargo, para que las TIC's cumplan su papel es necesario contar con un modelo de gobierno de TI que contemple los siguientes aspectos:

- Marco legal y normativo.
- Estructura de TI y procesos (ya definidos).
- Toma de decisiones.
- Gestión de relaciones con otras áreas y entidades.
- Gestión de proveedores.
- Acuerdos de servicios y de desarrollos.
- Alineación con los procesos.

Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
N/A	**SI**

Recomendación

Aplicar el modelo **COBIT**, estándar internacional para los temas de **Gobierno de TI**, e **ITIL** para la gestión de proveedores y la gestión de niveles de servicio.

El modelo **COBIT** define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro "dominios" principales:

1. **Planificación y organización**: cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio.
2. **Adquisición e implantación**: para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.
3. **Soporte y servicios**: hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.
4. **Monitoreo**: Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

   Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. Estos dominios y objetivos de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

Resultado

La evidencia analizada de la definición y descripción de los procesos es suficiente y satisfactoria, no obstante se recomienda aplicar las buenas prácticas de COBIT e ITIL para lo que corresponda.

No.	**Descripción, pregunta o actividad**

I3.	Determinar que el ambiente de control de TI esté alineado con la gestión de información y los sistemas de información.

Prueba realizada

Se hizo la revisión del "*Manual de Calidad 2018*", la certificación ISO 9001:2015, y el "*Plan de Seguridad y Privacidad de la Información*" y se tiene completamente definida la gestión de información cumpliendo con criterios como oportunidad, confiabilidad, completitud, pertinencia, privacidad y utilidad.

En el PETI, también están relacionados cada uno de los sistemas de información o soluciones de software que se utilizan en la Lotería de Medellín. Durante las entrevistas a las ingenieras del área de negocio y aplicaciones empresariales, se evidencia que se están desarrollando adecuaciones para hacer que las aplicaciones sean cada vez más operativas y útiles en el manejo de información y provean funciones ajustadas a las necesidades de la organización. Sin embargo, se han identificado algunos sistemas, como CYGNUS, que están desarrollados con herramientas muy antiguas y que requieren una renovación completa. Para lo cual la Oficina de TIC's ha venido estructurando proyectos de renovación de nuevas soluciones.

Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
N/A	**SI**

Recomendación

Tener en cuenta que MINTIC proporciona el "*Esquema para contratar proyectos de desarrollo de sistemas de información*" y las "*Mejores prácticas para la transformación de las entidades del Estado en el desarrollo de sistemas de información*", con el propósito de facilitarle a las entidades estatales la implementación de planes de re-ingeniería, desarrollo o compra de sistemas de información. Ver el siguiente link: https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6799.html

Resultado

La evidencia revisada y analizada es satisfactoria

No.	**Descripción, pregunta o actividad**
I4.	Determinar que el ambiente de control de TI esté alineado con la administración de la seguridad.

Prueba realizada

Se hizo la revisión del "*Plan de Seguridad y Privacidad de la Información*", ubicado en el portal web corporativo, en donde se define que la Lotería de Medellín, a través de la Dirección de Tecnologías de la Información y la Comunicación, impulsa la implementación del Modelo de Seguridad y Privacidad de la Información MSPI, basándose en el modelo PHVA, sin embargo, no se tuvo evidencia de la existencia de la definición de este modelo que debe estar acorde con las buenas prácticas de seguridad, incluyendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública.

También se revisó el documento "*MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION.pdf*", que tiene un contenido acorde con lo requerido, pero que está desactualizado, pues su revisión y la aprobación fue en diciembre de 2016.

De la misma manera, se evidenció que el contenido del documento "*Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información*" ubicado en el portal web de la Lotería

(https://www.loteriademedellin.com.co/gestion-y-control/informes-de-gestion) no tiene el contenido correspondiente con el título de este documento y no trata los riesgos de seguridad y privacidad de la información.

Por tal motivo, no fue posible revisar el "*Plan de tratamiento de riesgos de seguridad y Privacidad de la Información*".

Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
• Realizar la definición e implementación del Modelo de Seguridad y Privacidad de la Información. • Actualizar y someter a aprobación el documento "*MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION.pdf*" • Proveer para revisión el "*Plan de tratamiento de riesgos de seguridad*". • Tener en cuenta la norma ISO 17799:2005 que establece los diez (10) dominios de control que cubren por completo la Gestión de la Seguridad de la Información.	**NO**

Recomendación

- Utilizar el "*Instrumento de Evaluación MSPI*", herramienta del Ministerio de Tecnologías de la Información y las Comunicaciones de uso libre sin fines lucrativos, creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea (hoy Gobierno Digital) en su cuarto componente "*Seguridad y Privacidad de la Información*".
- Generar el documento de Continuidad de Negocio y el Análisis de Impacto de Negocio (BIA).

Resultado

La documentación suministrada y disponible para consulta NO evidencia el cumplimiento.

J.	**Verificar que los servicios TIC's se encuentran al nivel que la organización necesita para habilitar, potenciar y soportar de manera efectiva y eficiente sus funciones sustantivas.**

Según el fortalecimiento de la gestión TI en el estado, para disponer los sistemas de información es necesario desarrollar la estrategia de servicios tecnológicos que garantice su disponibilidad y operación. La gestión de tecnología debe proveer un servicio permanente que beneficie a todos los usuarios, tanto internos como externos. La gestión de los siguientes elementos garantiza la prestación de los servicios tecnológicos[1]:

- Suministro, administración y operación de infraestructura tecnológica y de sistemas de información.
- Alta disponibilidad para una operación continúa.
- Servicios de soporte técnico a los usuarios.
- Seguridad

La estrategia de servicios tecnológicos contempla el desarrollo de los siguientes aspectos:

- Arquitectura de infraestructura tecnológica
- Procesos de gestión: capacidad, puesta en producción y operación
- Servicios de conectividad
- Servicios de administración y operación
- Soporte técnico y mesa de ayuda
- Seguimiento e interventorías

No.	Descripción, pregunta o actividad
J1.	Determinar que el ambiente de control de TI esté alineado con los servicios tecnológicos (administración y operación de infraestructura tecnológica y de sistemas de información).

Prueba realizada

Se realizaron en dos (2) oportunidades, sendas inspecciones al centro de cómputo, se realizó una entrevista con el administrador de la plataforma tecnológica, ingeniero Camilo Aristizábal, y se utilizó un cuestionario de revisión de servicios e infraestructura del área de TIC's.

Como resultados de estas acciones se evidencia que el centro de cómputo principal, tiene las características tecnológicas apropiadas para soportar la operación de la lotería y satisfacer sus necesidades de gestión de información y de servicios tecnológicos; de manera similar las características tecnológicas del centro de cómputo alterno en INTERNEXA es suficiente para lo que hasta ahora se ha definido. Las principales características del mismo están verificadas en el cuestionario de revisión de servicios e infraestructura diligenciado.

No obstante, se identifican algunas características que requieren revisión:

- No existe una salida de emergencia.
- No se cuenta con equipo de suministro permanente de energía.
- Hay en el área un (1) solo extintor.
- No se ha adiestrado al personal en el uso de extintores.

[1]Tomando del sitio web de MINTIC (https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6800.html)

- No existen balanceadores.
- Los usuarios de las otras áreas no conocen las políticas y los procedimientos para el ingreso y la permanencia en el centro de cómputo.
- No hay mecanismos para la comunicación y divulgación de las normas de seguridad a los usuarios.
- No hay controles regulares para verificar la efectividad de las políticas.
- No se dispone (en la administración de activos y respaldo) de una clasificación de la información según la criticidad de la misma.
- No existen procesos para la gestión de la capacidad.
- Solo existe aplicación de las buenas prácticas ITIL (en un cierto grado) para gestión de portafolio de servicios y gestión de cambios.

Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
• Adiestrar al personal en el uso de extintores. • Crear mecanismos de divulgación para que los usuarios de las otras áreas conozcan las políticas y los procedimientos para el ingreso y la permanencia en el centro de cómputo, y las normas de seguridad. • Implementar controles regulares para verificar la efectividad de las políticas de seguridad.	**SI**

Recomendación

- Implementar completamente la gestión de cambios de **ITIL**.
- Iniciar la implementación de **ITIL** en la gestión de niveles de servicio, seguridad, disponibilidad, capacidad, continuidad de servicios y gestión de problemas.

Resultado

La información suministrada evidencia que la infraestructura tecnológica tiene las características mínimas suficientes para soportar las necesidades de información y soportar la operación de la Lotería de Medellín.

No.	Descripción, pregunta o actividad
J2.	Determinar que el ambiente de control de TI esté alineado con los servicios tecnológicos (Servicios de soporte técnico y mesa de ayuda).

Prueba realizada

Se realizaron entrevistas a los funcionarios de soporte y atención de mesa de ayuda. Se evidenció que el soporte y la atención de mesa de ayuda no solo se prestan a nivel interno dentro de las instalaciones de la Lotería y para los funcionarios de la misma, sino también a los distribuidores, vendedores y público en general.

Es importante destacar el profesionalismo y la buena actitud que muestran las personas encargadas de estas labores. Utilizan para ello el CRM y MABE (para casos de soporte interno).

Se evidencia que los casos de soporte interno no se registran al 100%, debido a la premura del servicio, a la urgencia del mismo o la actitud de colaboración que muestran los funcionarios de soporte.

Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
• Crear el mecanismo y propender por la disciplina en el registro de la totalidad de los casos de soporte interno.	**SI**

Recomendación

- Iniciar la implementación de **ITIL** en la gestión de eventos, incidencias, solicitudes o requerimientos, service desk.

Resultado

La información suministrada evidencia que los servicios de soporte técnico y mesa de ayuda se están desarrollando conforme a las necesidades de los usuarios internos y externos.

K.	**Contar con las recomendaciones necesarias para mitigar posibles riesgos que pongan en peligro a los activos de información y a la continuidad del negocio.**

No.	Descripción, pregunta o actividad
K1.	Verificación de la definición y tratamiento de los riesgos.

Prueba realizada

Se hizo la revisión de la definición de los riesgos incluidos en el "*Plan de Seguridad y Privacidad de la Información*" y la documentación y tratamiento, para determinar su completitud.

Se evidenció que la definición, caracterización y la documentación de su tratamiento está acorde con las buenas prácticas. Se identificaron los siguientes riesgos:

- R27: Daños físicos de los equipos.
- R28: Acceso inapropiado al entorno de programas e información.
- R29: Pérdida de información.
- R30: Acceso o uso indebido de Internet.
- R31: Fallas en el funcionamiento de los equipos.
- 65: Uso inadecuado de derechos de autor.

Haciendo un análisis exhaustivo, se sugiere incluir en la caracterización y tratamiento, los siguientes riesgos:

- Riesgo de insatisfacción de los usuarios.
- Riesgo de fallo o no disponibilidad de la plataforma tecnológica.
- Riesgo de fallo o no disponibilidad de la red de datos interna e Internet.
- Riesgo de fallo o no disponibilidad de los ambientes web de la entidad.
- Riesgo de ataques cibernéticos por deficiencias en el filtrado de correo electrónico.
- Riesgo de adoptar un enfoque tecnológico incompatible con las necesidades y misión de la entidad.
- Riesgo de imposibilidad de recuperación ante eventos o situaciones que afecten los servicios, por ausencia o desactualización del Plan de Continuidad del Negocio.
- Riesgo de imposibilidad de recuperación ante eventos o situaciones que afecten los servicios e infraestructura que informática soporta, por ausencia o desactualización del Plan de Contingencia.
- Riesgo de ataques cibernéticos por deficiencias en la detección y gestión de incidentes de seguridad.
- Riesgo de imposibilidad de recuperación ante pérdida de información misional sensible.
- Riesgo de no disponibilidad de los sistemas de información de la entidad por fallos o insuficiencia en los sistemas de almacenamiento.
- Riesgo de incumplir con los estándares de atención al ciudadano por no contar con la adecuación tecnológica necesaria.

Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
N/A	**SI**

Recomendación

- Se recomienda evaluar la lista de riesgos sugerida, encontrar otros aún no identificados e incluirlos en el análisis y la caracterización.

Resultado

La caracterización de riesgos evaluada es satisfactoria para el cumplimiento.

L.	**Evaluar la importancia del sistema de información para los procesos de negocio objeto de la auditoria y el soporte que los recursos tecnológicos dan a éstos.**

No.	**Descripción, pregunta o actividad**
L1.	Verificar el inventario de sistemas de información y las características técnicas de la infraestructura tecnológica que los soportan

Prueba realizada

Mediante las entrevistas a las tres (3) ingenieras del área de negocio y aplicaciones empresariales y al administrador de la plataforma tecnológica, se pudo constatar que los recursos tecnológicos son suficientes para soportar los sistemas existentes y en funcionamiento, las modificaciones que se realizan continuamente a los mismos y a los nuevos desarrollos que se vienen dentro del plan estratégico de TI (PETI).

Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**

N/A	**SI**
Recomendación	
N/A	
Resultado	
La evidencia analizada es satisfactoria.	

M.	**Estudiar y evaluar el control interno en el área de tecnologías de información en la Lotería de Medellín.**

No.	**Descripción, pregunta o actividad**
M1.	Verificar la gestión interna que realiza el área de TIC's para gestionar todas las iniciativas y proyectos de TI.

Prueba realizada

Con base en la información recolectada en las entrevistas con los funcionarios de la Oficina de TIC's que lideran proyectos y supervisan la ejecución de proyectos de los diversos proveedores, se identifica que no se apoyan en las buenas prácticas de gestión de proyectos y no tienen el conocimiento detallado de las condiciones contractuales y las obligaciones que debe cumplir cada contratista o proveedor.

Teniendo en cuenta que el Plan Estratégico de TI (PETI) define las estrategias de gobierno en cuanto a TI, sistemas de información y servicios tecnológicos, la Oficina de Tecnologías de la información y las Comunicaciones debe gestionar todas las iniciativas y proyectos de TI, utilizando una metodología formal de gestión de proyectos que incorpore el uso de lecciones aprendidas y un esquema de gestión de cambios, al igual que debe monitorear y hacer seguimiento a la ejecución de los proyectos de TI, por medio de un conjunto de indicadores de alcance, tiempo, costo y calidad que permitan identificar desviaciones y tomar las acciones correctivas pertinentes.

Se evidenció la existencia de cuadro en Excel en donde se registra el avance global de cada proyecto (que se actualizó para entregar a la presente auditoría), y se está procesando alimentación de los tableros de control del sistema gerencial. Sin embargo en la información recibida, estos cuadros no se habían actualizado recientemente.

Observaciones(Generar Plan de Mejoramiento)	**Cumplimiento**
• La Oficina de TIC's debe propender por la gestión de todas las iniciativas y proyectos de TI, utilizando una metodología formal de gestión de proyectos y de seguimiento a la ejecución de los mismos, utilizando mecanismos apropiados.	**Cumple parcialmente.**
Recomendación	
• Utilizar las buenas prácticas de gestión de proyectos como PMI o Scrum, según aplique al tipo de proyecto que se esté administrando o supervisando.	
Resultado	
La evidencia suministrada no es suficientemente satisfactoria.	

Anexo 1: ENTREVISTA A PERSONAL DEL ÁREA DE TIC's

Nombre:		Fecha: ___/___/_____

Cargo:	

¿En qué área desarrolla su trabajo?	○ Área de Negocio y aplicaciones empresariales ○ Área de infraestructura y telecomunicaciones ○ Área de gestión, planificación y estrategia de servicios ○ Otra. Especifique:_____

Funciones:	1.
	2.
	3.
	4.
	5.

