Huila
Territorio de vida,
sostenibilidad y desarrollo

OFICINA DE CONTROL INTERNO

Informe de seguimiento proceso TIC

1. OBJETIVO

Evaluar la Gestión y la efectividad de los controles aplicados en el proceso de Gestión de servicios TIC, con el propósito de identificar oportunidades de mejora que contribuyan al cumplimiento de los objetivos de la CAM.

2. ALCANCE

El periodo a auditar se encuentra comprendido entre el 01 de enero y el 30 de diciembre de 2023 y se hará énfasis en los siguientes aspectos:

• Seguimiento al Plan Estratégico de Tecnologías de la Información (PETI).
• Evaluación de la seguridad y privacidad de la información.

3. RESULTADOS DEL SEGUIMIENTO

a. CONTEXTO

En lo referente a la estructura bajo la cual se atienden los servicios de TIC; se puede establecer lo siguiente:

El proceso de Gestión de servicios TIC se encuentra como subproceso del proceso de Direccionamiento Estratégico y está a cargo de la Subdirección de Planeación y Ordenamiento Territorial.

La atención de los requerimientos se realiza a través del contrato No. 218 de 2022; en lo concerniente a:

SOPORTE Y ADMINISTRACIÓN DE LA PLATAFORMA DEL CENTRO DE DATOS Y RED DE DATOS (SEGUNDO NIVEL): Soporte, administración, configuración y mantenimiento a la plataforma de TI de la Corporación. Realizar la planeación, montaje, instalación y migración de la plataforma existente de servidores y/o sistemas centrales de la plataforma de TIC. Administrar, instalar, configurar y soportar las bases de datos. Descargar y aplicar actualizaciones de software adquiridas por la CAM o versiones liberadas de manera gratuita por fabricantes para Sistemas Operativos, Bases de Datos, parches de seguridad entre otros

SOPORTE INFORMÁTICO DE PRIMER NIVEL: En lo referente a brinda asistencia técnica requerida a través de la mesa de ayuda.

MANTENIMIENTO PREVENTIVO Y CORRECTIVO: A servidores, computadores, hardware y red de datos.

APOYO PARA LA GESTIÓN TIC: En lo que se refiera a asesoría y acompañamiento para la gestión y proyección de la plataforma TIC.

b. PLANEACIÓN DEL PROCESO

Dentro de las herramientas que se tienen para la planificación del proceso se encuentra: Ficha de caracterización que define las actividades que se llevan a cabo para la gestión de

servicios TIC; Procedimientos: P-CAM-031_Administracion_del_Centro_de_computo , P-CAM-032 Mantenimiento correctivo de equipos , P-CAM-033_Mantenimiento_preventivo_de_equipos y planes: Plan Estratégico TIC 2020 – 2023, Plan De Seguridad Y Privacidad De La Información, Plan de Tratamiento de la Información, Plan de Contingencia.

Recursos

Con el fin de asignar los recursos necesarios para atender las necesidades del proceso y de la entidad en materia de TIC, de manera anual se establecen los requerimientos a través de Plan Operativo Anual de Inversiones, en dónde se cuenta con el indicador del Plan de acción institucional: Porcentaje de actualización e implementación del Plan Estratégico Tecnológico de la CAM para el período 2020-2023, que para la vigencia 2023, tuvo una ejecución presupuestal de 702.939.342 equivalente al 94% de lo asignado para la vigencia.

c. EJECUCIÓN DEL PROCESO

En el año 2023 se avanzó en la ejecución de los proyectos definidos en el Plan Estratégico Tecnológico de la Corporación con el fin de garantizar una infraestructura tecnológica operativa y confiable con el fin de soportar los procesos misionales de la Corporación.

Los avances más importantes por cada una de las líneas de acción que lo integran son:

- Se plantearon e implementaron los diferentes planes institucionales para dar continuo cumplimiento de objetivos y metas del proceso y continuar soportando la operación de los diferentes procesos misionales de la entidad por medio de las TIC.
- Se prestó la asistencia y soporte técnico a usuarios de la entidad, según requerimientos, a través de la mesa de ayuda implementada, que reporta 3.462 solicitudes con un tiempo de atención de 20.910 horas y tiempo promedio de solución de 6,04 horas, manteniendo la meta del indicador que es igual o menor a 12 horas.
- Se apoyaron los reportes de información correspondientes a gestión informática.
- Se mantiene actualizada la sede electrónica, según las Resoluciones 1519-2020 y 2893-2020 del Ministerio de la Tecnologías de Información y las Comunicaciones MINTIC.
- Se mantienen actualizados los portales web de líneas temáticas.

Estrategias Implementadas Del PETI

El Plan de Tecnologías de la Información y las Comunicaciones 2020-2023 cuenta al corte del 31 de diciembre de 2023 alcanzó un avance del 95%.

