INFORME AUDITORÍA INTERNA INDEPENDIENTE

INFORME DE AUDITORÍA

Preliminar		Final	X

NOMBRE DE LA AUDITORIA

Auditoria a la Gestión de la seguridad de la Información en la Entidad

OBJETIVO

Verificar la apropiación de las buenas prácticas y los lineamientos de seguridad y privacidad de la información establecidos por la Entidad para mitigar y controlar los riesgos relacionados con confidencialidad, integridad y disponibilidad de la información física y digital.

ALCANCE DE LA AUDITORÍA

Se realizará la verificación de la apropiación de las buenas prácticas y los lineamientos de seguridad y privacidad de la información establecidos por la Entidad en el periodo comprendido entre enero de 2020 a febrero de 2021

CRITERIOS DE AUDITORÍA

Constitución Política de Colombia: Artículo 15 (Derecho a la intimidad y buen nombre), artículo 20 (Derecho de información) y artículo 74 (Acceso a documentos públicos).
Ley 80 de 1993 *por la cual se expide el Estatuto General de Contratación de la Administración Pública.*
LEY 87 DE 1993 "Por la cual se establecen normas para el ejercicio de control interno en la entidades y organismos del estado y se dictan otras disposiciones"
Ley 44 de 1993 "por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944." (Derechos de autor)
Ley 527 de 1999 "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones."
Ley 594 de 2000 "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones".
Ley Estatutaria 1266 de 2008, Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales
Ley 1273 de 2009. Ley por medio de la cual se crea y se protege el bien jurídico de la información y los datos personales. Así mismo, se tipifican conductas penales como daño informático, violación de datos personales, acceso abusivo a sistema informático, interceptación de datos informáticos, hurto por medios informáticos, entre otras.
Ley estatutaria 1581 de 2012 (Por la cual se dictan disposiciones generales para la protección de datos personales.).
Ley 1341 de 2009. "Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC
Decreto Reglamentario 1377 de 2013 "Por el cual se reglamenta parcialmente la Ley 1581 de 2012"
Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
Decreto 886 de 2014 "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos."
Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"
Decreto Único Reglamentario 1074 de 2015 (Compilatorio en ley de Protección de Datos Personales)

INFORME AUDITORÍA INTERNA INDEPENDIENTE

Decreto 103 de 2015: "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 (Ley de Transparencia y acceso a la información pública) y se dictan otras disposiciones."
Decreto 1081 de 2015, Título 1, Este Título tiene por objeto reglamentar la Ley 1712 de 2014, en lo relativo a la gestión de la información pública.
DIRECTIVA 003 DE 2013
Modelo Integrado de Planeación y Gestión MIPG.
Manual de seguridad de la información Plan de seguridad y privacidad de la información y Plan de gestión de riesgos de seguridad digital de la UAECOB
Procedimiento copias de seguridad
Demás normas que apliquen.

LÍDER DE PROCESO/DEPENDENCIA

Norma Cecilia Sánchez Sandino- Jefe Oficina Asesora de Planeación

EQUIPO AUDITOR

Rubén Antonio Mora Garcés- jefe Oficina de Control Interno
María del Carmen Bonilla- Profesional 219 grado 20 Oficina de Control Interno

PERIODO DE EJECUCIÓN DE LA AUDITORÍA

01 de marzo al 28 de mayo de 2021

METODOLOGÍA

De conformidad con la Guía de Auditoría para Entidades Públicas expedida por el DAFP, se emplearon los siguientes procedimientos de auditoría: Consulta, Observación, aplicación de encuestas Inspección y Revisión de evidencia física. Adicionalmente, se empleó la metodología PHVA (Planear, Hacer, Verificar, Actuar)

a) Planear:

- Elaboración del Plan de auditoría y la lista de verificación
- Definición de los objetivos, el alcance y los tiempos de ejecución.
- Preparar la auditoría decampo, papeles de trabajo, investigación documental y procedimental sobre el proceso auditado.

b) Hacer:

- Auditoría de campo a través de entrevista
- Recolección y verificación de lainformación obtenida de las entrevistas y evidencias documentales.
- Entrega del Informe preliminar de auditoría a los líderes y/o responsables de los procesos auditados.

c) Verificar:

- Análisis de la información, evidencias, y verificación del cumplimiento de acuerdo a lo establecido en los procedimientos, requisitos legales, normas aplicables definidas para la auditoría.