¿Están estas funciones incluidas en el manual de funciones y competencias laborales?	○ SI	○ NO
¿Recibió y firmó las funciones de su cargo?	○ SI	○ NO

¿Recibió inducción al asumir su cargo?	○ SI	○ NO

¿Ha recibido capacitación en instituciones u organismos externos en temas relacionados con su cargo?	○ SI	○ NO
Si la respuesta es SI, menciones algunas de ellas:		
Si la respuesta es NO, ¿cuáles considera que serían importantes para su desarrollar mejor su trabajo?:		

¿A cuáles procesos pertenecen las actividades que desarrolla?	○ Gestión de soluciones TIC's ○ Seguridad de la información ○ CRM ○ Administración de la plataforma tecnológica ○ Otro. Especifique:_____
Describa las actividades que desarrolla, para cada proceso	Proceso: _____ Actividades: _____ _____ _____ _____
	Proceso: _____ Actividades: _____ _____ _____ _____
	Proceso: _____ Actividades: _____ _____ _____ _____

¿Desarrolla o gestiona proyectos como parte de su labor?	○ SI	○ NO

Mencione los proyectos y su rol en cada uno	1. Rol: _____
	2. Rol: _____
	3. Rol: _____

Mencione las metodologías que aplica en el desarrollo de su trabajo o que debe seguir de acuerdo con lo establecido en la Lotería. Sea lo más específico posible.	1.
	2.

¿Qué controles sigue para minimizar riesgos en el desarrollo de sus funciones?	1.
	2.
	3.
	4.

Mencione los registros documentales que guarda como evidencia del desarrollo de sus funciones (Entregue copia de esas evidencias al auditor)	1.
	2.
	3.
	4.
	5.
	6.
	7.
	8.
	9.
	10.

Observaciones Adicionales:

Firma Auditado

Firma Auditor

Anexo 2: REVISIÓN DE SERVICIOS E INFRAESTRUCTURA EN ÁREA DE TIC's

Responsable:		Fecha: ___/___/_____

Cargo:	

INSTALACIONES E INFRAESTRUCTURA

1. ¿El lugar donde se ubica el Centro de Cómputo está seguro de inundaciones, robo o cualquier otra situación que pueda poner en riesgo los equipos?	○ SI	○ NO
2. ¿El Centro de Cómputo da hacia el exterior?	○ SI	○ NO
3. ¿La construcción del Centro de Cómputo es confiable?	○ SI	○ NO
4. ¿Dentro del Centro de Cómputo existen materiales que puedan ser inflamables o causar daño a los equipos? Si la respuesta es SI, Cuáles: _____	○ SI	○ NO
5. ¿El lugar es suficientemente amplio para alojar los equipos?	○ SI	○ NO
6. ¿Además del Centro de Cómputo, existe otro lugar para almacenar otros equipos de cómputo, muebles, suministros etc.? Si la respuesta es SI, especifique: _____	○ SI	○ NO
7. ¿Se cuenta con una salida de emergencia?	○ SI	○ NO
8. ¿Existen señales que la hagan visible? ¿Dónde?: _____	○ SI	○ NO
9. ¿Es adecuada la iluminación del Centro de Cómputo?	○ SI	○ NO
10. ¿El color de las paredes es el adecuado?	○ SI	○ NO
11. ¿Existen lámparas dentro del Centro de Cómputo? ¿Cuántas?_____	○ SI	○ NO

