Valledupar, Octubre 15 de 2026

OCI SIVA SAS - Oficio N° 090 del 2026

Doctor:
LUIS GABRIEL ARIAS RIVERA
Gerente (s)
Sistema Integrado de Transporte de Valledupar SIVA S.A.S

ASUNTO: INFORME DEFINITIVO DE AUDITORIA INTERNA BASADA EN RIESGOS PROCESO GESTIÓN TICS EMITIDO POR LA OFICINA DE CONTROL INTERNO VIGENCIA 2026.

Cordial saludo;

Teniendo en cuenta los lineamientos sobre auditoría interna determinados por el Instituto de Auditores Internos –IIA Global, recopiladas en la Guía de Auditoría para Entidades Públicas Versión 4. Mayo de 2020, del Departamento Administrativo de la Función pública DAFP en la Fase 4. Informe de auditoría (comunicación de resultados), en esta fase se presentan los resultados de la auditoría a través de un informe de auditoría y se suscriben los planes de mejoramiento, la norma 2440 establece que el director ejecutivo de auditoría (jefe de Control Interno) debe comunicar los resultados a las partes apropiadas y agrega en la interpretación lo siguiente, por tanto, el jefe de la oficina de Control Interno debe asegurarse de que los informes de auditoría interna lleguen a los usuarios y partes interesadas dentro de la entidad, así mismo, de que tomen las medidas correspondientes para subsanar las causas de las observaciones encontradas a través de un Plan de Mejoramiento.

Teniendo en cuenta el decreto 648 de 2017 Articulo 2.2.21.4.7. Relación administrativa y estratégica del Jefe de Control Interno o quien haga sus veces, Parágrafo 1. Los informes de auditoría, seguimientos y evaluaciones tendrán como destinatario principal al representante legal de la entidad y al comité de coordinación de control interno y/o comité de auditoría y/o junta directiva, y deberán ser remitidos al nominador cuando *éste lo requiera.*

Por lo anterior se hace entrega del Informe definitivo de auditoria interna basada en riesgos del Proceso de **GESTIÓN TICS** emitido por la oficina de control interno, vigencia 2026, para su respectivo conocimiento, revisión y aprobación. Se solicita enviar el plan de mejoramiento con las acciones correctivas y de mejora, este plan de mejoramiento deberá ser elaborado por los responsables del proceso y estará sujeto a seguimiento por parte de la oficina de control interno.

Anexo, 19 folios
Atentamente;

ORIGINAL FIRMADO
MARIA ANGELICA GONZALEZ OÑATE
Jefe de Oficina Control Interno
Sistema Integrado de Transportes de Valledupar SIVA S.A.S

SISTEMA INTEGRADO DE TRANSPORTE DE VALLEDUPAR SIVA S.A.S
OFICINA DE CONTROL INTERNO

INFORME DEFINITIVO AUDITORIA INTERNA BASADA EN RIESGOS EMITIDO POR LA OFICINA DE CONTROL INTERNO
PROCESO GESTION TICS
VIGENCIA 2026

VALLEDUPAR, CESAR
OCTUBRE 15 DE 2026

TABLA DE CONTENIDO

1. DATOS GENERALES…… 3
2. .OBJETIVO DE LA AUDITORIA……3
3. ALCANCE DE LA AUDITORIA……3
4. CRITERIOS DE LA AUDITORIA……3
5. METODOLOGIA DE LA AUDITORIA INTERNA…… 5
6. RESUMEN EJECUTIVO…… 8-11
7. MAPA DE RIESGO POR PROCESOS…….. 11
8. PLAN DE ACCION……..……13
9. INDICADORES DE GESTION…… 13
10. DESARROLLO DE LA AUDITORIA…… 13
11. RECOMENDACIONES……26
12. CONCLUSIONES…… 34
13. ANEXOS…… 36

1. DATOS GENERALES

FECHA DE EMISIÓN DEL INFORME	Día:	15	Mes:	10	Año:	2026

Aspecto Evaluable (Unidad Auditable):	Proceso Gestión TICS
Líder de Proceso / Jefe(s) Dependencia(s):	RICARDO CORRALES RIVERA Líder Proceso GESTIÓN ADMINISTRATIVA Alvaro Rosado Proceso Gestión TICS
2.OBJETIVO DE LA AUDITORÍA:	Evaluar la efectividad del control interno y la aplicación de los controles dentro del proceso de GESTIÓN TICS Evaluar la conformidad del Sistema de Gestión de Calidad de la SISTEMA INTEGRADO DE TRANSPORTES DE VALLEDUPAR SIVA, con base los requisitos de la NTC ISO 9001:2015, MIPG y las disposiciones planificadas en los procesos. Verificar el nivel de implementación del Sistema de Gestión de Calidad de la SISTEMA INTEGRADO DE TRANSPORTES DE VALLEDUPAR SIVA, verificando su cumplimiento y con el fin de contribuir a la Mejora Continua del S.G.C. Identificar oportunidades de mejora
3.ALCANCE DE LA AUDITORÍA:	Inicia con la administración, soporte y monitoreo de los servicios existentes en la infraestructura tecnológica, incluye definición de políticas informáticas, continua con la identificación de necesidades tecnológicos y finaliza con la adquisición herramientas de software y hardware requeridas Se evaluará la gestión de la vigencia 2026
4.CRITERIOS DE LA AUDITORÍA:	Modelo Integrado de Planeación y Gestión: Dimensión Gestión con valores, Mapa de riesgos, Plan de mejoramiento por procesos e institucional, Ley 1712 de 2014 Transparencia y acceso a la información pública, indicadores, Plan de acción, Manual de procesos y Procedimientos, y Normatividad Vigente aplicable. NTC ISO 9001:2015 41. 4.2, 4.4; 5.2, 6.1, 6.2, 6.3, 7.1; 7.2, 7.3, 7.5, 9.1, 10.1, 10.2, 10.3 Dimensión 4 Fortalecimiento Institucional Política de seguridad digital Dimensión3 Relación Estado – Ciudadanías Política de transparencia y acceso a la información, política Gobierno digital.

Reunión de Apertura						Ejecución de la Auditoría		Reunión de Cierre					
Día	5	Mes	10	Año	2026	Desde	Hasta	Día	9	Mes	10	Año	2026
						5/10/2026	9/10/2026						

Jefe oficina de Control Interno	Auditor Interno
MARIA ANGELICA GONZALEZ OÑATE	ORIGINAL FIRMADO

5. METODOLOGIA Y DESARROLLO DE LA AUDITORIA INTERNA

El Modelo Integrado de Planeación y Gestión (MIPG), definido como un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar las actividades de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resolver las necesidades y problemas de los ciudadanos con integridad y calidad en el servicio. Integra a través de la séptima dimensión la política de Control Interno, mediante la estructura del Modelo Estándar de Control Interno MECI, la herramienta base para la implementación y fortalecimiento del Sistema de Control Interno de las entidades.

El Modelo Integrado de Planeación y Gestión – MIPG constituye el marco de referencia para orientar la gestión de las entidades y organismos públicos hacia la generación de resultados con valor público, en condiciones de integridad, calidad, eficiencia y orientación al servicio de las ciudadanías. Su propósito es facilitar que la gestión institucional se traduzca en bienes y servicios que garanticen los derechos, atiendan las necesidades de los grupos de valor, fortalezcan la confianza en las instituciones y contribuyan al cumplimiento de los fines del Estado. El presente Manual Operativo, en su versión 7, actualiza los lineamientos para la implementación del MIPG a partir de los ajustes realizados a la estructura del Modelo, la reorganización de sus dimensiones operativas, la reubicación de algunas políticas dentro del esquema de operación, y la incorporación de una nueva política de gestión y desempeño institucional. Esta actualización responde, además, a los cambios introducidos en la metodología de Medición del Desempeño Institucional – MDI y en el Formulario Único de Reporte de Avances de la Gestión – FURAG, cuyo instrumento se orienta principalmente a identificar los resultados derivados de la implementación del Modelo y de sus políticas

las oficinas de control interno se definen como “uno de los componentes del Sistema de Control Interno, de nivel gerencial o directivo, encargado de medir y evaluar la eficiencia, eficacia y economía de los demás controles, asesorando a la dirección en la continuidad del proceso administrativo, la reevaluación de los planes establecidos y en la introducción de los correctivos necesarios para el cumplimiento de las metas u objetivos previstos”. En este sentido, el artículo 12 establece sus funciones, las cuales se orientan a verificar la eficiencia y efectividad de la estructura de control definida por cada entidad; velar por el cumplimiento de las leyes, normas, políticas, procedimientos, planes, programas, proyectos y metas de la entidad, y recomendar los ajustes necesarios; aplicar mecanismos de evaluación independiente (auditoría interna) que permita generar hallazgos y análisis con un enfoque basado en riesgos que prevenga la afectación al patrimonio público; así como establecer escenarios de relacionamiento claves que les permita servir de apoyo a los directivos en el proceso de toma de decisiones, con el fin de que se obtengan los resultados esperados y se garantice el cumplimiento misional

De acuerdo con el artículo 17 del Decreto 648 de 2017, dichos roles son: liderazgo estratégico, enfoque hacia la prevención, evaluación a la gestión del riesgo, evaluación y seguimiento y, relación con entes externos de control. A través de este rol de evaluación y seguimiento, las unidades de control interno, auditoría interna o quien haga sus veces deben desarrollar una actividad de evaluación de manera planeada, documentada, organizada, y sistemática, con respecto a las metas

estratégicas de gran alcance (mega), resultados, políticas, planes, programas, proyectos, procesos, indicadores, y riesgos, que la entidad ha definido para el cumplimiento de su misión, en el marco del sistema de control interno. Es importante resaltar que este rol debe desarrollarse de manera objetiva e independiente.