- Mesas de validación de hallazgos donde se presentó el informe preliminar, se aclararon y/o justificaron los hallazgos de no conformidad por parte de los auditores y de los auditados, respectivamente.
- Análisis de las evidencias e información adicional entregada por los auditados en la mesa de validación de hallazgos, y determinar la subsanación de las no conformidades u observaciones.
- Entrega del Informe final de auditoría a los líderes y/o responsables de los procesos auditados.

d) Actuar:

- Solicitud del Plan de Mejoramiento de los hallazgos o desviaciones encontrados, en el FOR-GI-04-01 Solicitud de ACPM.

Se realizaron dos entrevistas, una presencial al profesional responsable del área de tecnología, y, la segunda vía teams aplicada al nuevo responsable del área tecnología a partir del mes de abril de 2021.

Se aplico una encuesta a los directivos quienes son los responsables de fomentar la apropiación de las buenas prácticas y los lineamientos de seguridad y privacidad de la información y otra encuesta a una muestra de treinta y cinco (35) personas entre servidores públicos y contratistas.

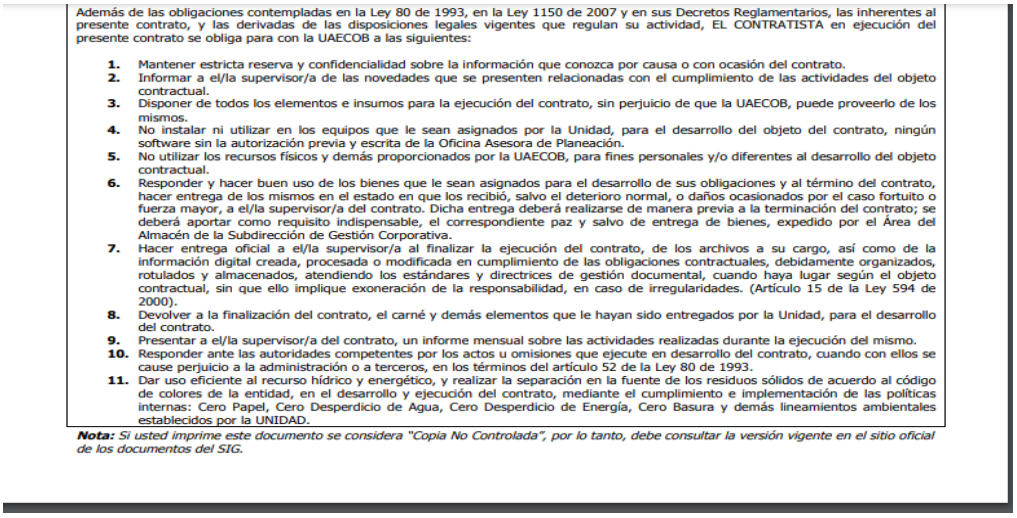
SITUACIONES GENERALES

1. FORTALEZAS

1.1. Se resalta el compromiso, responsabilidad y dedicación del equipo de profesionales que conforman el área de recursos tecnológicos para atender los diferentes frentes de servicios que demanda la Unidad.
1.2. Los servidores en los que se albergan la información de la Unidad se mantienen en un entorno de funcionamiento óptimo.
1.3. La seguridad de la red cuenta con herramientas como: firewalls, VPN, detección de intrusos, así como sistemas de monitoreo permanente observado por un profesional contratista.
1.4. Se cuenta con los siguientes documentos: Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI 2021-2024, Plan de Seguridad y Privacidad de la Información, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Manual de Políticas de Seguridad y Privacidad de la Información, aprobados en el Comité de Gestión y desempeño en la sesión del 27 de enero de 2021; documentos que promueven el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital. En cumplimiento a lo de lo establecido en el Decreto 1078 de 2015.