12. ¿Qué tipo de lámparas utilizan? _____

13. ¿Cómo se encuentran distribuidas las lámparas dentro del Centro de Cómputo? _____		
14. ¿Es suficiente la iluminación del Centro de Cómputo? ¿Por qué?_____	○ SI	○ NO
15. ¿La temperatura a la que trabajan los equipos es la adecuada, de acuerdo con las normas? Especifique la norma: _____	○ SI	○ NO
16. ¿Están limpios los ductos del aire acondicionado?	○ SI	○ NO
17. ¿La ubicación del aire acondicionado es adecuada?	○ SI	○ NO
18. ¿Existe algún otro medio de ventilación, además del aire acondicionado? ¿Cuál?: _____	○ SI	○ NO
19. ¿El aire acondicionado emite algún tipo de ruido?	○ SI	○ NO
20. ¿Se cuenta con conexión a tierra?	○ SI	○ NO
21. ¿El cableado se encuentra correctamente instalado?	○ SI	○ NO
22. ¿Se pueden identificar cuáles son positivos, negativos y conexión a tierra?	○ SI	○ NO
23. ¿Las conexiones están debidamente identificadas?	○ SI	○ NO
24. ¿Se cuentan con los planos de instalación eléctrica?	○ SI	○ NO
25. ¿La instalación eléctrica es independiente de otras instalaciones?	○ SI	○ NO
26. ¿Se cuenta con sistema de regulación eléctrica?	○ SI	○ NO
27. ¿Se verifica la regulación de las cargas máximas y mínimas?	○ SI	○ NO
28. ¿Se cuenta con equipo de suministro permanente de energía?	○ SI	○ NO

29. ¿Se tiene en un lugar visible switch de apagado para casos de emergencia?	○ SI	○ NO
30. ¿Los cables están dentro de paneles y canales eléctricos?	○ SI	○ NO
31. ¿Los interruptores de energía están debidamente protegidos y sin obstáculos para alcanzarlos?	○ SI	○ NO
32. ¿Con qué frecuencia se les da mantenimiento a las instalaciones y suministro eléctricos? _____		
33. ¿Existen equipos para protección de información y dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores de picos, UPS, generadores de energía?	○ SI	○ NO
34. ¿Se encuentra con alarma contra incendios? ¿Dónde está ubicada?: _____	○ SI	○ NO
35. ¿Existen extintores? ¿Cuántos?: _____	○ SI	○ NO
36. ¿Qué tipo de mantenimiento se realiza? ¿Con qué frecuencia?: _____	○ PREVENTIVO	○ CORRECTIVO
37. ¿El personal sabe qué hacer en caso de emergencia?	○ SI	○ NO
38. ¿Se ha adiestrado al personal sobre el uso de extintores?	○ SI	○ NO
39. ¿El personal encargado de la infraestructura tiene el perfil adecuado para desempeñar las funciones correspondientes?	○ SI	○ NO

HARDWARE Y SOFTWARE

40. ¿Existen los componentes tecnológicos requeridos para soportar los procesos de información de la Lotería?		○ SI	○ NO
41. ¿Servidores?	○ SI	¿Cuántos?: _____	○ NO
42. ¿Balanceadores?	○ SI	¿Cuántos?: _____	○ NO
43. ¿Enrutadores?	○ SI	¿Cuántos?: _____	○ NO
44. ¿Bases de datos?	○ SI	¿Cuántas?: _____	○ NO

45. ¿Servidores de aplicaciones?	○ SI	¿Cuántos?: _____	○ NO
46. ¿Componentes para respaldo de información?	○ SI	¿Cuántos?: _____	○ NO
47. ¿Componentes de seguridad?	○ SI	¿Cuántos?: _____	○ NO

48. ¿Cuál es la disponibilidad del Centro de Cómputo?: _____%

CONTROL DE ACCESOS

49. ¿Se cuenta con algún tipo de control de entrada y salida de usuarios?	○ SI	○ NO
50. ¿Se registra el acceso al Centro de Cómputo de personas ajenas a la Oficina de TIC's?	○ SI	○ NO
51. ¿Existe una gestión de los password de usuarios?	○ SI	○ NO
52. ¿Existe una autenticación de usuarios en conexiones externas?	○ SI	○ NO