En el marco de las funciones establecidas en el artículo 12 de la Ley 87 de 1993, las cuales, como se ha indicado en el numeral A, se orientan a verificar la eficiencia y efectividad de la estructura de control definida por cada entidad; velar por el cumplimiento de las leyes, normas, políticas, procedimientos, planes, programas, proyectos y metas institucionales, y recomendar los ajustes necesarios; mediante el artículo 2.2.21.5.3 del Decreto 1083 de 2015 define cinco roles que permiten enfocar su labor en temas clave que facilitan su relacionamiento interno y externo, así como para priorizar sus análisis con alcance en la gestión del riesgo, a través de los siguientes roles: i) liderazgo estratégico; ii) enfoque hacia la prevención, iii) evaluación de la gestión del riesgo; iv) evaluación y seguimiento y v) relación con entes externos de control, cuyo detalle se podrá consultar en la Guía rol de las unidades u oficinas de control interno, auditoría interna o quien haga sus veces, versión 3 de septiembre 2023.

Como parte de la actualización, las normas definen para las entidades del Sector Público lo siguiente: *Si bien las Normas Globales de Auditoría Interna se aplican a todas las funciones de auditoría interna, los auditores internos del sector público trabajan en un entorno político bajo estructuras de gobernanza, organización y financiamiento que pueden diferir de las del sector privado. La naturaleza de estas estructuras y las condiciones relacionadas pueden verse afectadas por la jurisdicción y el nivel de gobierno en el que opera la función de auditoría interna. Además, parte de la terminología utilizada en el sector público difiere de la del sector privado. Estas diferencias pueden afectar la forma en que las funciones de auditoría interna en el sector público aplican las Normas. La sección "Aplicación de las Normas Globales de Auditoría Interna en el Sector Público", que sigue al Dominio V: Prestación de Servicios de Auditoría Interna, describe las estrategias para la conformidad en medio de las circunstancias y condiciones únicas de la auditoría interna en el sector público. A través de esos mandatos, las funciones de auditoría interna del sector público suelen estar obligadas a centrarse en: i) Garantizar el cumplimiento de las leyes y/o reglamentos; ii) Identificar oportunidades para mejorar la eficiencia, eficacia y economía de los procesos y programas gubernamentales; iii) Determinar si los recursos públicos están adecuadamente salvaguardados y utilizados adecuadamente para prestar servicios de manera equitativa; iv) Evaluar si el desempeño de una organización se alinea con sus objetivos y metas estratégicas. (IIA Global, 2024).*

En este sentido, la auditoría interna se define de la siguiente manera: Una actividad independiente y objetiva de aseguramiento y asesoramiento diseñada para añadir valor a las operaciones de una organización. Ayuda a la organización a cumplir sus objetivos, aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gobierno, gestión de riesgos y control. (The IIA Global, glosario, 2024, p. 7). Se tiene entonces que, la auditoría interna mejora los siguientes aspectos de una entidad:

- El logro satisfactorio de sus objetivos

- La gestión institucional, la gestión de riesgos y el control
- La toma de decisiones, el monitoreo y el seguimiento
- La reputación y la confianza con los grupos de valor
- Su capacidad para servir al interés público (IIA Global, 2024, p. 11)

De este modo, como conclusión del desarrollo del Dominio I, los equipos de las Oficinas de Control Interno deberían comprender que la auditoría interna cumple su propósito cuando contribuye al logro de los objetivos institucionales y fortalece la capacidad de las entidades para crear, proteger y mantener el valor público (IIA Global, 2024). Para este efecto, en cuanto a los servicios de auditoría interna, su alcance abarca todos los procesos de la entidad, incluidas todas las actividades, activos y personal, a los cuales aplica, dependiendo del análisis realizado sobre el universo de auditoría.

Por lo tanto, los jefes de control interno, así como los miembros de su equipo (en los casos en que se disponga de estos), están llamados a observar las disposiciones normativas y reglamentarias en materia de integridad pública, al conocer, interiorizar y demostrar la integridad en su trabajo a través de sus comportamientos, alineados con los valores del Código de Integridad del Servicio Público Colombiano, el cual se constituye en el marco principal para la adhesión a los principios y reglas de conducta establecidos por las NOGAI™ (2024).

Estatuto de Auditoría Interna13, definido como un documento obligatorio, aprobado por el Comité Institucional de Coordinación de Control Interno que, adopta el propósito, autoridad y responsabilidad que se reconocerá a la función de auditoría interna para asegurar que cumpla su mandato.
En desarrollo de este dominio, los documentos mínimos obligatorios para la planeación, operación y seguimiento de la función de auditoría interna, adicionales a los descritos en el Artículo 2.2.21.4.8 del Decreto 1083 de 2015, son los siguientes:

a. Compromiso ético, conocimiento y adhesión a la integridad pública y profesionalidad del auditor interno.
b. La declaración de conflicto de interés.
c. Estatuto de auditoría interna.
d. Evaluaciones de calidad de la función de auditoría interna.
e. Estrategia de auditoría interna.
f. Universo de auditoría basado en riesgos
g. Plan anual de auditoría.
h. Carta de representación.
i. Entendimiento de la unidad auditable y/o matriz de evaluación preliminar de riesgos y controles.
j. Carta de compromiso. j. Programa de trabajo
k. Papeles de trabajo que evidencien la ejecución de las pruebas de auditoría interna aprobadas en el programa de trabajo.
l. Informe ejecutivo.
m. Informe detallado

En desarrollo de esta estrategia, la función de auditoría interna desplegará anualmente sus fases operativas: (i) planeación anual, (ii) planificación basada en riesgos, (iii) ejecución, (iv) comunicación de resultados y (v) seguimiento a planes de mejoramiento, bajo el enfoque transversal del Programa de Aseguramiento y Mejora de la Calidad (PAMC), como elemento estructural para garantizar la calidad, consistencia y mejora continua de la actividad.

Según la *Guía para la Gestión Estratégica y el Fortalecimiento de la Auditoría Interna en Entidades Públicas* Versión 5 de 2026, con su respectiva caja de herramientas se debe tomar en consideración las siguientes claridades: Plan Anual de Auditoría basado en riesgos de la vigencia 2026, el cual fue presentado y aprobado por el Comité Institucional de Coordinación de Control Interno, programa de trabajo de auditorías internas de gestión, informes de ley y actividades de seguimiento y acompañamiento que la oficina de control interno de SIVA desarrolló en la vigencia 2026.

Para dar inicio al proceso auditor, se seleccionó un equipo auditor teniendo en cuenta la competencia necesaria para lograr los objetivos de la auditoría. Para la escogencia del equipo auditor se tuvo en cuenta la objetividad, con el fin de que los auditores no auditaran procesos de los cuales hicieren parte en sus actividades diarias, asegurando así la independencia del equipo auditor con respecto a las actividades a auditar y evitando conflicto de intereses. Se estableció contacto con los auditados a través de comunicaciones en las que se le informaba el plan de trabajo de la auditoría interna, las fechas y horas para auditar sus procesos, además de los auditores asignados a las auditorías de cada uno de ellos.

Se dio inicio al desarrollo del Programa de trabajo de Auditorías internas en una reunión de inicio con el jefe de proceso, donde el líder auditor confirmó el plan de trabajo para cada auditoría por proceso y proporcionó un breve resumen de la metodología para llevar a cabo las actividades de la auditoría, sin dejar de lado la oportunidad que se le da a los auditados de manifestar sus inquietudes frente al objetivo, alcance y criterios de las mismas. Luego se procedió a cada dependencia a auditar, el equipo auditor recopiló y verificó la información (registros, procedimientos, indicadores, actividades, etc.), a través de entrevistas, cuestionarios, revisión documental, entre otras técnicas de auditoría legalmente establecidas e indicadas en la metodología. Se generaron hallazgos que fueron comunicados, para obtener el reconocimiento de las evidencias de la auditoría y que las no conformidades hubieren sido comprendidas. Dentro del proceso de auditoría interna se realizó la verificación transversal de los siguientes temas: conocimiento del direccionamiento estratégico, plan de acción, seguimiento mapa de riesgos por procesos, Seguimiento plan de mejoramiento Institucional y por procesos, indicadores de gestión, incluidos en el plan de trabajo de la auditoría interna. El informe de auditoría interna fue elaborado por la Oficina de Control Interno, el cual será presentado al Comité Institucional de Coordinación de Control Interno y hechas sus recomendaciones, se debe dar a conocer a los responsables y líderes de los procesos para que formulen un Plan de Mejoramiento que contenga las acciones correctivas y de mejora necesarias, para que el proceso subsane las inconsistencias, no conformidades y observaciones detectadas en la auditoría, sin dejar de lado las acciones establecidas en el plan de mejoramiento resultante de las auditorías internas realizadas en vigencias anteriores.

6. RESUMEN EJECUTIVO:

AUDITORIA INTERNA BASADA EN RIESGOS AL PROCESO DE GESTIÓN DE TICS

OBJETIVO DE LA AUDITORÍA:

Evaluar la efectividad del control interno y la aplicación de los controles dentro del proceso de GESTIÓN TICS

Evaluar la conformidad del Sistema de Gestión de Calidad de la SISTEMA INTEGRADO DE TRANSPORTES DE VALLEDUPAR SIVA, con base los requisitos de la NTC ISO 9001:2015, MIPG y las disposiciones planificadas en los procesos.

Verificar el nivel de implementación del Sistema de Gestión de Calidad de la SISTEMA INTEGRADO DE TRANSPORTES DE VALLEDUPAR SIVA, verificando su cumplimiento y con el fin de contribuir a la Mejora Continua del S.G.C.

Identificar oportunidades de mejora

ALCANCE DE LA AUDITORÍA:

Inicia con la administración, soporte y monitoreo de los servicios existentes en la infraestructura tecnológica, incluye definición de políticas informáticas, continua con la identificación de necesidades tecnológicos y finaliza con la adquisición herramientas de software y hardware requeridas
Se evaluará la gestión de la vigencia 2026.

6.1. GENERALIDADES:

AUDITORIA INTERNA AL PROCESO DE GESTION TIC

Prestar servicios de apoyo relativos a los sistemas informáticos tales como: salvaguardar la memoria institucional, realizar mantenimientos preventivos y correctivos, asesorar a los funcionarios en el manejo de los equipos informáticos y los softwares, atender las necesidades de las diferentes dependencias y velar por la implementación y administración de aplicaciones funcionales y misionales de SIVA.

