Medellin, 19 de octubre de 2023.

Lotería Medellín
Fecha de Indexación: 19/10/2023 15:16
Folios: 1
Radicado: 2023001193

Doctora
CLAUDIA PATRICIA WILCHES MESA
Gerente
Lotería de Medellín

ASUNTO: Informe definitivo de Auditoría al Proceso de Proceso de Gestión Tecnología de Información y las Comunicaciones – TIC de la Lotería de Medellín.

Respetada Gerente,

La Dirección de Auditoría Interna con fundamento en la Ley 87 de 1993, practicó Auditoría de seguimiento al Proceso de Gestión Tecnología de Información y las Comunicaciones – TIC de la Lotería de Medellín, por medio del contrato No.074 del 22 de agosto de 2023, suscrito con el Doctor Oscar Darío Marín Rivera.

La auditoría se llevó a cabo de acuerdo con las normas de auditoría y según el Artículo 17 del Decreto 648 del 19 de abril del 2017, el cual reza *"Las Unidades u Oficinas de Control Interno o quien haga* sus *veces desarrollarán su labor a través de los siguientes roles: liderazgo estratégico; enfoque hacia la prevención, evaluación de la gestión del riesgo, evaluación y seguimiento, y relación con entes externos de control"*. En cumplimiento del plan de auditorías de esta oficina, me permito remitir informe definitivo de auditoría realizada al Proceso de Gestión Tecnología de Información y las Comunicaciones – TIC, el cual contiene las situaciones encontradas y las recomendaciones efectuadas para mejorar la gestión y generar controles al proceso.

Es importante anotar que el informe preliminar fue remitido al Director de TICS por medio de correo electrónico el día 11 de octubre de 2023, para que si lo consideraban pertinente, realizaran las observaciones a que hubiera lugar. Se envío el informe final el día 19 de octubre de 2023. Quedando pendiente por suscribir el respectivo plan de mejoramiento para los hallazgos detectados.

Quedamos atentos a sus comentarios.

Atentamente,

DIEGO ALONSO BOTERO ALVAREZ
Director Auditoría Interna .

Medellín, 12 de octubre de 2023

Fecha de Indexación: 18/10/2023 17:03
Folios: 1
Radicado: 2023001018

Señores

LOTERÍA DE MEDELLÍN

Dr. DIEGO BOTERO ÁLVAREZ
Dirección de Auditoría Interna
Medellín

Asunto: Entrega del informe definitivo de auditoría interna al proceso TIC

Con base en el plan y cronograma de auditoría interna el proceso de gestión TIC radicado el 25 de agosto de 202, tengo el agrado de presentar el informe resultante de la actividad programada de auditoría interna al proceso gestión TIC.

Este informe se realiza de acuerdo con las fechas estipuladas en el contrato 074-2023_0001 del 2023.

Atentamente;

Oscar Darío Marín Rivera
CC. 71630964
Auditor TICS

	INFORME DE AUDITORIA INTERNA Componente de Seguridad y Ciber Seguridad de la información	

FECHA DE LA AUDITORIA: octubre 12 de 2023

Objetivo: Verificar la aplicación de los controles de Seguridad y Ciber seguridad se apliquen de manera planeada de acuerdo con los niveles de estrategia, operación y servicios de la LOTERIA DE MEDELLÍN en los componentes establecidos por la Entidad.

Referencia: "Prestación de servicios profesionales para realizar la Auditoria interna al proceso de Gestión de Tecnología de la información y las comunicaciones TIC"

Alcance: Esta actividad comprendió la evaluación de los controles dispuestos para atender las actividades de los procesos y establecer en nivel del riesgo asociado a estos.

Criterio: Se tomaron 4 componentes evaluativos, así:

1. Gestión de la estrategia, de los servicios y los requerimientos
2. Operación de los servicios (solicitudes de servicios de ti, diseño de los servicios, gestión de incidentes, gestión de problemas, gestión de cambios, transición de los servicios.
3. Gestión de requerimientos e incidentes de seguridad,
4. Gestión de seguridad de la información

Este marco de referencia hace parte del portafolio de auditorías de talla mundial, tomando como referencia las normas ISO de: Seguridad de la información (27001), Ciber Seguridad (27032), Incidentes (27035), Continuidad (22301) y Servicios de T.I (20000) y Gobierno Corporativo (COBIT 2019). Se incluyen las que aplican según acta de apertura del 23 de agosto de 2023 (se anexa el acta).