DIRECTIVA 003 DE 2013

Se evidenció que la Entidad incorporar en los contratos de prestación de servicios cláusulas relacionadas con la conservación y uso adecuado de los bienes, servicios y documentos de la Unidad, así como la obligación de responder por su deterioro o pérdida, a manera de ejemplo:



Además de las obligaciones contempladas en la Ley 80 de 1993, en la Ley 1150 de 2007 y en sus Decretos Reglamentarios, las inherentes al presente contrato, y las derivadas de las disposiciones legales vigentes que regulan su actividad, EL CONTRATISTA en ejecución del presente contrato se obliga para con la UAECOB a las siguientes:

1. Mantener estricta reserva y confidencialidad sobre la información que conozca por causa o con ocasión del contrato.
2. Informar a el/la supervisor/a de las novedades que se presenten relacionadas con el cumplimiento de las actividades del objeto contractual.
3. Disponer de todos los elementos e insumos para la ejecución del contrato, sin perjuicio de que la UAECOB, puede proveerlo de los mismos.
4. No instalar ni utilizar en los equipos que le sean asignados por la Unidad, para el desarrollo del objeto del contrato, ningún software sin la autorización previa y escrita de la Oficina Asesora de Planeación.
5. No utilizar los recursos físicos y demás proporcionados por la UAECOB, para fines personales y/o diferentes al desarrollo del objeto contractual.
6. Responder y hacer buen uso de los bienes que le sean asignados para el desarrollo de sus obligaciones y al término del contrato, hacer entrega de los mismos en el estado en que los recibió, salvo el deterioro normal, o daños ocasionados por el caso fortuito o fuerza mayor, a el/la supervisor/a del contrato. Dicha entrega deberá realizarse de manera previa a la terminación del contrato; se deberá aportar como requisito indispensable, el correspondiente paz y salvo de entrega de bienes, expedido por el Área del Almacén de la Subdirección de Gestión Corporativa.
7. Hacer entrega oficial a el/la supervisor/a al finalizar la ejecución del contrato, de los archivos a su cargo, así como de la información digital creada, procesada o modificada en cumplimiento de las obligaciones contractuales, debidamente organizados, rotulados y almacenados, atendiendo los estándares y directrices de gestión documental, cuando haya lugar según el objeto contractual, sin que ello implique exoneración de la responsabilidad, en caso de irregularidades. (Artículo 15 de la Ley 594 de 2000).
8. Devolver a la finalización del contrato, el carné y demás elementos que le hayan sido entregados por la Unidad, para el desarrollo del contrato.
9. Presentar a el/la supervisor/a del contrato, un informe mensual sobre las actividades realizadas durante la ejecución del mismo.
10. Responder ante las autoridades competentes por los actos u omisiones que ejecute en desarrollo del contrato, cuando con ellos se cause perjuicio a la administración o a terceros, en los términos del artículo 52 de la Ley 80 de 1993.
11. Dar uso eficiente al recurso hídrico y energético, y realizar la separación en la fuente de los residuos sólidos de acuerdo al código de colores de la entidad, en el desarrollo y ejecución del contrato, mediante el cumplimiento e implementación de las políticas internas: Cero Papel, Cero Desperdicio de Agua, Cero Desperdicio de Energía, Cero Basura y demás lineamientos ambientales establecidos por la UNIDAD.

Nota: *Si usted imprime este documento se considera "Copia No Controlada", por lo tanto, debe consultar la versión vigente en el sitio oficial de los documentos del SIG.*

También se comprobó que los particulares que ejercen actividades públicas que se desempeñan en esta área son conscientes de la responsabilidad del manejo de los documentos públicos y de los elementos que se ponen a su disposición para la ejecución de sus tareas.

2. DESVIACIONES

Para las vigencias 2020 y 2021 la Entidad celebró contratos enfocados a fortalecer la seguridad de la información entre los que se observan los siguientes:

