	FORMATO	Código: F-PLA-15
	Informe auditoría interna de calidad	Versión: 04 Fecha: 20/12/2012
		Página 1 de 10

Coordinador de Calidad:	SECRETARIA DE TIC
Auditor Líder:	José Duván Lizarazo Cubillos – Jefe de Oficina de control interno de Gestión
Equipo Auditor:	Carlos Andres Lozano Valencia – Auditor contratista OCIG
Objetivo:	Verificar el cumplimiento de los indicadores en el Mapa de Riesgos Institucional de la Secretaria de Tics, correspondiente al primer semestre de 2021.
Alcance:	Evaluación y Seguimiento al Mapa de Riesgos Institucional mediante las siguientes acciones: 1) El cumplimiento de los indicadores previstos en el Mapa de Riesgos en este periodo. 2) La publicación de la documentación en intranet a través del formato MR- TIC-01 3) El diligenciamiento del formato MECI- F-PLA-25 "Gestión y monitoreo del Riesgo"
Documentos de referencia:	Documentación del Modelo Integrado de Planeación y Gestión
Fecha de apertura:	26 de julio de 2021
Fecha de cierre:	18 de agosto de 2021
Proceso:	La oficina de control interno de Gestión a través de la solicitud emitida con la circular No. S.A.60.07.01-00774 del 13 de julio de 2021; recolecta las evidencias y confronta los resultados de manera que demuestren el cumplimiento de los indicadores contenidos en la Intranet en el proceso estratégico de la secretaria de Tics del Departamento del Quindío, y los cuales fueron entregados a través de la circular S.TIC-62.217.00431 y evidencias anexadas en CD.

Conclusiones del equipo auditor

1. Anotaciones iniciales

El equipo auditor procede a realizar la evaluación de los riesgos descritos a los que estaría expuesto la secretaria TICS Departamental, teniendo en cuenta las evidencias presentadas y entregadas a la Oficina de Control Interno de Gestión como respuesta a la circular No. S.A.60.07.01-00774 del 13 de julio de 2021; evidencias que soportan los cumplimientos de las acciones correctivas encaminadas a la mitigación de los Riesgos institucionales propios de la dependencia, con corte a junio 30 de 2021. Por tal Motivo al finalizar el presente documento, se extrae fortalezas o debilidades que susciten a través del seguimiento.

2. Aspectos relevantes

La secretaria de Tics, determinó los siguientes seis (06) riesgos institucionales en los que estaría expuesta la misma y es por ello que la Oficina de Control Interno en su **Rol de Evaluación y Seguimiento** que describe y aplica los instrumentos de juicios creados por la misma oficina con el fin de analizar el avance de cumplimiento en procura de la mitigación de riesgos evaluados a partir de las evidencias suministradas.

GESTION DE LA TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES

Fortalecer el uso, la innovación y la apropiación de las Tecnologías de la Información y las Comunicaciones y la gestión de la información, con el fin de propiciar el cumplimiento de los objetivos de la institucionalidad gubernamental; promoviendo, aplicando y gestionando el ecosistema digital departamental, contribuyendo en el acercamiento permanente de la Administración Central Departamental con los ciudadanos mediante la implementación de la Política de Gobierno Digital. Ellos son:

R1 HURTOS DE SISTEMAS DE INFORMACION EN CUSTODIA DE LA SECRETARIA TIC
R2 EQUIPOS SUCEPTIBLES A FALLOS ELECTRONICOS QUE SE ENCUENTRAN EN EL EDIFICIO DE LA GOBERNACION DEL QUINDIO
R3. INEFICIENCIA ADMINISTRATIVA POR DESCONOCIMIENTO O FALTA DE FORMACIÓN TI
R4. ADULTERAR, MODIFICAR, SUSTRAER O ELIMINAR DATOS O INFORMACIÓN SENSIBLE, CONFIDENCIAL, CRÍTICA EN BENEFICIO PROPIO O DE TERCEROS
R5. COPIAS DE SEGURIDAD SISTEMAS DE INFORMACION
R6. POLITICA DE GOBIERNO DIGITAL CON BAJA IMPLEMENTACION