Tipo de auditoría: En sitio basado en entrevistas y en los criterios de auditoría.

ASPECTOS RELEVANTES

- El recurso humano de LOTERIA DE MEDELLÍN demuestra el compromiso adquirido para el desarrollo de actividades que buscan proteger la información de sus partes interesadas y opera ininterrumpidamente sus controles con dedicación al aprendizaje continuo y de manera proactiva.
- En nuestro acompañamiento a los procesos siempre se ha mostrado un avance en la búsqueda de nuevas soluciones que permitan acceder a componentes tecnológicos competitivos frente a la misión Corporativa.
- Las actividades resultantes de prácticas de Ciber seguridad han mostrado que se tienen en cuenta elementos que impactan controles para demostrar confianza a clientes externos y usuarios internos.
- Se percibe el afán de realizar controles basados en requisitos de industria para generar competitividad Corporativa.

OPORTUNIDADES

- LOTERIA DE MEDELLÍN puede encontrar oportunidades de potenciar los controles de Seguridad y Ciber seguridad, aplicando un despliegue del control basado en **activos de información**, los cuales son el punto final de las amenazas internas y/o externas que potencian riesgos de Seguridad y Ciber Seguridad.
- LOTERIA DE MEDELLÍN puede encontrar factores competitivos y la generación de valor a sus procesos mediante la aplicación de una visión integradora de actividades con prácticas que incluyan el ciclo PHVA en todos sus procesos.
- Con la puesta a prueba de los controles definidos mediante simulacros programados con el fin de verificar el grado de adherencia que tienen los controles a los procesos, se obtendrán oportunidades de mejorar y ajustar los controles con mayor relevancia competitiva.

1. GESTIÓN DE LA ESTRATEGIA, DE LOS SERVICIOS Y LOS REQUERIMIENTO

Objetivo: Determinar la conformidad, eficacia y mejoramiento continuo de cumplimiento a Entidades internas y externas teniendo como referente los dominios del modelo de arquitectura Empresarial y control interno para la gestión de la tecnología respecto a los criterios establecidos, incluyendo la legislación aplicable y la documentación de la Entidad.

ACTIVIDAD	Se verifica que LOTERIA DE MEDELLÍN en su Plan Estratégico de TI busque el cumplimiento de los objetivos de las TIC´S alineado con los objetivos estratégicos de la Entidad y se optimicen los recursos de T.I.
HALLAZGO	Basado en las evidencias presentadas frente a los criterios de auditoria se puede concluir que es una desviación positiva, frente a: • Se realiza un adecuado plan para satisfacer las necesidades relacionadas con el manejo y gestión de la información en la Entidad • Oportuna administración y mantenimiento asertivo de la plataforma tecnológica. • La optimización de los recursos tecnológicos (Infraestructura, aplicativos, servicios tercerizados y recursos humanos) • Prácticas de industria que han impulsado la transformación digital en Loteria de Medellín de acuerdo con el plan estratégico institucional para el cuatrienio 2020-2023.
RIESGOS	En vista del manejo adecuado de la estrategia de T.I. y el cumplimiento de esta en el cuatrienio 2020-2023 y según "7.7.1 DOFA y 7.7.2. Análisis CAME" del plan estratégico, se perciben amenazas Organizacionales como: • **Pérdida de ventaja competitiva** por vulnerabilidades asociadas a la desactualización de la estrategia, falta o insuficiencia de disposiciones de seguridad de la información, falta o ausencia de vigilancia tecnológica. • **Materialización de riesgos** de seguridad de la información proporcionados por respuestas inadecuadas a los requisitos de los servicios y la ausencia del responsable de los controles. • **Pérdida de continuidad** de los servicios críticos ocasionados por la ausencia de las simulaciones del plan de continuidad del negocio según el análisis CAME
RECOMENDACIONES	Para permitir una continuidad asertiva en relación con la estrategia de T.I, la LOTERIA DE MEDELLÍN deberia: • Realizar un análisis de la brecha tecnología actual frente a normativas y marcos de referencia de industria como COBIT 2019, ISO 27001, NIST e ITIL (de elección)