Se inicia el proceso auditor con la presentación del equipo de trabajo conformado así:

Líder del Proceso: RICARDO CORRALES RIVERA- PROFESIONAL GESTION ADMNISTRATIVA

ÁLVARO JOSÉ ROSADO QUINTERO
CONTRATO DE PRESTACION DE SERVICIOS PROFESIONALES N PSP-021-2026
PRESTACION DE SERVICIOS PROFESIONALES COMO INGENIERO ELECTRONICO PARA BRINDAR ACOMPAÑAMIENTO, SOPORTE Y GESTION TÉCNICA EN LA ADMINISTRACIÓN, OPERACIÓN, MANTENIMIENTO Y MEJORA DE LA INFRAESTRUCTURA TECNOLÓGICA Y DE LOS SISTEMAS ELECTRONICOS, ELÉCTRICOS Y DE TELECOMUNICACIONES QUE REQUIERA SIVA SAS
PLAZO OCHO 8 MESES
ACTA MODIFICATORIA NO 001 PRÓRROGA Y ADICIÓN VER N: FECHA 23/12/2016 NO PSP.021-2026 Prorrogar por UN término de TRES (03) MESES Y CINCO (5) DIAS CALENDARIOS,

6.2. DOCUMENTOS ENTREGADOS:

1. Caracterización
2. Procedimientos
3. Copia de contratos de prestación de servicios de los profesionales de Gestión TICS.
4. Plan de Acción y su ejecución
5. Indicadores de Gestión y su ejecución
6. Mapa de riesgos del proceso, acciones ejecutadas.
7. Política de gobierno y seguridad digital
8. Política de protección de datos personales
9. Política de seguridad información (actualizada)
10. Plan estratégico de tecnologías de la información PETI 2025-2027
11. Modelo de seguridad digital MSPI
12. Plan de tratamiento de riesgos de la información
13. Plan de seguridad de la información actualizado
14. Plan de mantenimiento de equipos y su ejecución
15. Ficha técnica de equipos
16. Registro de Copias de seguridad evidencia
17. Matriz de cumplimiento de ley transparencia y acceso a la información

CONTEXTO DE LA ORGANIZACIÓN:

COMPRENSION DE LA ORGANIZACIÓN Y SU CONTEXTO

ANALISIS DOFA:

DEBILIDADES:

- ✓ Infraestructura física obsoleta y no cubre las necesidades de la operación
- ✓ Insuficiente talento humano.
- ✓ Desconocimiento de las mejores prácticas en ITI
- ✓ Poca inversión en tecnología

OPORTUNIDADES:

- ✓ Apoyo de entidades, cooperación horizontal de apoyo tecnológicos.
- ✓ Capacitaciones externas realizadas.
- ✓ Acceso a tecnologías de la información, aplicativos de las entidades del orden nacional
- ✓ Marcos conceptuales de Arquitectura de TI.
- ✓ Intercambio de conocimientos y herramientas tecnológicas para fortalecer los procesos internos.

FORTALEZA:

- ✓ Talento humano con capacidades profesionales que favorecen al área.
- ✓ Aprendizaje continúo.
- ✓ Sistema de seguridad informática (Antimalware y Sistema de protección perimetral)

AMENAZAS:

- ✓ Cambio de políticas nacionales del Min TIC
- ✓ Ruptura de relaciones comerciales entre el Estado o la entidad con proveedores de servicios tecnológicos
- ✓ Cambio de regulaciones internacionales en materia de tecnologías
- ✓ Ataques cibernéticos.
- ✓ Fuga de información
- ✓ Daño a la propiedad que afectan los centros de cómputo.

IDENTIFICACIÓN Y PRIORIZACIÓN DE LOS REQUISITOS, NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

Se realizó la revisión de la matriz de partes interesadas (cliente, cliente interno, socios, gobierno, Proveedores Externos, personas naturales o jurídicas que suministran un bien o prestan un servicio requerido y entes de control).

ANALISIS DE PARTES INTERESADAS:

Ministerio de tecnologías de la información y las comunicaciones (MINTIC)
Entes de Control,
Usuarios,
Gestor Externo (contratista)
Proveedores de infraestructura tecnológica

SISTEMA DE GESTION DE LA CALIDAD Y SUS PROCESO

Se evidencia caracterización VERSIÓN: 3.0 FECHA: 30/09/2025

TIPO DE PROCESO	APOYO	
NOMBRE DEL PROCESO	GESTIÓN DE TIC'S	
RESPONSABLE	PROFESIONAL DE GESTION DE PLANEACIÓN	
OBJETIVO	Prestar servicios de apoyo relativos a los sistemas informáticos tales com salvaguardar la memoria institucional, realizar mantenimientos preventivos correctivos, asesorar a los funcionarios en el manejo de los equipos informáticos los softwares, atender las necesidades de las diferentes dependencias y velar por implementación y administración de aplicaciones funcionales y misionales de SIVA	
ALCANCE	Inicia con la administración, soporte y monitoreo de lo servicios existentes en la infraestructura tecnológica incluye definición de políticas informáticas, continu con la identificación de necesidades tecnológicos finaliza con la adquisición herramientas de software hardware requeridas	**DEPENDENCIAS INVOLUCRADAS** Todas las Dependencias

7. MAPA DE RIESGOS

Identificación del riesgo				Análisis del riesgo inherente			Evaluación del riesgo Valoración de los controles		Plan de Acción		
Causa	Riesgo	Consecuencias	Clasificación del Riesgo	Probabilidad Inherente	%	Zona de Riesgo Inherente	No. Control	Descripción de Control	Plan de Acción	Seguimiento	Estado
obsolencia de quipos perdida de capacidad operativa	Posibilidad de afectación económica por daños permanentes o temporales en las herramientas tecnológicas de la entidad, a causa de un uso indebido, obsolescencia de estos, o falta de mantenimiento preventivo	Daños en los equipos. Aumento de los gastos por mantenimientos correctivos perdida la informacion	Tecnológicos	Media	60%	Moderado	1	Programa de mantenimiento de equipos	Implementación del programa de mantenimiento prevent de equipos	Durante el segundo semestre de la vigencia, se realizaron los mantenimientos preventivos programados a los equipos de cómp y demás elementos de la infraestructura tecnológica, de acuer con el cronograma establecido, con e propósito de garantizar su adecuado funcionamiento, disponibilidad, rendimiento y continuidad de las actividades institucionales.	finalizado
Uso indebido de los equipos tecnologicos la entidad.							2	seguimiento al buen uso de los equipos	Implementación del programa de mantenimiento prevent de infraestructura TICS	El programa se encuentra implementado, y se esta ejecutando según lo estipulado. En la nueva sede se esta ejecutando el CONTRATO DE SRESTACION DE SERVICIOS DE APOYO A LA GESTION N' PSAG.052-2026 SIVA SA.s Y JAVIER ALFONSO YANCE SUAREZ6, CONTRATO DE SRESTACION DE SERVICIOS DE APOYO A LA GESTION N' PSAG.052-2026 SIVA SA.s Y JAVIER ALFONSO YANCE SUAREZ	finalizado
empleados con entrenamiento deficiente, , descontentos, malintencionados, negligentes, deshonestos o despedidos. perdida de equipos funcionarios que suministren informac a personas ajenas al entidad	Posibilidad de afectación reputacional y económica por corrupción debido a la eliminación, alteración o uso de información confidencial de la entidad en beneficio propio o de un tercero.	Detrimento patrimonial. Fallas en las operaciones del servicio deficiente prestacion del servicio uso indebido de la informacion para benefciio de terceros Perdida de informacion institucional. Hallazgos disciplinarios y/o fiscales.	Corrupción	Alta	80%	Alto	1	comtrol de acce seguro a los sistemas operativos	Mejorar la seguridad d la información almacenada en los equipos de la entidad a traves de la Implementación de la politica de seguridad d información.	La actividad se encuentra implementada y en desarrollo, conforme a lo establecido. Se realizan copias de seguridad, mantenimientos y almacenamiento digital de la información mediante discos duros y servicios en la nube, contribuyendo a su disponibilidad, integridad y conservación.	En curso
							2	Copia de informacion operativa en la nube	Asignacion de usuarios de seguridad de informacion y creación correos electrónicos intitucionales para resguardar la informaci relevante de la entidad	La entidad cuenta con cuentas de correo electrónico institucional asignadas a los funcionarios y contratistas, de acuerdo con las necesidades y áreas de trabajo. Asimismo, se cuenta con el servicio contratado y disponible para la creación y asignación de nuevas cuentas de correo institucional cuando sean requeridas, garantizan la disponibilidad de este recurso para el desarrollo de las actividades institucionales.	Finalizado

Virus informaticos Daños en los equipos. Software sin licencias originale Deficientes capacitaciones er seguridad informatica Uso inadecuado los sistemas de información de la entidad No se realizan Backups de la información Errores en realización de backups Deficiente person tecnico para los procesos de TICS deficiente infraestructura tecnologica	Posibilidad de afectación reputacional y economica debido a perdida o daño la información a causa de fallos tecnologicos que interrumpen o dañan los sistemas de información.	Reprocesos de las actividades Fallas en las operaciones del servicio deficiente prestacio del servicio uso indebido de la informacion para benefciio de tercero Sanciones legales, disciplinarias y penales Perdidas economica Violación de la infraestructura tecnolgica Perdida de la credibilidad en la entidad	Tecnológicos	**Alta**	80%	**Alto**	1	Copia de seguridad	Realizar backups de la información que sea desee soportar en medios electronicos/digitales.	Se realizan copias de seguridad (backups) de la información institucional que requiere respaldo en medios electrónicos y digitales, utilizando medios de almacenamiento físico y servicios en la nube, de acuerdo con las necesidades de la entidad. Esta actividad permite conta con mecanismos de respaldo para facilitar la recuperación y conservacio de la información ante posibles pérdidas o incidentes.	En curso
							2	Mantenimiento a software Mantenimiento c equipos	Realización de capacitacion en seguridad digital	En el segundo semestre del año se realizaran las 3 capacitaciones programadas por el area de TIC´s. Accesibilidad Web, Seguridad Digital, gobierno Digital:	En curso
							3	Politicas de seguridad y privacidad de la información	Adquisición de antivirus para seguridad de la información mitigar la probabilidad de perdida de la información,	Contrato # PS-075-2025 Objeto: Contratar el mantenimiento tecnológicas, adquisición de licencias microsoft, y demás licencias requerid para el fortalecimiento institucional d sistema integrado de transporte publ de valledupar siva s.a.s.	En curso