Conclusiones del equipo auditor

RIESGO 1. HURTO DE SISTEMAS DE INFORMACION EN CUSTODIA DE LA SECRETARIA TIC

El tipo de Riesgo: Operativo
Improbabilidad: 2
Impacto: 2 (Menor)
Zona de Riesgo: Bajo

Descripción: Hace referencia al hurto de la información, de los mismos equipos de cómputo o equipos de red con los que cuenta la gobernación de Quindío

Causas: Falta de controles de seguridad apoyados en la tecnología que garanticen la seguridad de los bienes tecnológicos del edificio de la gobernación del Quindío

Control: Para reducir el riesgo de robo la gobernación del Quindío cuenta con un inventario de los sistemas de información con el que cuenta la entidad, indicando así si se ha perpetuado algún hurto

Indicador:

a) *N° de inventarios realizados / N° de inventarios programados *100*

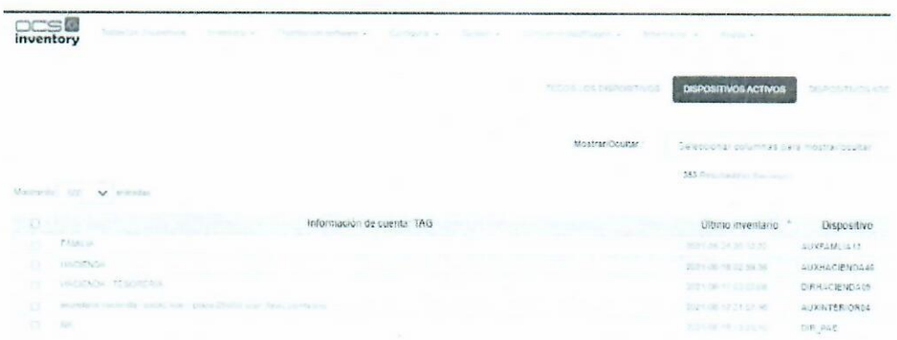
Aplicación:

a) *353 inventarios realizados / 353 inventarios programados *100 =* ***100%***

Evidencias:

Para el riesgo 1, la secretaria de Tecnologías de la Información y las Comunicaciones realizo durante el primer semestre de 2021, 353 inventarios de activos de información sobre 353 inventarios programados. A través de un software especializado instalado en todos los equipos de la entidad, se realiza automáticamente el inventario diario de activos de equipos de cómputo de la gobernación del Quindío. En este inventario se puede observar el nombre del equipo, ultimo inventario realizado, nombre de usuario, sistema operativo, RAM y CPU. De esta forma se lleva una inspección virtual de los equipos de la entidad y se indica si se ha perpetuado algún hurto, sin embargo, este control permitirá detectar el hurto después de haberse ocurrido y no se evidencian controles físicos para contrarrestar el riesgo antes de que ocurra.

La secretaria TIC envía PDF y archivo en Excel con los 353 inventarios realizados a los equipos de la gobernación.



Conclusiones del equipo auditor

RIESGO 2. EQUIPOS SUSCEPTIBLES A FALLOS ELECTRONICOS QUE SE ENCUENTRAN EN EL EDIFICIO DE LA GOBERNACIOND EL QUINDIO

El tipo de Riesgo: Operativo
Probabilidad: 4 (Probable)
Impacto: 2 (Menor)
Zona de Riesgo: Alto

Descripción: Los factores como traumatismos en los diferentes procesos informáticos de la administración Central Departamental por daño, falta de mantenimiento o virus en los equipos electrónicos de la entidad, ocasiona equipos susceptibles a fallos electrónicos que se encuentran en el edificio de la Gobernación del Quindío.

Causas: Traumatismos en los diferentes procesos informáticos de la administración Central Departamental por daño, falta de mantenimiento o virus en los equipos electrónicos de la entidad.