	con el fin de establecer un marco de gobierno de T.I y definir una arquitectura de seguridad de la Entidad. • Potencializar la Plataforma tecnológica alineada con las ventas tradicionales y el portal de ventas en línea, proporcionará gestión de capacidad para el uso de los recursos y proyecciones de requisitos futuros que buscaran el cumplimiento de metas Corporativas. • Buscando aumentar la competitividad de la Entidad, determinar la competencia requerida de las personas que realizan, bajo su control, las actividades relacionadas con la seguridad y ciber seguridad de la información.
2. OPERACIÓN DE LOS SERVICIOS (solicitudes de servicios de TI, diseño de los servicios, gestión de incidentes, gestión de problemas, gestión de cambios, transición de los servicios). Objetivo: Evidenciar la capacidad para planificar, establecer, implementar, operar, monitorear, evaluar, mantener y mejorar los servicios desde la solicitud hasta la solución.	
ACTIVIDAD	Se verifica el Modelo integrado de planeación y gestión, la mesa de servicios (CAU, Centro de Atención al Usuario) como los recursos tecnológicos y humanos, que prestan servicios a usuarios con el fin de establecer la pertinencia de estos recursos como componente de soporte a las tecnologías de información.
HALLAZGO	En el análisis de esta documentación y operación de los servicios, se puede concluir que la LOTERIA DE MEDELLÍN define sus servicios basados en prácticas de ITIL como buena práctica para la gestión de servicios de tecnologías de la información y aunque es una guía de industria, esta no alcanza a desarrollarse en su implementación en la Entidad pues aún no se puede evidenciar la gestión en su planificación, operación, seguimiento y mejora continua.
RIESGO	Incapacidad de medición y mejora continua de los servicios de T.I. causado por la ausencia de elementos claves como la continuidad, capacidad, presupuesto, relaciones del servicio y otros.
RECOMENDACIÓN	Para una gestión de los servicios de TI, La LOTERIA DE MEDELLÍN debería fortalecer los elementos de configuración de los servicios con gestión de: capacidad, continuidad, niveles, seguridad, presupuesto, incidentes, problemas, cambios y mediciones como componentes de los servicios con el fin de llevar controles adecuados a las necesidades de la Entidad.
3. GESTIÓN DE REQUERIMIENTOS E INCIDENTES DE SEGURIDAD. Objetivo: Evaluar que los requerimientos e incidentes de seguridad estén aplicados como controles de seguridad de los sistemas de información.	
ACTIVIDAD	Se verifica que LOTERIA DE MEDELLÍN asegura que una gestión a los requerimientos e incidentes la Seguridad sea una parte integral de los sistemas de información como componente critico de la gestión de las tecnologías de información
HALLAZGO	• No se evidencia un análisis y especificaciones de requisitos de seguridad para nuevos sistemas o para mejoras de estos • No se lleva un enfoque que permita controlar con trazabilidad un incidente de seguridad hasta llevarlo a una base de datos de conocimiento
RIESGO	Posibilidad de pérdida de controles o no visibilizarlos en las actividades de seguridad operativas de las incidentes y los rewqueriemientos en l ciclo de desarrollo de software.
RECOMENDACIÓN	• LOTERIA DE MEDELLÍN debería establecer una práctica de análisis de los requerimientos de sistemas que incluyan temáticas relacionadas con la seguridad

	de la información (Confidencialidad, Disponibilidad e integridad) con el fin de asegurar la practicas de desarrollo encaminadas al desarrollo de software seguro. • LOTERIA DE MEDELLÍN debería contar con una actividad atención de incidentes con atributos de responsabilidades y escalamientos, evaluación, protocolo de atención, respuesta y lecciones aprendidas para todos los incidentes de seguridad. • Asignar un responsable de la seguridad de la información (CISO), que planee y ejecuta permanentemente las actividades de control de seguridad y ciberseguridad de la Entidad con el fin de establecer mecanismos de detección, prevención y protección de la información.