Vigencia 2020

# Contrato	Contratista	Objeto	Valor	Ejecución en meses	Observación
659-2020	SOLUCIONES TECNOLOGIA Y SERVICIOS S A STS S A	ACTUALIZACIÓN Y COMPLEMENTACIÓN DE LA SEGURIDAD PERIMETRAL DE LA UAECOB.	359.800.000	3	Finalizado el 20/01/2021
677-2020	SOCIEDAD CAMERAL DE CERTIFICACION DIGITAL CERTICAMARA S.A.	CONTRATAR LA ADQUISICIÓN DE LOS CERTIFICADOS DIGITALES DE SEGURIDAD SSL PARA LOS SISTEMAS DE INFORMACIÓN Y LA FIRMA DIGITAL PARA EL SISTEMA DOCUMENTAL DE LA UAECOB	24.901.940	1	Finalizado el 02//01/2021
660-2020	PROXEL COLOMBIA S.A.S.	CONTRATAR LA REVISIÓN Y DIAGNÓSTICO DE LA SEGURIDAD ELECTRÓNICA DEL EDIFICIO COMANDO	2.800.000	1	Finalizado el 24/12/2020
715-2020	REDNEET SAS	CONTRATAR LA TRANSICIÓN DE IPV4 A IPV6 PARA LA UAECOB	98.692.650	4	Finalizado el 31/03/2021
697-2020	COLOMBIA TELECOMUNICACIONES S.A. E.S.P	CONTRATAR LOS SERVICIOS DE NUBE PÚBLICA PARA LA UAECOB.	191.305.287	12	Contrato en ejecución finaliza el 11/11/2021

578-2020	JUAN DARIO CHACON MELO	PRESTAR SERVICIOS PROFESIONALES COMO OFICIAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UAECOB, EN EL MARCO DE LA ARQUITECTURA EMPRESARIAL Y DEL COMPONENTE DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ESTRATEGIA GOBIERNO DIGITAL	15.750.000	4.5	Finalizado el 23/01/2021
288-2020	JHON ALEXANDER ALARCON GUZMAN	PRESTAR SERVICIOS PROFESIONALES EN LA OFICINA ASESORA DE PLANEACIÓN EN LO RELACIONADO CON LAS REDES DE DATOS Y MONITOREO DE LOS SISTEMAS DE SEGURIDAD INFORMÁTICA DE LA ENTIDAD.	54.400.000	8,5	Finalizado el 30/12/2020
383-2020	JAIME ANDRES ORTIZ TENORIO	PRESTAR SERVICIOS PROFESIONALES PARA LA ADMINISTRACIÓN, MANTENIMIENTO Y GESTIÓN DE SERVICIOS INFORMÁTICOS RELACIONADOS CON LA SEGURIDAD INFORMÁTICA DE LA UAECOB.	42.000.000	7	Finalizado el 02/01/2021
705-2020	JOSE ORINSON ALVAREZ BERMUDEZ	PRESTAR SERVICIOS DE APOYO A LA OFICINA ASESORA DE PLANEACIÓN PARA APOYAR EN EL SEGUIMIENTO DE LOS INCIDENTES RELACIONADOS CON SEGURIDAD DE LA INFORMACIÓN	6.400.000	2	Finalizado el 01/02/2021
230-2020	DIANA MILENA MARTINEZ BOCANEGRA	PRESTAR SERVICIOS PROFESIONALES PARA GESTIONAR, DOCUMENTAR Y MONITOREAR LOS SERVIDORES Y DISPOSITIVOS DE ALMACENAMIENTO DE LA PLATAFORMA TECNOLÓGICA DE LA ENTIDAD.	60.800.000	9.5	Finalizado el 31/12/2020
Total			**856.849.877**		

Fuente: Oficina Asesora Jurídica- UAECOB Corte 31 de diciembre de 2020.

Vigencia 2021

# Contrato	Contratista	Objeto	valor	Ejecución en meses	Observación
056-2021	JENIFFER VANESSA BRIÑEZ REMISIO	PRESTAR SERVICIOS PROFESIONALES EN LA OFICINA ASESORA DE PLANEACIÓN, PARA APOYAR LAS ACTIVIDADES NECESARIAS QUE PERMITAN LA CONSOLIDACIÓN DE LA ESTRATEGIA Y GOBIERNO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN LA UAECOB.	36.000.000	9	En ejecución desde el 26/01/2021