Control: El Director de Sistemas verifica periódicamente que los equipos se encuentren con el anti-virus instalado y licenciado correctamente, a través de la consola del aplicativo instalado en uno de los servidores de la entidad, además de esto se realiza mantenimiento preventivo anualmente a los equipos tecnológicos de la gobernación del Quindío; en caso de encontrar fallas en algún equipo o algún anti-virus no licenciado se procede a realizar el mantenimiento correctivo que se requiere y se deja como evidencia los informes presentados por el director de sistemas y el mantenimiento en el aplicativo en la mesa de ayuda.

Indicador:

a. *N° de equipos con antivirus licenciado / N° total de equipos de la gobernación del Quindío *100*
b. *N° de mantenimientos preventivos realizados / N° de mantenimientos preventivos programados *100*

Aplicación:

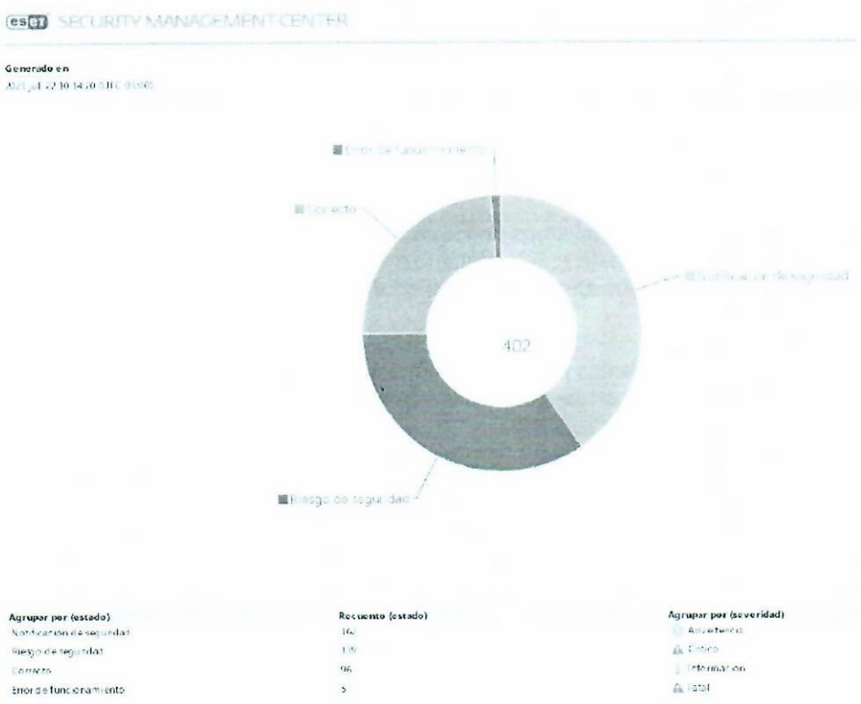
a. *402 equipos con antivirus licenciado / 402 total de equipos de la gobernación del Quindío *100 = 100%*
b. *248 mantenimientos preventivos realizados / 249 mantenimientos preventivos programados *100 = 99%*

Evidencias:

a. La gobernación del Quindío cuenta con 402 equipos instalados y licenciados correctamente con antivirus. Desde el security management center se puede evidenciar que 96 equipos se encuentran sin amenazas de virus, funcionamiento correcto. 162 equipos requieren atención o presentan notificación de seguridad, 139 tienen riesgo de seguridad y 5 equipos tienen error de funcionamiento. Se indica el estado de conexión, estado de los dispositivos, el estado de la administración y la versión del producto. De esta forma se está llevando el control y todos los equipos se encuentran con antivirus para evitar el riesgo de fallos electrónicos por virus.

   La secretaria TIC envía evidencia del archivo generado por la aplicación Security Management Center (ESET) generado el 22 de julio de 2021.

Conclusiones del equipo auditor



b. Durante el primer cuatrimestre de 2021 se recibieron 249 solicitudes de mantenimiento, de las cuales 248 fueron atendidas. Solo se evidencia 1 requerimiento asignado vencido.

Se realizaron 222 encuestas, de las cuales 202 fueron con respuesta de atención oportuna. Solo 21 encuestados respondieron que los requerimientos no fueron atendidos oportunamente.