8. INDICADORES DE GESTIÓN CORTE 30 DE JUNIO :

PROCESO GESTION TICS					
Objetivos	Realizar las actividades de Gestión Tecnológicas y de Información necesarias para dar operatividad al Sistema Integrado del transporte público de la ciudad de Valledupar SIVA S.A.S.				
INDICADOR	**ACCIONES**	**INDICADOR**	**META**	**%**	**ANALISIS DE DATOS**
Cumplimiento del plan de mantenimiento	Plan de mantenimiento	(Nº total de mantenimientos ejecutados / Nº tota de mantenimientos programados) x 10	100%	100%	En el segundo semestre del año se realizaron los matenimientos preventivos a los equipos de computo qu en su totalidad son 27, y 5 impresoras Se realizó limpiez general de la impresora retirando polvo, residuos de pap y suciedad acumulada en las superficies externas y componentes accesibles del equipo. Esta actividad se efectuó con el propósito de conservar la impresora en adecuadas condiciones de limpieza, contribuir a su correcto funcionamiento, prevenir posibles inconveniente durante la operación y mantener una adecuada calidad d impresión.
Soporte Técnico	Procedimiento soporte técnico	(Nº solicitudes por requerimientos técnicos atendidos Nº solicitudes por requerimientos técnicos solicitados X 100	100%	100%	En el segundo semestre del año se han realizado cuatro servicios de soprte tecnico requerido, todas han sido par las impresoras a las que ha tocado cambiarle piezas que se han desgastado por el uso.
Página Web de la entidad	Publicaciones de página WEB	(Nº Solicitudes a Realizar / Nº Solicitudes Realizadas) X 100	100%	100%	Las publicaciones en la pagina WEB, que se han realizado durante el segundo semestre

Gobierno Digital	Capacitaciones Gobierno Digital	(Nº Capacitacion Realizadas/ Capacitaciones Establecidas) X 10	10%	0%	En el segundo semestre del año se realizaran las capacitaciones programadas por el area de TIC Accesibilidad Web, Seguridad Digital: gobierno Digital:

9. DESARROLLO DE LA AUDITORIA :

PLANEAR :

DEFINICIÓN DE POLÍTICAS Y LINEAMIENTOS PARA LA SEGURIDAD DE LA INFORMACIÓN DE LA ENTIDAD.

Se evidencia en la página web de la entidad los documentos referentes a la planeación del proceso de Gestión de TICS así: link Gestión tecnológica https://siva.gov.co/planes-institucionales/#244-605-gestion-tecnologia-de-la-informacion

PLAN ESTRATÉGICO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI 2025-2028 VERSIÓN: 1.0 FECHA: 30/09/2021
https://siva.gov.co/download/605/gestion-tecnologia-de-la-informacion/15013/plan-estrategico-de-las-tecnologias-de-las-comunicaciones-y-la-informacion-2025-2028-v2-4.pdf

PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026
https://siva.gov.co/download/605/gestion-tecnologia-de-la-informacion/15012/modelo-y-politica-de-seguridad-de-la-informacion-siva.pdf

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026
Dentro del plan de seguridad y privacidad de la información existe un PLAN DE TRABAJO Y CRONOGRAMA DE ACTIVIDADES para dar cumplimiento al Plan de Seguridad y Privacidad de la Información, se tiene prevista la ejecución de las actividades según el siguiente cronograma, del cual no se reportaron avances y seguimiento a las acciones ejecutadas, se hace la observación de realizar seguimiento y verificar el cumplimiento de los planes de TICS y proyectos del PETI:

Acción o Actividad	Producto	Responsable	Fecha de inicio	Fecha Fi	Actividad
Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información (Si aplica)	Informe Diagnóstic estado actual de SDM.	Profesional de gestión de TIC	15/02/2026	30/03/202	Se realizó la revisión y actualización del autodiagnóstico de Seguridad y Privacidad de la Información, identificando el nivel de cumplimiento, la brechas existentes y las acciones de mejora requeridas.
Actualizar las Políticas de Seguridad de Información (Si aplica	Documento Actualizado	Profesional de gestión de TIC	15/02/2026	30/12/202	Se realizó la revisión de las Políticas de Seguridad de la Información de la entidad, verificando su vigencia y pertinencia frente a las condiciones actuales, los riesgos identificados y los

					lineamientos aplicables, determinando que no se requieren modificaciones para el periodo evaluado.
Gestionar los activos de información en cad dependencia y/o proceso	Informe Administrativo	Profesional de gestión de TIC	15/02/2026	30/12/2026	Se realizó la revisión y actualización de los activos de información de las diferentes dependencias y/o procesos de la entidad, verificando su identificación, responsable, ubicación, clasificación y estado, con el fin de mantener actualizado el inventario de activos de información.
Gestionar los registros activos de informació conforme a la ley 1712	Activos de información	Profesional de gestión de TIC	15/02/2026	30/12/2026	Se realizó la revisión y actualización del Registro de Activos de Información, conforme a los lineamientos establecidos en la Ley 1712 de 2014.
Socializar la Guía de gestión de incidentes d seguridad de la información	Socialización realizada	Profesional de gestión de TIC	15/02/2026	30/12/2026	Se realizó la socialización de la Guía de Gestión de Incidentes de Seguridad de la Información, dando a conocer los lineamientos y procedimientos para el reporte y atención de incidentes.
Elaborar plan de concientización, formació socialización en seguridad de la información apropiación del SGSI.	Documento Administrativo	Profesional de gestión de TIC	15/02/2026	30/12/2026	Se elaboró el plan de concientización, formación y socialización en Seguridad de la Información, orientado al fortalecimiento de las buenas prácticas y la apropiación del SGSI por parte del personal de la entidad.
Implementar las estrategias y campaña incluidas en el plan de concientizació formación, socialización en seguridad de información y apropiación del SGSI	Estrategias campañas	Profesional de gestión de TIC	15/02/2026	30/12/2026	Se implementaron las estrategias y campañas de concientización y formación en Seguridad de la Información, fortaleciendo las buenas prácticas y la apropiación del SGSI por parte del personal de la entidad.
Realizar pruebas de vulnerabilidades y pe test de acuerdo con el alcance y metodología establecida.	Documento Administrativo	Profesional de gestión de TIC	15/02/2026	30/12/2026	Se realizaron pruebas de vulnerabilidades y Pen Test a los activos tecnológicos definidos en el alcance, con el fin de identificar y evaluar posibles vulnerabilidades de seguridad.
Elaborar Plan de copias de respaldo de información para la VIGENCIA 2026	plan de copias de respaldo de información	Profesional de gestión de TIC	15/02/2026	30/12/2026	Se elaboró el Plan de Copias de Respaldo de la Información para la vigencia 2026, estableciendo responsables, periodicidad, medios de almacenamiento y mecanismos de verificación de las copias de seguridad.
Desarrollar la Fase Planeación de IPv6: la cu representa una etapa crítica e importante d proceso de transición por cuanto comienz con el inventario de activos de información se consolida con el plan de diagnóstico de la infraestructuras de TI.	Lograr redes automáticamente más seguras	Profesional de gestión de TIC	15/02/2026	30/12/2026	Se evaluo la fase de Planeación de IPv6, mediante la revisión del inventario de activos de información y tecnológicos y el diagnóstico de la infraestructura de TI, como base para la planificación de la transición a IPv6.
Adquisición de Cuentas de Correo Electrónic Institucional	15 cuentas de correos adquiridas	Profesional de gestión de TIC	15/02/2026	30/12/202	Se realizó la adquisición y habilitación de cuentas de correo electrónico institucional para los usuarios y áreas que lo requerían, fortaleciendo los canales oficiales de comunicación de la entidad.

Definir Mantenimiento preventivo y correctiv periódicos de Hardware y software	Plan De mantenimiento de equipos ejecutado	Profesional de gestión de TIC	15/02/2026	30/12/202	Se definieron y programaron las actividades de mantenimiento preventivo de hardware y software, con el fin de garantizar el adecuado funcionamiento y disponibilidad de los equipos tecnológicos.
Elaborar y/o Actualizar el Inventario de Activ (activos de información)	Inventario de activos informátic actualizados	Profesional de gestión de TIC	15/02/2026	30/12/202	Se realizó la actualización de l inventario de activos de información, identificando y registrando los activos asociados a los diferentes procesos y dependencias de la entidad.
Realizar mantenimiento correctivo preventivo a la UPS de la red eléctri regulada de la entidad	Plan de mantenimien de UPS y redes eléctrica ejecutado	Profesional de gestión de TIC	15/02/2026	30/12/202	Se realizó mantenimiento preventivo a la UPS de la red eléctrica regulada, verificando su funcionamiento y condiciones de operación para garantizar la continuidad del suministro eléctrico de los equipos tecnológicos.
Definir un Plan de capacitación, sensibilizaci y comunicación en seguridad de la informaci	Plan De capacitación ejecutada	Profesional de gestión de TIC	15/02/2026	30/12/202	Se elaboró y definió el Plan de Capacitación, Sensibilización y Comunicación en Seguridad de la Información, orientado a fortalecer los conocimientos y buenas prácticas del personal de la entidad.
Adquirir licencias de antivirus e instalar y hac seguimiento desde la consola o central	Licencias adquiridas	Profesional de gestión de TIC	15/02/2026	30/12/202	Se adquirieron e instalaron las licencias de antivirus, realizando la configuración, administración y seguimiento de los equipos desde la consola central de seguridad.