149/2021	ELKIN ROBERT LOPEZ BOLIVAR	Prestar Servicios Profesionales como gestor de Servicios Tecnológicos para apoyar los procesos relacionados con la gestión de la capacidad, continuidad, disponibilidad y seguridad de la infraestructura tecnológica de la UAECOB.	52.000.000	8	En ejecución desde el 08/02/2021
327/2021	JAIME ANDRES ORTIZ TENORIO	Prestación de servicios profesionales para aplicar los lineamientos impartidos en la política de seguridad y privacidad de la información en la UAECOB	52.000.000	8	En ejecución desde el 31/03/2021
326/2021	JHON ALEXANDER ALARCON GUZMAN	Prestar servicios profesionales como administrador de redes para gestionar la infraestructura tecnológica de redes LAN y WAN de la UAECOB	52.000.000	8	En ejecución desde el 30/03/2021
348/2021	CLUSTER DE SERVICIOS SAS	CONTRATAR LA ADQUISICIÓN Y RENOVACIÓN DEL LICENCIAMIENTO DE ANTIVIRUS PARA LA UAECOB	49.820.948	2	En ejecución desde el 31/03/2021
330/2021	MARISOL LOZANO OLAVE	PRESTACIÓN DE SERVICIOS PROFESIONALES COMO OFICIAL DE SEGURIDAD QUE PERMITA ESTRUCTURAR, IMPLEMENTAR Y HACER SEGUIMIENTO A TODAS LAS ACTIVIDADES NECESARIAS PARA DESARROLLAR LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA UAECOB	52.000.000	8	En ejecución desde el 08/04/2021
339/2021	DIANA MILENA MARTINEZ BOCANEGRA	PRESTAR SERVICIOS PROFESIONALES COMO ADMINISTRADOR DE BASES DE DATOS EN LA UAECOB	52.000.000	8	En ejecución desde el 09/04/2021
Total			**345.820.948**		

Fuente: SIDEAP (enero- abril 2021)

Tal como se evidencia en los cuadros anteriores la Entidad ha venido realizando una inversión importante de recursos para garantizar la seguridad de la información en la entidad, no obstante, se evidenciaron algunas deficiencias que mencionamos a continuación:

2.1 Se evidenció el documento denominado Plan de gestión de riesgos de seguridad digital, el cual contempla la amenazas, vulnerabilidades y riesgos, pero no se tiene establecido la declaración de aplicabilidad de los controles, al revisar los seis (6) procedimientos existentes para el proceso de Gestión Tecnológica no se observó que los controles existentes mitiguen los riesgos identificados en el mencionado plan, incumpliendo lo establecido en el procedimiento PROD-GI-01 V9 Administración de riesgos.

2.2 Se realizó la verificación de las actividades del procedimiento PROD-GT-01 V4 Copias de Seguridad, se solicitaron los formatos en donde se registran las hojas de vida de los servidores, el control de restauración, control de cintas y almacenamiento de cintas y se observó que no se encuentran actualizados y en algunos casos no se están diligenciando, caso puntual el almacenamiento de cintas. Lo observado pone en riesgo la continuidad del negocio en caso de presentarse un desastre ya sea natural o provocado por el vandalismo, como tampoco se tiene un lugar adecuado o bodega en donde se almacenen las cintas del Dataprotector, incumpliendo lo establecido en el procedimiento en comento.

2.3 En cumplimiento del "Propósito 5 - Construir Bogotá Región con gobierno abierto, transparente y ciudadanía consciente", contenido en el Plan de Desarrollo "Un nuevo contrato social y ambiental para la Bogotá del siglo XXI", la Entidad estableció la meta proyecto: "Implementar 100 % del modelo de seguridad y privacidad de la información en la UAECOB alineado a la Política de Gobierno Digital", en el proyecto de inversión "7637 - Fortalecimiento de la infraestructura de tecnología informática y de comunicaciones".

La mencionada meta proyecto cuenta con indicador en SEGPLAN, que dé cuenta del grado de avance en su ejecución y, revisada la batería de indicadores, se observa que para el área de recursos tecnológicos están definidos los dos (2) indicadores relacionados a continuación:

Nombre indicador	Factor de éxito
Medir el cumplimiento en la atención de incidentes reportados a la mesa de ayuda mediante el aplicativo de reporte de incidentes tecnológicos	Eficacia
Medir la disponibilidad de los aplicativos misionales y funcionales de la Entidad	Eficacia

Como puede observarse, los mencionados indicadores no dan cuenta del cumplimiento de la meta Proyecto, contenida en el Proyecto de inversión 7637.