SEGURIDAD

53. ¿Existe una persona responsable de la seguridad y la autorización de acceso?	○ SI	○ NO
54. ¿Los usuarios de otras áreas conocen las políticas y los procedimientos para el ingreso y la permanencia en el Centro de Cómputo?	○ SI	○ NO
55. ¿Existe documento de políticas de seguridad?	○ SI	○ NO
56. ¿Hay un responsable de las políticas, normas y procedimientos?	○ SI	○ NO
57. ¿Existen mecanismos para la comunicación de las normas a los usuarios?	○ SI	○ NO
58. ¿Existen controles regulares para verificar la efectividad de las políticas?	○ SI	○ NO
59. ¿Existen programas de formación en seguridad para los empleados, clientes y terceros?	○ SI	○ NO
60. ¿Existe y está implementado un acuerdo de confidencialidad de la información?	○ SI	○ NO

61. ¿Existen controles contra software maligno?	○ SI	○ NO
62. ¿Se ha incorporado medidas de seguridad a la computación móvil?	○ SI	○ NO
63. ¿Están establecidos controles para realizar la gestión de los medios informáticos (cintas, discos, removibles, informes impresos)?	○ SI	○ NO

ADMINISTRACIÓN DE ACTIVOS Y RESPALDO

64. ¿Existe un inventario de activos actualizado?	○ SI	○ NO
65. ¿El Inventario contiene activos de datos, software, equipos y servicios?	○ SI	○ NO
66. ¿Se dispone de una clasificación de la información según la criticidad de la misma?	○ SI	○ NO
67. ¿Existe un responsable de los activos?	○ SI	○ NO
68. ¿Se disponen de mecanismos de respaldo de información en cintas (tapes) u otros mecanismos con la capacidad suficiente para garantizar la recuperación de la información?	○ SI	○ NO
69. ¿La custodia de los dispositivos de almacenamiento de respaldo se hace a través de un externo que ofrezca dicho servicio en condiciones técnicas acordes con las normas archivísticas nacionales, en una ubicación física diferente?	○ SI	○ NO
70. ¿Están implementadas las pruebas de recuperación de información (backups) desde los medios de almacenamiento de respaldo?	○ SI	○ NO

ADMINISTRACIÓN DE INCIDENTES

71. ¿Se comunican los eventos de seguridad?	○ SI	○ NO
72. ¿Se comunican las debilidades de seguridad?	○ SI	○ NO
73. ¿Están definidas las responsabilidades ante un incidente?	○ SI	○ NO

GESTIÓN DE PROCESOS DE NEGOCIO

74. ¿Existen procesos para la gestión de la capacidad?	○ SI	○ NO

75. ¿Existe un plan de emergencia de acuerdo al plan de continuidad del negocio?	○ SI	○ NO

76. ¿Existe un DRP?	○ SI	○ NO

77. ¿Están implementadas los procesos y funciones ITIL?	○ SI	○ NO

Estrategia del Servicio

- ○ Gestión del portafolio de servicios
- ○ Gestión financiera de TI
- ○ Gestión de relaciones de negocio

Diseño del Servicio

- ○ Coordinación del diseño
- ○ Gestión de niveles del servicio
- ○ Gestión del catálogo de servicios
- ○ Gestión de proveedores
- ○ Gestión de la seguridad
- ○ Gestión de la disponibilidad
- ○ Gestión de la capacidad
- ○ Gestión de la continuidad de servicios

Transición del Servicio

- ○ Planificación de la transición y soporte
- ○ Gestión de la configuración y de activos del servicio
- ○ Gestión de cambios
- ○ Gestión de liberación e implementación
- ○ Gestión de conocimiento

Operación del Servicio

Procesos:

- ○ Gestión de eventos
- ○ Gestión de incidencias
- ○ Gestión de solicitudes
- ○ Gestión de problemas
- ○ Gestión de accesos

Funciones

- ○ Service Desk
- ○ Gestión técnica
- ○ Gestión de aplicaciones
- ○ Gestión de operaciones

Mejora continua del Servicio

- ○ Informes de servicio
- ○ Medición del servicio

Observaciones Adicionales:

Firma Auditado

Firma Auditor

Anexo 3: Papeles de Trabajo Diligenciados

***** Fin del Documento *****