4. CONTROLES DE SEGURIDAD EN LA INFRAESTRUCTURA
Objetivo: Evaluar los controles actuales de la Entidad para encontrar la oportunidad de la placabilidad de estos y aplicables a la infraestructura de la Entidad

ACTIVIDAD	Se verifica que en LOTERIA DE MEDELLÍN que la seguridad de la información esté diseñada e implementada dentro de la infraestructura y su oportunidad de endurecer los controles y su pertinente evaluación.
HALLAZGO	LOTERIA DE MEDELLÍN cuenta con aliados que realizar evaluaciones de **servidores locales** y actividades evaluativas de las **operaciones de T.I.**, pero aún no se pude evidenciar un despliegue desde un procedimiento o política que permita las validaciones en equipos, redes, terceros, recurso humano, proveedores que demuestre que los controles de seguridad estén activos y son los adecuados al negocio.
RIESGO	Pérdida o desconocimiento de informacion de todos los componentes de las TIC´s de la Empresa que permitan controlar las actividades que puedan generar amenazas internas y/o externas a la información.
RECOMENDACIÓN	LOTERIA DE MEDELLÍN debería establecer un mecanismo, procedimiento o política de evaluación de los **componentes de T.I** donde se describan actividades pertinentes a la seguridad y la Ciber seguridad enfocadas a contar con información oportuna y tener en cuenta **cuando sea aplicable:** **Seguridad en servidores** • On Premises • En Nube (propia, publica, hibrida) • Virtualizados • En hosting, colocation, otras **Seguridad en Telecomunicaciones** • Redes internas/externas • Conectividad • VPN • Segmentación • Perímetro **Validación del HARDENING a:** • Sistemas operativos • Servidores • Bases de datos • Aplicativos • Recurso Humano

	• Conectividad
5. CONTROLES DE SEGURIDAD A LOS PROCESOS Objetivo: Verificar los controles de seguridad aplicados para la búsqueda de la mejora continua de los procesos de la Entidad.	
ACTIVIDAD	Se verifica que LOTERIA DE MEDELLÍN asegura la protección de la información resultante de las actividades de los procesos de la Entidad.
HALLAZGO	• Se evidencia que la política de seguridad considera normas de referencia con versión desactualizada (ISO 27001:2006). • Se evidencia que el plan de continuidad solo tiene en cuenta los procesos misionales. • No se puede evidenciar la aplicación de pruebas o simulacros del plan de continuidad y la seguridad asociada
RIESGO	• Perdida del control en las operaciones para las actividades rerefentes al cumplimiento de las politicas. • Posible pérdida de informacion de procesos de apoyo que no se incluyen en el plan de continuidad de LOTERIA DE MEDELLÍN.
RECOMENDACIÓN	• Revisar el esquema documental de la seguridad y evaluar el cumplimiento de las políticas en términos del nivel de actualización y dejar el registro del nivel de cumplimiento de las políticas por parte de los usuarios y la pertinencia técnica asociada. • LOTERIA DE MEDELLÍN debería desplegar el plan de continuidad del negocio a otros procesos de apoyo a los misionales que también podría causar pérdida de información crítica. • LOTERIA DE MEDELLÍN debería considerar la realización de simulacros documentados referente al nivel de riesgo percibido en las operaciones y continuidad de los procesos referentes a la pérdida de información crítica y sensible. • Actualizar la politica de seguridad de la informacion a vesiones vigentes (por ejemplo ISO 27001:2022), con el fin de potenciar a la Entidad en practicas de industria y establecer la orientacion y el direccionamiento a las partes interesadas en la seguridad de la informacion.
6. CONTROLES DE SEGURIDAD PROVENIENTES DEL PLAN DE TATAMIENTO DE RIESGOS Objetivo: Validar los controles provenientes de los riesgos de seguridad de la información para establecer las condiciones metodológicas aplicables a la Entidad.	
ACTIVIDAD	Se verifica que los controles definidos para la gestión de los riesgos sean apropiados a las necesidades y requisitos del negocio. Tomado del "Plan de tratamiento de riesgos de seguridad y privacidad de la información, LOTERIA DE MEDELLIN – 2023" y la "matriz riesgos tics.xls"
HALLAZGO	• Identificación de riesgos que no permite la asignación de controles que impacten los procesos de la LOTERIA DE MEDELLÍN. • El modelo propuesto no demuestra la aplicación de la NTC/ISO 27005, pues no identifica amenazas y vulnerabilidades aplicables a los activos de información y asi mismo la aplicación de controles basados a estos.