50	WBILLMER GRAJALES PUENTES	SECRETARIA DE HACIENDA	2021-06-04 07:53:48	2021-06-05 07:53:59		Luis Enrique Diaz Aranzazu	Asignada (Vencida)	Asignacion Claves CHIP

RIESGO 3. INEFICIENCIA ADMINISTRATIVA POR DESCONOCIMIENTO O FALTA DE FORMACIÓN TI.

El tipo de Riesgo: Operativo
Probabilidad: 4 (Probable)
Impacto: 2 (Menor)
Zona de Riesgo: Alto

Descripción: Riesgo asociado a la falta de actualización y capacitación de los conocimientos en sistemas de información e implementación de la estrategia de gobierno digital en la gobernación del Quindío

Causa 1: Falta de difusión planes y políticas asociadas a la administración y el manejo de la infraestructura tecnológica.

Conclusiones del equipo auditor

Causa 2: Falta de capacitación para la administración y actualización de la infraestructura tecnológica

Control: El Director de Gobierno Digital semestralmente, realizará verificación del Plan de difusión de Planes y políticas de la Secretaría TIC, a través de informe estadístico de consolidación de capacitaciones y/o difusiones. En caso de que encuentre el no cumplimiento del Plan de sensibilización, se realizará reajuste del cronograma establecido. Como evidencia se tendrá el Plan de difusión y cronograma, informes estadísticos y listados de asistencia.

Indicador:

a. *N° de estrategias de difusión implementadas / N° de estrategias programadas en el Plan *100*

b. *N° capacitaciones realizadas / N° de capacitaciones programadas en el Plan *100*

Aplicación:

a. *1 estrategias de difusión implementadas / 1 estrategias programadas en el Plan *100 =* ***100%***

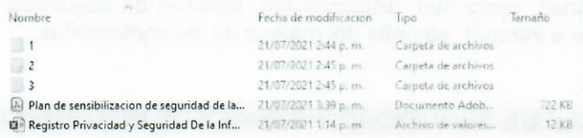
b. *2 capacitaciones realizadas / 2 de capacitaciones programadas en el Plan *100 =* ***100%***

Evidencias:

a. La dirección de gobierno digital de la secretaria TIC elaboro la estrategia para brindar capacitaciones sobre temas de política TIC, seguridad y privacidad de la información y ofimática a los funcionarios de la administración departamental.

b. Mediante oficio S.TIC -62.217.00-0236 la secretaria TIC envía invitación al secretario administrativo para realizar capacitación a los funcionarios y contratistas de la secretaria administrativa en temas de políticas de seguridad y privacidad de la información y ofimática. Dicha capacitación se realizó el día 27 y 29 de abril de 2021, capacitando a 38 personas de la secretaria administrativa y planeación.

También se realizó capacitación del Plan de Sensibilización y Comunicación para la seguridad de la información los días 27 de abril y 04 de mayo de 2021. Se capacitaron 62 personas de varias secretarias de la Gobernación.



Nombre	Fecha de modificacion	Tipo	Tamaño
1	21/07/2021 2:44 p. m.	Carpeta de archivos	
2	21/07/2021 2:45 p. m.	Carpeta de archivos	
3	21/07/2021 2:45 p. m.	Carpeta de archivos	
Plan de sensibilizacion de seguridad de la...	21/07/2021 3:39 p. m.	Documento Adob...	722 KB
Registro Privacidad y Seguridad De la Inf...	21/07/2021 1:14 p. m.	Archivo de valores...	12 KB

Evidencias

RIESGO 4. ADULTERAR, MODIFICAR, SUSTRAER O ELIMINAR DATOS O INFORMACIÓN SENSIBLE, CONFIDENCIAL, CRÍTICA EN BENEFICIO PROPIO O DE TERCEROS.

El tipo de Riesgo: Corrupción
Probabilidad: 2 (Improbable)
Impacto: 5 (Catastrófico)
Zona de Riesgo: Extremo

Descripción: Hace referencia a accesos a las bases de datos no autorizados de los diferentes aplicativos misionales de la entidad y de computadores que manejen información confidencial de la misma.