Con base en lo expuesto, se puede concluir que no se tienen contemplados indicadores de gestión que permitan monitorear el comportamiento de factores críticos en la ejecución de las actividades relacionados con el cumplimiento del proyecto de inversión 7637, lo que impide evaluar el grado de avance de la meta propuesta.

La carencia de indicadores limita los elementos de evaluación con los que debería contar la alta dirección para la toma de decisiones estratégicas encaminadas a alcanzar el cumplimiento de dicha meta y, consecuentemente, del proyecto de inversión 7637.

Lo expuesto, incumple lo establecido en la '3ra. Dimensión - Gestión con valores para resultados' del Modelo Integrado de Planeación y Gestión (MIPG) y en el numeral 4.4.1 literal C, el numeral 9 Evaluación del desempeño, especialmente el 9.1.1 y 9.1.3 de la Norma Técnica de Calidad NTC-ISO 9001:2015.

2.4 Con el fin de establecer la apropiación de la seguridad de la información por parte de los Directivos, funcionarios y contratistas de la entidad, se aplicó a 35 personas una encuesta que contenía preguntas relacionadas con las Políticas de Seguridad para el manejo de la información contenida en la resolución interna 366 de 2014 que se encontraba vigente para el año 2020, y se obtuvo el siguiente resultado:

Directivos:

Pregunta	Respuesta acertada	Respuesta incorrecta
Conocimiento del acto administrativo que adopto la política de seguridad de la información	0,83	0,17
Claridad de las responsabilidades como directivo con relación a la seguridad de la información	1,00	0,00

Conocimiento de cuál área es responsable de la administración del inventario de recursos tecnológico	1,00	0,00
Claridad de quien debe realizar el backups de la información sensible de las dependencias	0,60	0,40
Conocimiento de la periodicidad para realizar el backups de la información sensible o importante que manejan las dependencias	0,20	0,80

Cuadro 2

Funcionarios y Contratistas:

Pregunta	Respuestas		
	Si	No	Parcialmente
¿Recibió inducción sobre la política de seguridad de la información y del uso y administración de los recursos tecnológicos en la Entidad?	0,30	0,37	0,33

Preguntas	Respuesta correcta	Respuesta incorrecta
Conocimiento de las actividades prohibidas para los usuarios en cuanto a la seguridad de la información en la Entidad.	0,13	0,87
Conocimiento de la periodicidad para realizar el Backup de la información sensible o importante que manejan las dependencias	0,07	0,93
Conocimiento del acto administrativo que adopto la política de seguridad de la información	0,6	0,4
Conocimiento de cuál área es responsable de la administración del inventario de recursos tecnológico	0,87	0,13

Cuadro 3

Como se puede observar en los cuadros 2 y 3, a pesar que los Directivos tiene claridad de la responsabilidad relacionada con la seguridad de la información, esta no se ve reflejada en los funcionarios y contratistas; teniendo en cuenta los resultados de la encuesta se evidenció:

- No se ha distribuido una copia de las políticas de seguridad de la información a los funcionarios y contratistas vinculados a la Entidad.
- No hay claridad frente a la responsabilidad de realizar los backup de la información sensible.
- No se tiene certeza de las actividades prohibidas para los usuarios en cuanto a la seguridad de la información.
- No se ha socializado en ningún escenario las políticas de seguridad de la información.

Sumado a la anterior, en sesión del 27 de enero de 2021, el Comité de Gestión y Desempeño aprueba el Manual de Políticas de Seguridad y Privacidad de la Información, que contiene lineamientos relacionados con la seguridad de la información en la Entidad, manual que es similar a lo contemplado en la resolución interna 366 de 2014, con lo cual, actualmente la entidad cuenta con dos lineamientos vigentes para la seguridad de la

información. No obstante existir dos lineamientos que versan sobre el mismo tema y tal como se pudo evidenciar en el resultado de las encuestas, no es claro para los funcionarios y contratitas las responsabilidades que les competen con relación a las buenas prácticas en el manejo, tratamiento, custodia y salvaguarda de la información institucional, no se ha realizado la derogatoria de la resolución 366 de 2014 a través de acto administrativo o documento pertinente, ni tampoco se han adelantado las socializaciones y capacitaciones a los funcionarios de planta y contratistas del manual vigente.