POLITICAS DE GOBIERNO DIGITAL

Se evidencia Resolución No. 113 (17 De Octubre De 2023) “Por La Cual Se Adopta La Política De Gobierno Digital y la Politica De Seguridad Digital (Política De Seguridad y Privacidad De La Informacion (MSPI)) En El Sistema Integrado De Transorte De Valledupar SIVA SAS.” file:///C:/Users/sugol/Downloads/MODELO-Y-POLITICA-DE-SEGURIDAD-DE-LA-INFORMACION-SIVA.pdf

MANUAL DE PROTECCION DE DATOS PERSONALES

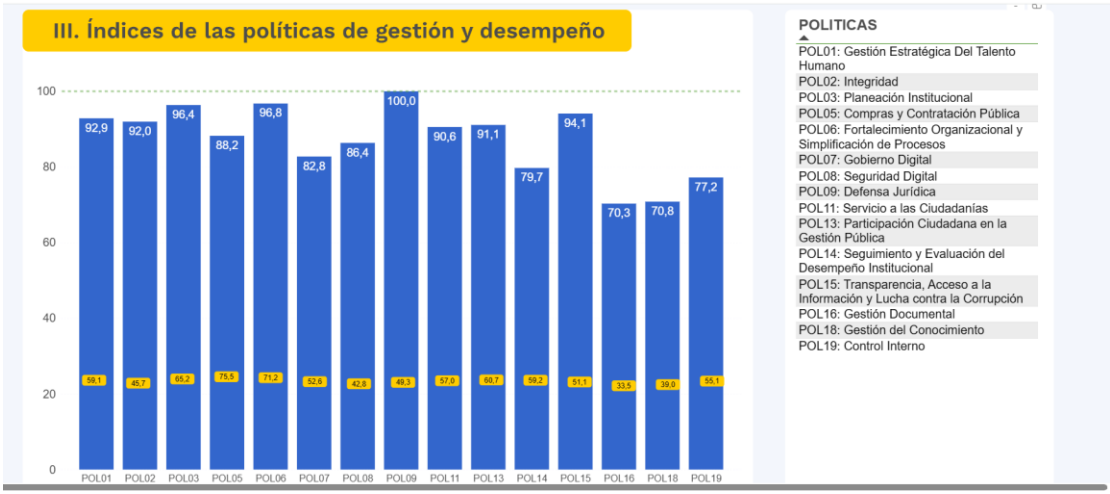
Resolución no. 059 (9 de junio de 2022) 'Por medio de la cual se adoptan el Manual de Política y Procedimiento para la protección de Datos personales y el Derecho de Acceso a la Información Publica en el Sistema Integrado de Transporte de Valledupar – SIV https://siva.gov.co/download/605/gestion-tecnologia-de-la-informacion/15011/resolucion-no-059-2022-adopcion-politica-proteccion-de-datos-2.pdf

GUÍA PARA LA GESTIÓN Y CLASIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 2023
file:///C:/Users/sugol/Downloads/GUIA-PARA-LA-GESTION-Y-CLASIFICACION-DE-INCIDENTES-SEGURIDAD-DE-LA-INFORMACION.pdf

PLAN DE CONCIENTIZACIÓN, FORMACIÓN, SOCIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN Y APROPIACIÓN DEL SGSI
https://siva.gov.co/download/605/gestion-tecnologia-de-la-informacion/15010/plan-de-concientizacion-en-seguridad-de-la-informacion-2.pdf

RESULTADOS FURAG POLITICA DE GOBIERNO DIGITAL





Recomendación FURAG política de seguridad y gobierno digital

Política	Recomendación	Política
Gobierno Digital	Implementar el Modelo de Arquitectura Empresarial (MAE) del Marco de Referencia de Arquitectura Empresarial (MRAE).	POL07
Gobierno Digital	Implementar el Modelo de Gestión de Proyectos de Tecnologías de la Información (MGPT del Marco de Referencia de Arquitectura Empresarial (MRAE).	POL07
Gobierno Digital	Desarrollar e implementar una estrategia de uso y apropiación de tecnologías actuales y emergentes (blockchain, inteligencia artificial, internet de las cosas, automatización robótica de procesos).	POL07
Gobierno Digital	Establecer estrategias para consolidar el conocimiento y las lecciones aprendidas del áre de Tecnologías de la Información.	POL07
Gobierno Digital	Utilizar datos externos a la entidad para apoyar la toma de decisiones relacionadas con s misionalidad.	POL07
Gobierno Digital	Implementar la técnica de 'análisis de causalidad' para el análisis de datos de la entidad. uso de esta técnica permite analizar como un conjunto de variables puede afectar el comportamiento de otra variable.	POL07
Gobierno Digital	Implementar la técnica de 'análisis predictivo' para el análisis de datos de la entidad. El us de esta técnica permite predecir las tendencias o posibles comportamientos futuros de un variable.	POL07
Gobierno Digital	Implementar la técnica de 'análisis prescriptivo' para el análisis de datos de la entidad. El uso de esta técnica permite establecer cuál es la mejor acción para tomar bajo un contex específico.	POL07
Gobierno Digital	Implementar el criterio de accesibilidad 'CC10. Permitir saltar bloques que se repiten' en l sede electrónica de la entidad, acorde con el anexo 1 de la Resolución 1519 de 2020.	POL07
Gobierno Digital	Utilizar medios digitales como redes sociales o la sede electrónica de la entidad para los ejercicios de rendición de cuentas.	POL07
Gobierno Digital	Establecer instancias/dependencias de toma de decisiones sobre la implementación de la Política de Gobierno Digital en la entidad, tales como el Comité de Gestión y Desempeño Institucional, la Oficina de Tecnologías de Información, la Oficina de Planeación, entre otras.	POL07
Seguridad Digital	Designar de manera clara un área o responsable de la seguridad digital.	POL08

Seguridad Digital	Contar con un Plan de Continuidad del Negocio -BCP-, que esté definido, documentado e implementado para los procesos críticos y misionales de la entidad.	POL08

REALIZACIÓN DE MANTENIMIENTOS PREVENTIVOS Y/O CORRECTIVOS

Se evidencia que la entidad cuenta con un formato de CRONOGRAMA DE INSPECCION Y MANTENIMIENTO DE EQUIPOS DE COMPUTOS de la entidad, en el cual se encuentra programado los mantenimientos preventivos y correctivos para la vigencia 2026 que se ejecutaron en el mes de septiembre de la vigencia.

La programación del mantenimiento de los computadores se realiza a través de una planilla programada anualmente donde de manera de acuerdo a como surja la necesidad del equipo se programa la actividad de mantenimiento correctivo.

El programa de mantenimiento se venía realizando de manera correctiva ya que la entidad no Cuenta con un profesional idóneo para realizar las actividades de mantenimiento preventivo.

Según el programa evidenciado se observa que el mes de septiembre de los cómputos de la entidad fueron programados y ejecutado el programa de mantenimiento correctivo a través de la ejecución del contrato Nº CS-052-2026 CONTRATO PRESTACION DE SERVICIOS DE APOYO A LA GESTION PSAG.052-2026 CONTRATARLA PRESTACIÓN DE SERVICIOS DE APOYOALA GESTION PARA EL DESARROLLO DE ACTIVIDADES ASISTENCIALES EN EL MANTENIMIENTO DE LA RED DE TRABAJO Y DE LOS EQUIPOS DE CÓMPUTO DEL SISTEMA INTEGRADO DE TRANSPORTE DE VALLEDUPAR - SIVA S.A.S., Y DEMÁS OBJETO ACTIVIDADES RELACIONADAS EN MATERIA DE TICS DEL ENTE GESTOR DEL SISTEMA ESTRATÉGICO DE TRANSPORTE PÚBLICO COLECTIVO DE LA CIUDAD DE VALLEDUPAR - SETPC.
JAVIER ALFONSO YANCE SUAREZ
PLAZO DOS MESES
Su fórmula es: (Mantenimientos preventivos ejecutados a las instalaciones / mantenimientos Preventivos programados a las instalaciones) *100. En la revisión de sistema de gestión se evidencia que el indicador se encuentra en ejecución 100%, se programaron 73 equipos para mantenimiento y se realizaron los 73 mantenimientos programados.

COMPUTADOR JANUS CON TORRE CODIGO P0002-0007 PREVENTIVO 1
Serial 190315473043

MANTENIMIENTOS REALIZADO		
FECHA	**TIPO DE MANTENIMIENTO**	**DESCRIPCION**
2026 SEPTIEMBRE	PREVENTIVO	Se le realizo mantenimiento preventivo que consta de: Retiro de tapas o paneles de acceso, se realizó limpieza interna de polvo y suciedad, limpieza de ventiladores, disipadores y rejillas de ventilación, Limpieza de la placa madre utilizando herramientas adecuada, limpieza de los módulos de memoria RAM y sus zócalos, revisión del funcionamiento de ventiladores, actualización del sistema operativo, actualización de controladores (drivers),mantener actualizado el software de seguridad, análisis en busca de malware, eliminación de archivos temporales y archivos innecesarios, realizar y verificar copias de seguridad de información.

6.Computador portátil Modelo: Notebook pc ASUS UX303U Número de serie: PD97265NG Características: Procesador Intel Core I5-6200u RAM DDR4-2400 8GB

MANTENIMIENTOS REALIZADO		
FECHA	**TIPO DE MANTENIMIENTO**	**DESCRIPCION**
2026 SEPTIEMBRE	PREVENTIVO	Se le realizo mantenimiento preventivo que consta de: Retiro de tapas o paneles de acceso, se realizó limpieza interna de polvo y suciedad, limpieza de ventiladores, disipadores y rejillas de ventilación, Limpieza de la placa madre utilizando herramientas adecuada, limpieza de los módulos de memoria RAM y sus zócalos, revisión del funcionamiento de ventiladores, actualización del sistema operativo, actualización de controladores (drivers),mantener actualizado el software de seguridad, análisis en busca de malware, eliminación de archivos temporales y archivos innecesarios, realizar y verificar copias de seguridad de información importante

12.Computador todo en Uno. Modelo: HP 22-dd0522la Número de serie: 8CC2035sv8 Características: Procesador Intel Celeron J4025 RAM DDR4-2400 MHz de 4gb

MANTENIMIENTOS REALIZADO		
FECHA	**TIPO DE MANTENIMIENTO**	**DESCRIPCION**
2026 SEPTIEMBRE	PREVENTIVO	Se le realizo mantenimiento preventivo que consta de: Retiro de tapas o paneles de acceso, se realizó limpieza interna de polvo y suciedad, limpieza de ventiladores, disipadores y rejillas de

		ventilación, Limpieza de la placa madre utilizando herramientas adecuada, limpieza de los módulos de memoria RAM y sus zócalos, revisión del funcionamiento de ventiladores, actualización del sistema operativo, actualización de controladores (drivers),mantener actualizado el software de seguridad, análisis en busca de malware, eliminación de archivos temporales y archivos innecesarios, realizar y verificar copias de seguridad de información Recomendaciones: El equipo cuenta actualmente con un solo módulo d 8 GB DDR4 a 2400 MHz. Esta cantidad es insuficiente para las exigencias de navegación web y aplicaciones de oficina actuales. Recomendaciones: Instalar dos módulos idénticos de 8 GB DDR4 a 2400 MHz para alcanzar un total de 16 GB. Sustituye el disco principal por un SSD de tecnología SATA de 2.5 pulgadas (o un formato M.2 si t placa lo permite) de hasta 1 tb de almacenamiento.