RIESGO	Alta posibilidad de perdida de control en caso de incidentes de seguridad que puedan comprometer a la Empresa en impactos legales y de continuidad de las operaciones.
RECOMENDACIÓNES	• LOTERIA DE MEDELLÍN debería establecer un método de gestión de riesgos de seguridad de la información aplicable a todos los procesos y basado en activos de información, con el fin de obtener permanentemente un abordaje a los riesgos de manera granular y especifica, pues la dinámica de la gestión tecnológica exige un conocimiento predictivo de las potencialidades de amenazas que puedan aprovechar las vulnerabilidades y generar impactos no deseables en la Entidad. • Se sugiere la adopción de la NTC-ISO/IEC 27005:2020 para actualizar las caracteristicas y la metodologia aplicable a los riesgos de la Entidad.

7. CONCLUSIONES

De acuerdo con las evidencias recolectadas en este acompañamiento y a las recomendaciones planteadas se puede concluir que LOTERIA DE MEDELLÍN:

1. Ha desarrollado planes de trabajo para atender los requisitos de negocio, pero aún no puede demostrar gestión de sus controles mediante un análisis transversal del impacto de la asignación de los controles en los procesos de la Empresa.
2. Ha adquirido acompañamiento externo a sus controles críticos con Empresas de seguridad y Ciber seguridad expertas y desarrolla prácticas de T.I. acordes a la operación lo cual genera confianza a las partes interesadas, pero falta incursionar en los procesos del día a día con los usuarios con un mapeo y acompañamiento permanente en el manejo y la responsabilidad de los usuarios en el uso de la información.
3. Con la atención de las recomendaciones anteriores, LOTERIA DE MEDELLÍN encontrará oportunidades para potenciar la gestión de las tecnologías de información y encontrará factores competitivos para el cumplimiento de los objetivos Corporativos, pues está cimentado en normas y marcos de referencia de talla mundial.

RECOMENDACIONES A NIVEL INSTITUCIONAL

- LA LOTERIA DE MEDELLÍN debe establecer, implementar, operar, hacer seguimiento y mejorar continuamente la gestión de la Seguridad y Ciber seguridad de la información con el fin de tomar decisiones respecto al nivel de inversión que realiza en sus tecnologicas y poder establecer la relacion costo-beneficio de las acciones aplicadas con la busqueda de beneficios y cumplimiento de objetivos.
- LA LOTERIA DE MEDELLÍN debería establecer una arquitectura de seguridad y Ciber Seguridad que pemita desarrollar conductores de objetivos y la manera de cumplirlos, a través de un oficial de seguridad de información.
- LA LOTERIA DE MEDELLÍN debería contemplar el ciclo de vida de los procesos con el fin de encontrar oportunidades para el negocio mediante ciclos P-H-V-A para la gestión de la Seguridad y Ciber Seguridad de la información

	INFORME DE AUDITORIA INTERNA Componente de Seguridad y Ciber Seguridad de la información	

FIRMA DEL AUDITOR Oscar Darío Marín Rivera Consejo Profesional Nacional de Ingeniería COPNIA Matrícula Profesional No. 05862231190ANT	
	OBSERVACIONES:
FIRMA DEL RESPONSABLE DEL PROCESO	