Lo observado, contraviene lo establecido en la resolución interna 366 de 2014 y en el Manual de Políticas de Seguridad y Privacidad de la información; poniendo en riesgo uno de los activos importantes de la Entidad como es la información, lo que podría afectar la continuidad del negocio en una situación crítica.

Incumple lo establecido en la Norma técnica de calidad 9000:2015 numeral 4.4.1 literal C, G; así como el numeral 7.3, numeral 7.5.2 literal C; 7.5.3.2 literal C.

CUADRO RESUMEN DE HALLAZGOS

ÍTEM	DESCRIPCIÓN	CRITERIO
2.1	Se evidenció el documento denominado Plan de gestión de riesgos de seguridad digital, el cual contempla la amenazas, vulnerabilidades y riesgos, pero no se tiene establecido la declaración de aplicabilidad de los controles,	PROD-GI-01 V9 Administración de riesgos
2.2	Se realizó la verificación de las actividades del procedimiento PROD-GT-01 V4 Copias de Seguridad, se solicitaron los formatos en donde se registran las hojas de vida de los servidores, el control de restauración, control de cintas y almacenamiento de cintas y se observó que no se encuentran actualizados y en algunos casos no se están diligenciando	PROD-GT-01 V4 Copias de Seguridad
2.3	No se tienen contemplados indicadores de gestión que permitan monitorear el comportamiento de factores críticos en la ejecución de las actividades relacionados con el cumplimiento del proyecto de inversión 7637, lo que impide evaluar el grado de avance de la meta propuesta.	Modelo integrado de planeación y gestión 3ra. Dimensión Gestión con valores para resultados. Norma técnica de calidad 9000:2015 numeral 4.4.1 literal C, el numeral 9 Evaluación del desempeño, especialmente el 9.1.1 y 9.1.3
2.4	No se han realizado las socializaciones y/o capacitaciones a los funcionarios y contratistas, sobre el Manual de Políticas de Seguridad y Privacidad de la Información, indicando las responsabilidades, políticas de backup y demás temas relevantes del mismo, sumado a que actualmente se cuenta con dos documentos (Resolución 366-2014 y Manual de Políticas de Seguridad y Privacidad de la Información, que versan y dan lineamientos sobre la seguridad de la información.	Norma técnica de calidad 9000:2015 numeral 4.4.1 literal C, G; así como el numeral 7.3, numeral 7.5.2 literal C; 7.5.3.2 literal C.

OBSERVACIONES

3.1 Pese a que la entidad cuenta con elementos físicos que permiten garantizar la continuidad y disponibilidad de los servicios de tecnologías de la información, no tiene un plan de continuidad de negocio ni un plan de recuperación de desastres.

3.2. Se evidenció que la Entidad tiene implementada una infraestructura de comunicaciones en el edificio comando que permite obtener una escalabilidad en la red, en multiservicios, capacidades y administración dando a la entidad un avance sustancial para el soporte de las comunicaciones con los beneficios de la organización de cuartos de equipos, herramientas de gestión, escalabilidad, administración, conectividad inalámbrica de alta densidad, recursos compartidos en multiservicio, soporte de voz, datos y video, lo que apunta a que esta infraestructura puede aportar al cumplimiento de lo establecido en la meta 349 del actual plan de desarrollo Distrital relacionada con "Diseñar e implementar al 100% el plan integral de mejoramiento tecnológico para la seguridad", meta a cargo del sector seguridad convivencia y justicia; por lo que se hace importante adelantar las gestiones necesarias con la Secretaría de Seguridad convivencia y Justicia para poner a disposición la infraestructura de comunicación (Data Center) bajo el liderazgo de la Entidad, con el fin de dar cumplimiento a la mencionada meta.