DESCRIPCIÓN DEL EQUIPO: IMPRESORA MULTIFUNCIONAL EN FUNCION Y EN BUEN ESTADO, BLANCO & NEGRO

TIPO DE EQUIPO IMPRESORA FABRICANTE: RICOH
MODELO: MP5002
SERIE: W532L400799

MANTENIMIENTOS REALIZADO		
FECHA	**TIPO DE MANTENIMIENTO**	**DESCRIPCION**
2026 SEPTIEMBRE	PREVENTIVO	Se realizó mantenimiento preventivo a la impresora RICOH MP 5002, que incluyó la limpieza general del equipo, retirando polvo, residuos de papel y suciedad acumulada en las superficies y componentes accesibles. Asimismo, se efectuó el cambio de tóner, verificando su correcta instalación y funcionamiento. Estas actividades se realizaron con el propósito de garantizar condiciones adecuadas de operación, contribuir a la calidad de impresión y mantener el equipo en buenas condiciones operativas.





CODIGO DE INVENTARIO:	0003-00027	**NOMBRE DEL EQUIPO:**	IMPRESORA	**AREA**	JURIDICA
DESCRIPCIÓN DEL EQUIPO:	IMPRESORA LASER EN FUNCION Y EN BUEN ESTADO ,BLANCO & NEGRO				
TIPO DE EQUIPO		**FABRICANTE:**	**MODELO:**		**SERIE:**
IMPRESORA		HP	MFP521		CNB7HDHKBG
PARTES DEL EQUIPO:	IMPRESORA HP LASSERJET, CONFORMADA CON FUENTE DE PODER, CABLE DE RED Y TONER MULTI COLOR.				

MANTENIMIENTOS REALIZADO		
FECHA	**TIPO DE MANTENIMIENTO**	**DESCRIPCION**
2026 SEPTIEMBRE	OCASIONAL	Se realizó limpieza general de la impresora retirando polvo, residuos de papel y suciedad acumulada en las superficies externas y componentes accesibles del equipo. Esta actividad se efectuó con el propósito de conservar la impresora en adecuadas condiciones de limpieza, contribuir a su correcto funcionamiento, prevenir posibles inconvenientes durante la operación y mantener una adecuada calidad de impresión.





CODIGO DE INVENTARIO:	0003-000	**NOMBRE DEL EQUIPO:**	SCANEER SCAN MATE	**AREA:**	VENTANILLA UNIC
DESCRIPCIÓN DEL EQUIP	ESCANER FUNCIONAL EN BUEN ESTADO				
TIPO DE EQUIPO		**FABRICANTE:**	**MODELO:**	**SERIE**	
ESCANER		KODAK	ALARIS S2050	611814	
PARTES DEL EQUIPO:	ESCANER, CABLE DE PODER, Y CABLE USB				
ESPECIFICACIONES	Equipo apropiado para uso laboral, personal, con gran tecnología en procesadores, calidad respaldada por mas 100 pruebas realizadas, capacidad de escaneo constante				

MANTENIMIENTOS REALIZADO		
FECHA	**TIPO DE MANTENIMIENTO**	**DESCRIPCION**
2026 SEPTIEMBRE	PREVENTIVO	Se llevó a cabo el mantenimiento preventivo del escáner documental Kodak S2050, iniciando con la remoción de polvo en la carcasa y bandejas mediante aire comprimido, seguido de la limpieza profunda de los rodillos del sistema de arrastre con líquidos especializados para restablecer su agarre y prevenir atascos de papel. Adicionalmente, se higienizó el sistema óptico limpiando las guías de imagen y los sensores con paños de microfibra antiestáticos y alcohol isopropílico para asegurar una digitalización nítida y libre de manchas. Por último, tras verificar el buen estado del adaptador de corriente y el cable USB, se realizaron pruebas de escaneo a doble cara en distintas resoluciones, confirmando que el equipo quedó completamente operativo, calibrado y funcionando en óptimas condiciones.

CODIGO DE INVENTARIO:	0003-00024	**NOMBRE DEL EQUIPO:**	VIDEO PROJECTOR	**AREA**	ADMINISTRATIVA
DESCRIPCIÓN DEL EQUIPO:	VIDEO BEAM (funcional y en buen estado)				
TIPO DE EQUIPO		**FABRICANTE:**	**MODELO:**	**SERIE:**	
VIDEO PROJECTOR		EPSON	H382F	V11H382120	
PARTES DEL EQUIPO:	EQUIPO PROYECTOR, CONFORMADO CON FUENTE DE PODER Y CABLE HDMI, CABLE VGA				
ESPECIFICACIONES	Equipo apropiado para uso laboral, personal, con gran tecnología en procesadores, calidad respaldad por mas de 100 pruebas realizadas, pantalla full HD, capacidad de proyeccion full HD				

MANTENIMIENTOS REALIZADO

FECHA	TIPO DE MANTENIMIENTO	DESCRIPCION
2026 SEPTIEMBRE	PREVENTIVO	Se realizó limpieza general de la parte externa del videobeam, retirando polvo y suciedad acumulada en la carcasa, lente, panel de control, puertos de conexión y rejillas de ventilación. Esta actividad se efectuó con el propósito de conservar el equipo en adecuadas condiciones de limpieza, prevenir la acumulación de partículas que puedan afectar su funcionamiento y contribuir a su correcto desempeño y presentación.

CODIGO DE INVENTARIO:	0003-00005	**NOMBRE DEL EQUIPO:**	VIDEO PROJECTOR	**AREA:** ARCHIVO
DESCRIPCIÓN DEL EQUIPO:	VIDEO BEAM (funcional y en buen estado)			
TIPO DE EQUIPO	**FABRICANTE:**	**MODELO:**	**SERIE:**	
VIDEO PROJECTOR	EPSON	S12	SNPSPF221179L	
PARTES DEL EQUIPO	EQUIPO PROYECTOR, CONFORMADO CON FUENTE DE PODER Y CABLE HDMI, CABLE VGA			
ESPECIFICACIONES	Equipo apropiado para uso laboral, personal, con gran tecnología en procesadores, calidad respaldada por mas de 100 pruebas realizadas, pantalla fu HD, capacidad de proyeccion full HD			
RECOMENDACIONES	Mantenga la unidad apartada de aparatos de calefacción, zonas húmedas, sin exposición directa a luz solar.			

MANTENIMIENTOS REALIZADO		
FECHA	**TIPO DE MANTENIMIENTO**	**DESCRIPCION**
2026 SEPTIEMBRE	PREVENTIVO	Se realizó limpieza general de la parte externa del videobeam, retirando polvo y suciedad acumulada en la carcasa, lente, panel de control, puertos de conexión rejillas de ventilación. Esta actividad se efectuó con el propósito de conservar el equipo en adecuadas condiciones de limpieza, prevenir la acumulación de partículas que puedan afectar su funcionamiento y contribuir a su correcto desempeño y presentación.

CODIGO DE INVENTARIO:	0003-00060	**NOMBRE DEL EQUIPO:**	TABLETA	**AREA**	ADMINISTRATIVA
DESCRIPCIÓN DEL EQUIPO:	TABLETA FUNCIONA, EN BUEN ESTADO				
TIPO DE EQUIPO		**FABRICANTE:**	**MODELO**	**SERIE:**	
TABLETA		SAMSUNG	SM-X205	R8YW105PABA	
PARTES DEL EQUIPO:	TABLETA DIGITAL, CABLE USB, CABEZOTE DE PODER				
ESPECIFICACIONES	TABLETA DIGITAL FUNCIONAL CON MEMORIA DE DIACO INTERNO DE 64 GB, CAPACIDAD CON ERRANURA DE EXPASION, Y ERRANURA DE SINCARD DISPONIBLE PARA CUALQUIER OPERADOR.				

MANTENIMIENTOS REALIZADO		
FECHA	**TIPO DE MANTENIMIENTO**	**DESCRIPCION**
2026 SEPTIEMBRE	PREVENTIVO	Se realizó limpieza externa de la tablet, retirando polvo, suciedad y residuos acumulados en la pantalla, carcasa, puertos de conexión y demás superficies accesibles del equipo. Esta actividad se efectuó con el propósito de mantener el dispositivo en

		adecuadas condiciones de limpieza, contribuir su correcto funcionamiento y conservarlo en buenas condiciones operativas.