Conclusiones del equipo auditor

Causa 1: Ofrecimiento de dadivas o presión por parte de un externo o superior para el acceso no autorizado a información

Causa 2: Baja capacitación en los lineamientos de seguridad y privacidad de la información, y las consecuencias de la violación de la ley.

Control: El Director de Gobierno Digital cuatrimestralmente, realizará una capacitación a los funcionarios en el Plan de Seguridad y Privacidad de la Información, así como en las implicaciones legales como sanciones y multas en caso de propiciar vulneración a los sistemas de información de la entidad. En caso de evidenciar que no son suficientes las capacitaciones, se ajustará la periodicidad de las mismas. Como evidencia quedan listados de asistencia, el Plan de Seguridad y Privacidad de la Información y cronograma

Indicador:

*N° capacitaciones realizadas / N° de capacitaciones programadas en el Plan *100*

Aplicación:

*2 capacitaciones realizadas / 2 capacitaciones programadas en el Plan *100* = ***100 %***

Evidencias:

Durante el primer cuatrimestre del año 2021 la secretaria TIC realizo campañas de sensibilización en temas claves como la privacidad y seguridad de la información en distintas jornadas de capacitación a cada una de las secretarias y dependencias adscritas al Centro Administrativo Departamental. Las capacitaciones se realizaron los días 26 y 27 de abril. Allí se explica la normatividad de la estrategia de gobierno digital, temas de seguridad de la información, confidencialidad, integridad, disponibilidad, políticas de seguridad y privacidad de la información en la web, correo electrónico e intranet, además del manejo de las contraseñas.

RIESGO 5. COPIAS DE SEGURIDAD SISTEMAS DE INFORMACION INEXISTENTES

El tipo de Riesgo: Operativo
Probabilidad: 3 (Posible)
Impacto: 3 (Moderado)
Zona de Riesgo: Alto.

Descripción: Riesgo asociado a la falta de copias de seguridad de las bases de datos de los sistemas de información con los que cuenta la entidad, dichas copias se deben realizar diariamente y por la Secretaría TIC.

Causa: Falta de capacitación en el manejo y realización diaria a diferentes funcionarios de la secretaría TIC de las copias de seguridad de las bases de datos

Conclusiones del equipo auditor

Control: La Secretaría TIC, cuenta con una política de respaldo de la información de los servidores de la gobernación, este respaldo se realiza todos los días en discos duros externos que se encuentran en el data center y se replican a la unidad de almacenamiento NAS que se encuentra en el centro de convenciones.

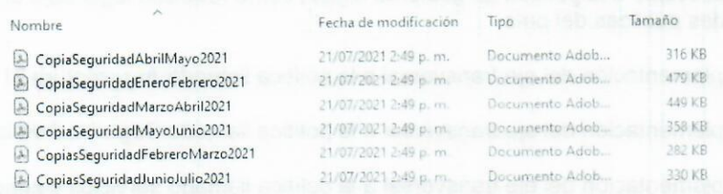
Indicador:

*No. Copias de seguridad a las bases de datos (PCT, Humano, Sevenet, SISCAR) realizadas / No. de copias de seguridad(PCT, Humano, Sevenet, SISCAR) programadas *100*

Aplicación:

*501. Copias de seguridad a las bases de datos (PCT, Humano, Sevenet, SISCAR) realizadas / 648 copias de seguridad(PCT, Humano, Sevenet, SISCAR) programadas *100* = **77.3 %**

Evidencias:



Nombre	Fecha de modificación	Tipo	Tamaño
CopiaSeguridadAbrilMayo2021	21/07/2021 2:49 p. m.	Documento Adob...	316 KB
CopiaSeguridadEneroFebrero2021	21/07/2021 2:49 p. m.	Documento Adob...	479 KB
CopiaSeguridadMarzoAbril2021	21/07/2021 2:49 p. m.	Documento Adob...	449 KB
CopiaSeguridadMayoJunio2021	21/07/2021 2:49 p. m.	Documento Adob...	358 KB
CopiasSeguridadFebreroMarzo2021	21/07/2021 2:49 p. m.	Documento Adob...	282 KB
CopiasSeguridadJunioJulio2021	21/07/2021 2:49 p. m.	Documento Adob...	330 KB