3.3. Con la entrada en vigencia de la resolución 306 de 2019 se creó el Comité de Gestión y desempeño instancia que absorbió (excepto aquellos obligatorios por mandato legal) los comités que tenían relación con el Modelo integrado de planeación y gestión, entre esos el Comité de tecnología de la información y las comunicaciones, en esta misma resolución se crearon los equipos técnicos de gestión con el fin de servir de apoyo al Comité de Gestión y desempeño. Con el fin de establecer la gestión adelantada por el equipo técnico encargado de gestionar e implementar la política de seguridad digital se solicitó al profesional encargado del área de tecnología evidenciar las sesiones adelantadas en donde se trataron los asuntos relacionados con las necesidades de recursos físicos, financieros, técnicos entre otros, para dar cumplimiento a lo establecido en la resolución 004 de 2017 de la Comisión Distrital de Sistemas y se evidenció que dentro del área de tecnología no se encuentra formalmente establecido el mencionado equipo técnico y que no se han venido adelantando reuniones o sesiones en donde se traten los temas establecidos en la resolución 004 de 2017, por lo que se hace importante que se adelanten las gestiones necesarias con el fin de establecer de manera formal el mencionado equipo técnico.

RECOMENDACIONES

Al líder del proceso de Gestión tecnológica:

- Establecer la declaración de aplicabilidad de los controles para el Plan de gestión de riesgos de seguridad digital, con el fin de mantener administrados los riesgos identificados y mitigar su materialización, así como dar cumplimiento a lo establecido en el procedimiento PROD-GI-01 V9 Administración de riesgos.
- Con su equipo de trabajo, revisar los documentos que hacen parte del proceso de Gestión tecnológica con el fin de evitar la redundancia normativa y asegurar que los documentos existentes se encuentran actualizados y facilitan la consulta a las partes interesadas.
- Asegurar que el responsable de operativizar el procedimiento de Copias de seguridad PROD-GT-01 V4, de cumplimiento a cada una de las actividades establecidas, así como el diligenciamiento de los formatos establecidos en el mencionado procedimiento, en lo posible revisar la pertinencia de actualizarlo.
- Revisar la batería de indicadores existente con el fin de que definan indicadores gestión que permitan monitorear el comportamiento de factores críticos en la ejecución de las actividades relacionados con el cumplimiento del proyecto de inversión 7637, que permitan evaluar el grado de avance de la meta propuesta.

- Revisar y definir cuál de los dos documentos que actualmente existen en la Entidad será el derrotero frente a la seguridad de la información, pues se cuenta con el Manual de seguridad de la información y la Resolución interna 366 de 2014, los dos documentos relacionados con la seguridad de la Información, evidenciándose una redundancia normativa pues las dos regulan el mismo supuesto de hecho.

Al comité de gestión y desempeño:

- Designar la tarea al equipo técnico que corresponda, construir el plan de continuidad de negocio y el plan de recuperación de desastres que garantices la resiliencia de la Entidad ante situaciones adversas, especialmente aquellas que afecten la seguridad de la información.
- Asegurar que el equipo técnico de gestión y desempeño encargado de implementar la política de seguridad digital, establezca un responsable para la seguridad de la información que garantice la aplicación de la política de seguridad de información en todos los niveles jerárquicos de la Entidad, con el fin de garantizar el debido cuidado de unos de los activos más importantes, para el caso que nos ocupa "la información".

CONCLUSION

Con base en la evaluación adelantada por la Oficina de Control Interno y una vez evaluados los hallazgos presentados, se puede concluir que se presentan debilidades frente a la apropiación de las buenas prácticas y los lineamientos de seguridad y privacidad de la información establecidos por la Entidad para mitigar y controlar los riesgos relacionados con confidencialidad, integridad y disponibilidad de la información física y digital, en todos los niveles jerárquicos de la Entidad.

Se hace importante recordar que la implementación del plan estratégico de tecnologías de la información, así como de la política de seguridad de la información, es un asunto institucional, no es solo del área de recursos tecnológicos, por lo tanto es importante que desde cada dependencia se designe un referentes que lidere las actividades requeridas para la implementación de cada uno de los lineamientos establecidos por el comité de gestión y desempeño, se redefina un plan de acción y se cuenten con los recursos necesarios para su ejecución.

EQUIPO AUDITOR	
Nombre(s): María del Carmen Bonilla- Profesional 219 grado 20 OCI	**Firma(s):** 

JEFE OFICINA DE CONTROL INTERNO	
Nombre: Rubén Antonio Mora Garcés	**Firma:**