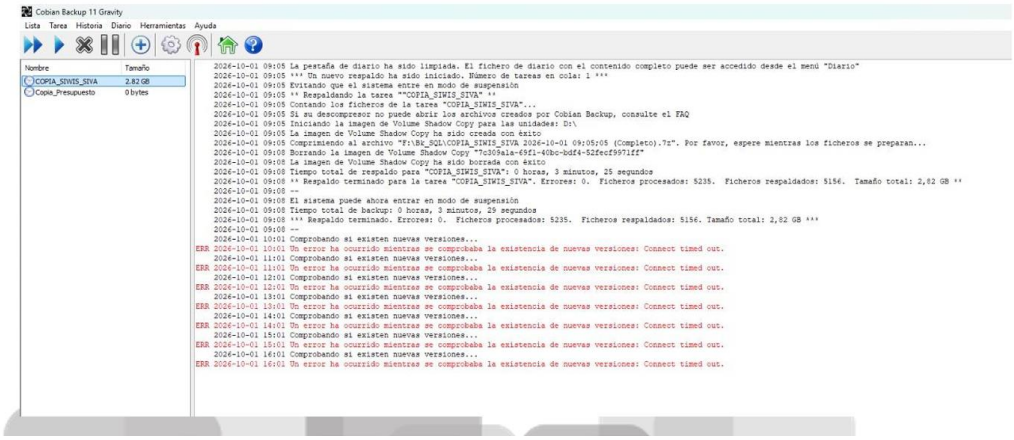
CODIGO DE INVENTARIO:	0003-00008	**NOMBRE DEL EQUIPO:**	ESTABILIZADOR	**AREA:**	JURIDICA
DESCRIPCIÓN DEL EQUIPO:	ESTABILIZADOR FUNCIONAL EN BUEN ESTADO				
TIPO DE EQUIPO		**FABRICANTE:**	**MODELO:**	**SERIE:**	
ESTABILIZADOR		NICOMAR	N/A	00.55	
PARTES DEL EQUIPO:	ESTABILIZADOR DE 1000W , CABLE DE PODER				

MANTENIMIENTOS REALIZADO		
FECHA	**TIPO DE MANTENIMIENTO**	**DESCRIPCION**
2026 SEPTIEMBRE	PREVENTIVO	Se ejecutó la remoción de polvo y limpieza de la carcasa metálica negra, prestando especial atención a mantener despejadas las áreas de ventilación para prevenir el sobrecalentamiento del equipo en su ubicación actual, Se efectuaron mediciones con multímetro en los tomacorrientes posteriores, confirmando que los valores de voltaje de salida se encuentran dentro de los rangos seguros y estabilizados para proteger la carga conectada El equipo EV 2000 E se encuentra en óptimas condiciones físicas y eléctricas, operando de manera estable y entregando la potencia regulada requerida

Registros EVIDENCIAS TICS

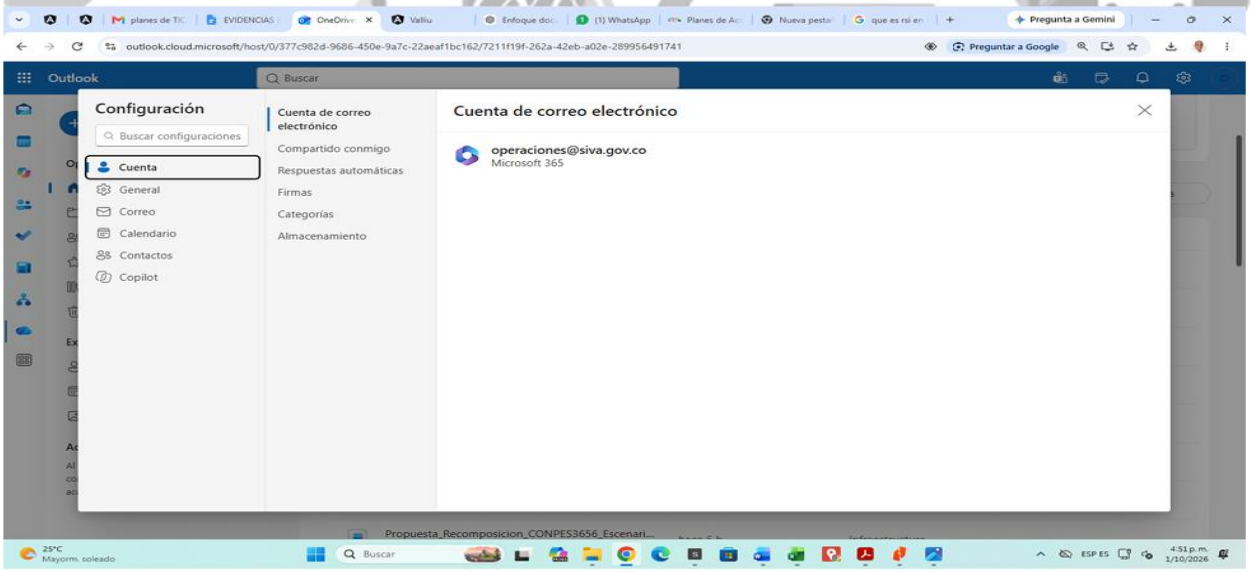
Se realizó copia de seguridad para salvaguardar la información en algunos computadores de la entidad como protocolo de seguridad.

1-REGISTRO DE COPIA DE SEGURIDAD CONTABILIDAD



2- MECANISMO DE RESPALDO SEGURIDAD OPERACIONES

En el área de Operaciones se utiliza One Drive como mecanismo complementario para el almacenamiento y respaldo de la información generada y gestionada diariamente, permitiendo disponer de una copia adicional de los archivos y facilitar su acceso y recuperación.



ADMINISTRACIÓN DE LA PÁGINA WEB

Se evidencia el siguiente contrato por medio del cual se realizaron mejoras en la página web de la entidad así: **https://siva.gov.co/**

TIPO CONTRATO	NO. CONTRATO	AÑO	MODALIDAD	RUBRO	OBJETO	CONTRATISTA	VALOR CONTRATO	PLAZO
PS		2026	Solicitud de Única Oferta	Proyecto	CONTRATAR LA PRESTACIÓN DE SERVICIOS DE ACTUALIZACIÓN DEL SITIO WEB Y HOSTING, CON CORREO ELECTRÓNICO INCLUIDO Y DEMÁS ESPECIFICACIONES TÉCNICAS REQUERIDAS POR LA ENTIDAD SISTEMA INTEGRADO DE TRANSPORTE DE VALLEDUPAR SAS – SIVA SAS	GOPHER GROU SAS	33,820.000	11 MESES

Link TRANSPARENCIA Y ACCESO A LA INFORMACIÓN

Se evidencia las mejoras en el Link de Transparencia y acceso a la información cumpliendo con los requisitos de la Resolución 1519 de 2020 del Ministerio de Tecnologías de la información MIN TIC: **LINK DE TRANSPARENCIA** https://siva.gov.co/transparencia-y-acceso-a-la-informacion/



LICENCIAS Y ANTIVIRUS

ACEPTACIÓN DE LA OFERTA Nº PS-075-2025 (Contrato de Prestación de Servicios)

CONTRATAR EL MANTENIMIENTO DE HERRAMIENTAS TECNOLÓGICAS, ADQUISICIÓN DE LICENCIAS MICROSOFT, Y DEMÁS LICENCIAS REQUERIDAS PARA EL FORTALECIMIENTO INSTITUCIONAL DEL SISTEMA INTEGRADO DE TRANSPORTE PÚBLICO DE VALLEDUPAR SIVA SAS.
VALOR DEL CONTRATO: TRECE MILLONES SETECIENTOS TRECE MIL QUINIENTOS SESENTA PESOS ($13.713.560) M/L

INSTALACIÓN Y SUMINISTRO DE TRES (03) LICENCIAS SUSCRIPCIÓN UN AÑO DE MICROSOFT 365 EMPRESA ESTÁNDAR, PARA 5 USUARIOS 3.1. CÓDIGO DE ACTIVACION DEL PRODUCTO: WQJG4-KGDHK-HYMPC-F7KY4-7RMQZ ACTIVACIÓN: 31-12-2025 USUARIO ASOCIADO: sivalicencias@sivalicencias.onmicrosoft.com CONTRASEÑA: siva2024* URL DE GESTION: https://www.microsoft.com/es-es/microsoft-365/business/microsoft-365- administration

3.2. . CÓDIGO DE LICENCIA: GRYR4-444MW-PVM2F-7CMD4-FFR3 ACTIVACIÓN: SIN ACTIVAR. Para el proceso de activación se suministra el siguiente enlace: https://signup.microsoft.com/get-started/setupKey?origin=Office&brandingId=28b276fb-d2a0-4379-a7c0-57dce33da0f9&ali=1 3.3. CÓDIGO DE LICENCIA: DKDM7-HCF2X-MYMV9-TJT4V-4GCKZ ACTIVACIÓN: SIN ACTIVAR. Para el proceso de activación se suministra el siguiente enlace: https://signup.microsoft.com/get-started/setupKey?origin=Office&brandingId=28b276fb-d2a0- 4379-a7c0-57dce33da0f9&ali=1

LICENCIAS			
NOMBRE	**VERSIÓN**	**DETALLE**	**VIGENCIA**
ANTIVIRUS	3 LICENCIA DE ANTIVIRUS KASPERSKY PREMIUM PARA 5 DISPOSITIVOS	Usuario Asociado: licenciasiva@gmail.com Contraseña: siva2025* Código de activación del producto: 7CF3Z-53D2Q-3YCR2-HNYY Código de activación del producto: 7JHQ4-C49H5-W4AGG-UQZ7K Código de activación del producto: JKHMK-B2UA8-SAUVJ-2DHE	DICIEMBRE 2025-DICIEMBRE 2026
MICROSOFT OFFICE	LICENCIA DE MICROSOFT 365 EMPRESA ESTÁNDAR, PARA 5 USUARIOS	Usuario asociado: sivalicencias@sivalicencias.onmicrosoft.com Contraseña: siva2024* Url de gestion: https://www.microsoft.com/es-es/microsoft-365/business/microsoft-365 administración	DICIEMBRE 2025-DICIEMBRE 2026

MICROSOFT OFFICE	LICENCIAS DE MICROSOFT 365 BUSINESS STANDARD AND MICROSOFT 365 COPILOT BUSINESS	Usuario asociado: gerencia@siva,gov,co Contraseña: siva2024*	DICIEMBRE 2025-DICIEMBRE 2026
SOFTWARE CREATIVO PARA PROFESIONALES	LICENCIA DE ADOBE ACROBAT PRO	Usuario asociado: licenciasiva@gmail.com Contraseña: Siva2025* Enlace de descarga de la aplicación Adobe Creative Cloud: https://creativecloud.adobe.com/apps/download/creative-cloud	DICIEMBRE 2025-DICIEMBRE 2026
SOFTWARE SIIGO	Presupuesto Net, licencia siigo servicios ofical	INTEGRASOFT CON REGISTRO DE DERECHO DE AUTOR N° 13-15-88 DEL 24 DE OCTUBRE DEL 2005 N° DE LICCENCIA 01902012122205	2026