Se recopila la información presentada por la secretaria TIC para revisar la cantidad de backups realizados a los sistemas de información Humano, PCT, Sevenet y Siscar. De acuerdo a los datos presentados se elabora la siguiente tabla:

	MES						PROMEDIO MENSUAL	TOTAL
APLICATIVO	Enero	Febrero	Marzo	Abril	Mayo	Junio		
Humano	24	23	19	26	15	26	22,1	133
PCT	24	23	16	27	26	27	23,8	143
Sevenet	18	19	20	22	21	16	19,3	116
Siscar	18	19	18	12	21	21	18,1	109
TOTAL	84	84	73	87	83	90	83,5	501

Para el cálculo de la formula del indicador, se tiene en cuenta que cada mes se deberían realizar 27 copias de seguridad de cada una de las bases de datos. Para el primer semestre de 2021 se tienen 648 copias de seguridad (4 x 27 x 6 = 648)

En total se realizaron 501 copias de seguridad de los sistemas de información en el primer semestre de 2021.

Conclusiones del equipo auditor

Observaciones:

Teniendo en cuenta que cada mes se deberían realizar 27 copias de seguridad sin contar los días festivos, en algunos meses se puede observar baja cantidad de backups realizados. Para el sistema de información Humano, en el mes de mayo se realizaron 15 copias. Para PCT en el mes de marzo se realizaron 16, para Sevenet en promedio se realizaron 20 copias mensuales y para Siscar en el mes de abril se observa una cantidad muy baja de backups realizados (12). Por esta razón, se solicita a la secretaria TIC ser constante con los backups realizados, los cuales deben ser diarios. Aunque se observa una mejoría comparado con el seguimiento del periodo anterior.

RIESGO 6. POLITICA DE GOBIERNO DIGITAL CON BAJA IMPLEMENETACION

El tipo de Riesgo: Operativo
Probabilidad: 4 (Probable)
Impacto: 3 (Moderado)
Zona de Riesgo: Alto

Descripción: Riego asociado a la política de gobierno digital, como requisito legal bajo el decreto 2008 de 2018 para todas las entidades públicas del país.

Causa 1: Falta de implementación del eje transversal a la política llamado Arquitectura TI

Causa 2: Falta de implementación del eje transversal a la política llamado Seguridad de la información

Causa 3: Falta de implementación del eje transversal a la política llamado servicios ciudadanos digitales

Control: A través de la dirección de gobierno digital se pretende dar seguimiento a la implementación de la política de gobierno digital en la gobernación del Quindío a través de la creación y/o actualización de planes y/o políticas correspondientes a la estrategia

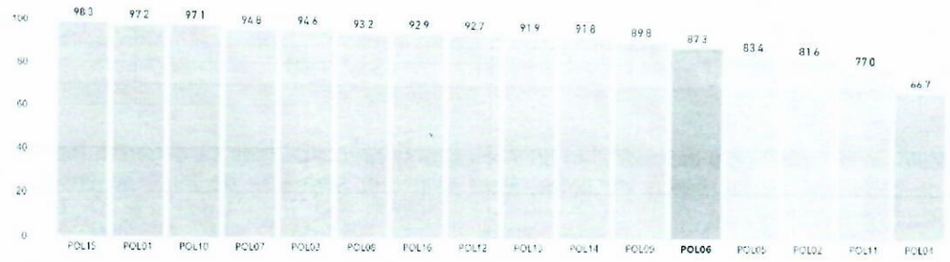
Indicador:

a) Indice de implementación de la política de gobierno digital en la entidad

Aplicación:

a) Indice de implementación de la política de gobierno digital en la entidad = 87,3 %