INSTALACIÓN Y SUMINISTRO DE LICENCIAS POR SUSCRIPCIÓN A UN AÑO DE MICROSOFT 365 BUSINESS STANDARD AND MICROSOFT 365 COPILOT BUSINESS CÓDIGO DE ACTIVACIÓN DEL PRODUCTO: V6THK-QKH39-YMK4F-MF9W4-F6KXZ ACTIVACIÓN: SIN ACTIVAR. Para el proceso de activación se suministra el siguiente enlace: https://signup.microsoft.com/get-started/setupKey?origin=Office&brandingId=28b276fb-d2a0-4379-a7c0-57dce33da0f9&ali=1

5. INSTALACIÓN Y SUMINISTRO DE TRES (03) LICENCIA SUSCRIPCIÓN POR UN AÑO DE ANTIVIRUS
licencia de antivirus kaspersky PREMIUM / 5 dispositivos CÓDIGO DE ACTIVACIÓN DEL PRODUCTO: 7CF3Z-53D2Q-3YCR2-HNYYE CÓDIGO DE ACTIVACIÓN DEL PRODUCTO: 7JHQ4-C49H5-W4AGG-UQZ7K CÓDIGO DE ACTIVACIÓN DEL PRODUCTO: JKHMK-B2UA8-SAUVJ-2DHBU USUARIO ASOCIADO: LICENCIASIVA@GMAIL.COM CONTRASEÑA: Siva2025

INSTALACIÓN Y SUMINISTRO DE LICENCIA SUSCRIPCIÓN POR UN AÑO DE ADOBE ACROBAT PRO Inicio de sesión con Google Correo electrónico: licenciasiva@gmail.com Contraseña: Siva2025* Enlace de descarga de la aplicación Adobe Creative Cloud: https://creativecloud.adobe.com/apps/download/creative-cloud

SOFTWARE/APLICATIVOS	
NOMBRE	**DETALLE**
Antivirus	KASPERSKY PREMIUM 1 AÑO BASE (ELECTRÓNICA) (CONSUMO)
Microsoft Office	Licencias Microsoft Office 365 Apps for Business ESD
MICROSOFT OFFICE	LICENCIAS DE MICROSOFT 365 BUSINESS STANDARD AND MICROSOFT 365 COPILOT BUSINESS

SOFTWARE CREATIVO PARA PROFESIONALES	LICENCIA DE ADOBE ACROBAT PRO
CHIP	APLICATIVO DE CONSOLIDADOR DE HACIENDA E INFORMACION FINANCIERA
SOFTWARE SIIGO	Presupuesto Net, licencia siigo servicios oficial
SECOP	Sistema Electrónico de Contratación Pública
SIA OBSERVA	Es una plataforma digital que permite organizar información y presentar informes de manera estandarizada en línea por parte de los sujetos de control.
SAE	APLICATIVO QUE GENERA EL OPERADOR PARA HACER SUPERVICION DE FLOTA
SIGEP	Este aplicativo forma parte del Sistema de Información Gestión del Empleo Público

Incidentes informáticos

Inscripción en el CESIT se realizó la solicitud ante gobierno digital
No se presentaron incidentes de seguridad informáticos en la vigencia 2026

PLAN DE MEJORAMIENTO AUDITORIA INTERNA :

PRINCIPALES SITUACIONES DETECTADAS/ RESULTADOS DE LA AUDITORÍA / RECOMENDACIONES

HALLAZGOS:

Incumplimiento del mantenimiento preventivo de los equipos de cómputo programados para el segundo semestre de la vigencia, no se presentaron evidencias de su ejecución.

Se evidencio un cronograma de mantenimiento de equipos con una programación de mantenimientos para el segundo semestre, de la cual no se presentaron registros, se verifico la hoja de vida de los equipos, sin información del mantenimiento realizado.

Deficiente seguimiento y verificación del cumplimiento de los planes de TICS y proyectos del PETI

Dentro del plan de seguridad y privacidad de la información existe un PLAN DE TRABAJO Y CRONOGRAMA DE ACTIVIDADES para dar cumplimiento al Plan de Seguridad y Privacidad de la Información, se tiene prevista la ejecución de las actividades según el siguiente cronograma, del cual No se reportaron avances y seguimiento a las acciones ejecutadas, se hace la observación de

realizar seguimiento y verificar el cumplimiento de los planes de TICS y proyectos del PETI 2021-2024.

“Implementación Política Gobierno Digital”, no se pudo hacer una valoración del avance y mejora en la implementación de la Política de Gobierna Digital.

8. Resumen de los hallazgos o observaciones encontradas

No se determinaron hallazgos en la auditoria

9. RECOMENDACIONES GENERALES DE LA AUDITORÍA INTERNA:

En el marco del mejoramiento continuo y con miras a apoyar el fortalecimiento del sistema de gestión, la Oficina de Control Interno recomienda:

Fortalecer la seguridad de la información y accesos:

Implementar revisiones periódicas de los perfiles de usuario y accesos a bases de datos y sistemas críticos. Formalizar y probar regularmente los **planes de respaldo (*back-ups*)** y recuperación ante desastres (DRP).
Optimizar la infraestructura tecnológica: Realizar jornadas de ordenamiento de cableado, mantenimiento preventivo de equipos de cómputo y revisión de normativas técnicas en conexiones eléctricas.
Actualizar el inventario de activos de hardware y software, clasificándolos según su nivel de criticidad.

Actualizar el marco normativo y documental: Revisar y ajustar las políticas del Sistema de Integrado de Gestión (SIG) para alinearlas con la normatividad vigente y los estándares actuales (como lineamientos de MinTIC o ISO 27001).Documentar de forma explícita los roles, responsabilidades y compromisos del personal en relación con la seguridad digital y el manejo de datos.

Monitoreo y gestión de riesgos: Establecer indicadores de gestión (KPI) para medir la efectividad del soporte técnico, la resolución de incidentes de seguridad y el cumplimiento de los niveles de servicio (SLA).

Continuar fortaleciendo los controles que mantengan los antivirus actualizados en los equipos del cómputo utilizados para trabajo, tanto propios de la entidad, como de propiedad de los servidores y contratistas, que permitan asegurar que estos de encuentren con protección de antivirus.

Liderar y apoyar la organización e incorporación de todos los actores internos necesarios para definir los roles y responsabilidades del MPSI y política de Gobierno y Seguridad Digital, de

conformidad con los lineamientos, exigencias, manual de funciones y obligaciones contractuales, con el fin de apoyar y fortalecer su implementación.

Se recomienda mantener la integridad de la información de la entidad y poner en marcha estrategias para evitar ataques cibernéticos, recordar a los colaboradores las políticas de seguridad de la información y el uso y privacidad de los datos, así mismo proteger y monitorear los sistemas de información a través de backups, cifrado de información para los datos sensibles, antivirus que cubra todos los dispositivos que acceden a la información de la entidad, firewall, entre otros, con el objetivo de mitigar el riesgo de pérdida, indisponibilidad, deterioro o acceso no autorizado.

10. CONCLUSIONES GENERALES DE LA AUDITORÍA:

En el ciclo auditor, se logró la cobertura del 100% del Proceso de Gestión Tic, por parte del Auditor de la Oficina de Control Interno, con el apoyo de todos contratistas y el jefe de proceso, auditando en modalidad documental e in-situ.

En el desarrollo de la auditoría, se denotó un ambiente favorable para el desarrollo de los productos del proceso, las condiciones procedimentales se encuentran en un nivel donde pueden ser controlados por los responsables.

1. (Nivel de Madurez y Cumplimiento):

- El proceso de Gestión de TI cuenta con una estructura operativa base; sin embargo, **el nivel de madurez de los controles internos es moderado**, evidenciando brechas importantes entre los procedimientos ejecutados en el día a día y las políticas formalmente documentadas por la organización.

- Se determinó que el área de TI responde de manera reactiva a las necesidades operativas, lo que limita su alineación estratégica con los objetivos del negocio y dificulta la mitigación oportuna de riesgos tecnológicos globales.

2. Seguridad de la Información y Gestión de Accesos:

- **Deficiencia en el control de privilegios:** Los controles para la asignación, modificación y revocación de accesos a los sistemas críticos son deficientes. Se identificaron usuarios activos pertenecientes a excolaboradores y perfiles con privilegios excesivos no justificados por su rol actual.

- **Vulnerabilidad en políticas de autenticación:** La ausencia de políticas robustas de contraseñas y la falta de implementación del doble factor de autenticación (2FA) en

plataformas clave elevan el riesgo de accesos no autorizados y fuga de información sensible.

3. Continuidad del Negocio y Copias de Respaldo (Backups)

- **Inexistencia de pruebas de recuperación:** Si bien se ejecutan copias de respaldo de las bases de datos de forma periódica, **no existe evidencia institucional de pruebas de restauración de datos**, lo que impide garantizar la integridad y disponibilidad de la información ante un incidente crítico o un ataque cibernético.

- **Desactualización del Plan de Contingencia:** El Plan de Recuperación ante Desastres (DRP) se encuentra desactualizado y no contempla los nuevos sistemas adquiridos en el último año, dejando a la organización expuesta a tiempos prolongados de inactividad operativa.

11. APROBACIÓN INFORME DE AUDITORÍA INTERNA

AUDITOR LÍDER		
Auditores	**Nombre completo**	**Firma**
JEFE DE LA OFICINA DE CONTROL INTERNO	MARIA ANGELICA GONZALEZ OÑATE	ORIGINAL FIRMADO

Para constancia se firma en Valledupar, Cesar a los quince (15) días del mes de octubre del año 2026.

APROBACIÓN DEL INFORME DE AUDITORÍA		
Nombre Completo	**Responsabilidad** (cargo)	**Firma**

ANEXO: REGISTROS FOTOGRAFICO