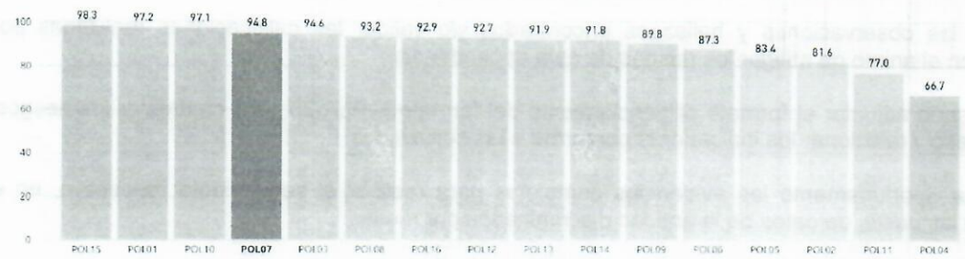
Evidencias:



Nota: Los colores en este gráfico representan un ranking de las políticas según los puntajes obtenidos. No necesariamente determinan un alto o bajo desempeño.

POL06: Gobierno Digital

Conclusiones del equipo auditor



Nota: Los colores en este gráfico representan un ranking de las políticas según los puntajes obtenidos. No necesariamente determinan un alto o bajo desempeño.

POL07: Seguridad Digital

La secretaria TIC lleva a cabo la implementación de la estrategia de gobierno digital de la gobernación del Quindío a través de la dirección de gobierno digital. El índice de cumplimiento de esta estrategia se realiza a través del Furag, el cual se realiza cada año.

3. Hallazgos de auditoría:

En general la secretaria TIC cumplió con los indicadores del Mapa de Riesgos con porcentajes altos. Para el riesgo 5 (copias de seguridad de sistemas de información) el porcentaje de cumplimiento fue de 77.3%. En este riesgo se recomienda realizar las copias de seguridad de cada uno de los sistemas de información a diario, para evitar perdida de información.

Tipo	Requisito	Descripción
Observación 1	Riesgo 1. Hurto de sistemas de información en custodia de la secretaria TIC. Se debe realizar control e inventario físico.	Para este riesgo se realizan controles del inventario mediante software, pero es importante recordar que también se deben seguir realizando controles físicos, tanto al ingreso como a la salida del personal del Centro Administrativo Departamental para evitar que se cometa el hurto. Si bien los sistemas de información están bien resguardados, se deben implementar controles o visitas para verificar el estado y la seguridad de los sistemas de información con el fin de prevenir los hurtos y actuar antes de que sucedan.
Observación 2	Riesgo 5. Copias de seguridad sistemas de información inexistentes.	Los backups realizados a los sistemas de información Humano y PCT se encuentran aceptables, pero se debe procurar por mejorar la cantidad de copias de seguridad realizadas a los sistemas de información Sevenet y Siscar. En algunos meses se nota una baja sustancial en las copias de seguridad realizadas, por esto se recomienda realizarla a cada uno de los sistemas a diario.

4.Recomendaciones para auditorías posteriores

- Atender las observaciones y hallazgos encontrados y/o validar las calificaciones realizadas por el equipo Auditor, con el ánimo de mitigar los riesgos de esta dependencia.

- Es necesario adjuntar el formato diligenciamiento del formato F-PLA-25 para contrastar los riesgos inherentes en el proceso y relacionar los indicadores conforme a las actividades.

- Presentar oportunamente las evidencias completas para realizar el seguimiento respectivo, en especial los backups a las bases de datos de la entidad discriminados por meses.

AUTORIZACIÓN PARA COMUNICAR ESTE INFORME:
Este informe se comunicará después de la auditoría únicamente a los procesos involucrados y no será divulgado a terceros sin su autorización.

Nombre completo	Responsabilidad	Firma
José Duván Lizarazo Cubillos	Auditor Líder	
Carlos Andres Lozano Valencia	Equipo Auditor -OCIG	

ELABORACIÓN	REVISIÓN	APROBACIÓN
Elaborado por: Henry Giraldo Gallego	Revisado por: Martha Liliana Agudelo Valencia	Aprobado por: Martha Liliana Agudelo Valencia
Cargo: Profesional Universitario	Cargo: Secretario de Despacho	Cargo: Secretario de Despacho