	Proyectos		
	Área Líder	ID	Nombre de proyecto
Iniciativas de operación	Planeación	IO-001	Outsourcing TIC
		IO-002	Conectividad
		IO-003	Soporte Base de Datos Oracle

	Proyectos		
	Área Líder	ID	Nombre de proyecto
		IO-004	Soporte Software Geográfico Arcgis
		IO-005	Software Gestión Documental
		IO-009	Adquisición de Hardware
		IO-012	Correo Electrónico
		IO-013	Suministro de Repuestos
Iniciativas de Transformación	Planeación	IT-010	Alcance Informático del PIRMA

El Modelo Integrado de Planeación y Gestión MIPG, define las estrategias en esta materia, por lo que el Plan Estratégico de las Tecnologías de la Información y las Comunicaciones está estructurado con base en dichas estrategias, en ese orden de ideas la Corporación ha avanzado en los siguientes aspectos:

- Asegurar la disponibilidad y continuidad de los servicios tecnológicos, gestionando las necesidades de infraestructura tecnológica y los servicios informáticos requeridos para la operación de la entidad.
- Implementar acciones en el proceso TIC alineadas con estrategias institucionales y sectoriales para asegurar la generación de valor en la gestión y la satisfacción de los ciudadanos.
- Implementar y modernizar los sistemas de información de acuerdo con los objetivos institucionales para fortalecer las capacidades tecnológicas de la entidad.
- Trabajar en la implementación de la Arquitectura Empresarial de la Corporación en el marco de referencia impulsado por el Gobierno Nacional.

Seguridad y Privacidad de la información

Respecto a seguridad y privacidad de la información; está a cargo de la Subdirección de Planeación y Ordenamiento Territorial con el liderazgo del Comité Institucional de Gestión y Desempeño con funciones de Comité de Seguridad y Privacidad de la Información (CSPI); se han venido desarrollando las siguientes acciones:

- Actualización de Inventario de Activos de Información.
- Integración de documentos de seguridad en el PETI.
- Seguimiento de riesgos de seguridad de la información y digital.
- Seguimiento de indicadores de gestión seguridad de la información.

Se ha venido trabajando en políticas de seguridad de la información orientadas a la posterior implementación del Sistema de Gestión de Seguridad de la Información ISO27001.

En cuanto a infraestructura para la seguridad la entidad cuenta con un dispositivo firewall de marca Fortinet referencia Fortigate 100-D, que cumple la función de proxy, en el que se han configurado reglas de salida para los diferentes aplicativos.

La solución de antivirus para los equipos de la Corporación es ESET NOD32, el cual incluye una consola de administración instalada en los servidores, a través de la cual se monitorean los computadores conectados a la red de la Corporación. En esta consola se han configurado tareas de actualización de la base de datos, análisis y búsqueda de vulnerabilidades, así mismo se ha establecido la exigencia de vacunar cualquier dispositivo de almacenamiento externo que se conecte a los equipos.

d. FORTALEZAS DEL PROCESO

- Amplia experiencia y formación del Talento humano en las actividades relacionadas con las tecnologías de la información y comunicación.
- Se evidencia interés, compromiso y disposición de la Alta Dirección en la ejecución del PETI, teniendo en cuenta la asignación de recursos que ha permitido la ejecución de proyectos planeados.
- Se refleja una robusta infraestructura tecnológica de la entidad, la cual ayuda a mejorar los servicios de toda la comunidad institucional, soportada con licenciamientos de sistemas de información, mantenimiento de los softwares y plataforma para gestión documental, contabilidad, sistema integrado de gestión y página web.

e. RIESGOS DEL PROCESO

Actualmente el proceso Gestión de Servicios TIC; tiene identificados 4 riesgos en total: 2 de gestión, 1 de seguridad de la información y 1 de corrupción como se relaciona a continuación. Se puede evidenciar que los controles establecidos impactan la escala de probabilidad por lo que, en 3 de los cuatro riesgos identificados, la zonal de riesgo residual no cambio de nivel respecto a la zona de riesgo inherente.

De acuerdo a monitoreo realizado por la subdirección de planeación; como segunda línea de defensa; se establece que se cumple con los controles y que no durante la vigencia 2023 no se materializaron riesgos.

Identificador	Tipo de Riesgo	Causas	Zona inherente	Controles	Zona residual
Posibilidad de afectación reputacional por infraestructura tecnológica en mal estado y/o obsoleta debido a falta de mantenimiento y/o no renovar los equipos oportunamente	Gestión	* Tecnología - Infraestructura tecnológica en mal estado y/o obsoleta. * Tecnología - Falta de mantenimiento y/o no renovar los equipos oportunamente	ZONA RIESGO MODERADA	* Anualmente, el outsourcing de sistemas diseña el plan de mantenimiento preventivo y correctivo, con el fin de poder asignar plazos y recursos para su cumplimiento. * El outsourcing sistemas, como mínimo anualmente realiza seguimiento, reporte y proyección oportuna sobre las necesidades de renovación tecnológica, con el fin de priorizar para la correspondiente reposición * El Outsorcing de Sistemas, semestralmente realiza seguimiento al programa de mantenimiento de la infraestructura física que hace parte o soporta la plataforma tecnológica	ZONA RIESGO BAJA
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros a cambio de entregar o manipular información	Corrupción	* Talento humano - Influencia de particulares o terceros interesados Intereses políticos Acceso a herramientas por trabajo remoto sin controles	ZONA RIESGO EXTREMA	* Cada aplicativo cuenta con usuarios autorizados y contraseñas con el fin de que no todoas las personas puedan acceder a todo tipo de información	ZONA RIESGO EXTREMA
Posibilidad de afectación Reputacional por Indisponibilidad de los servicios de plataforma tecnológica debido a daño lógico en la infraestructura tecnológica, daño físico de equipos y/o no contar con los mecanismos tecnológicos para desarrollar trabajo remoto.	Gestión	* Tecnología - Indisponibilidad de los servicios de plataforma tecnológica. * Tecnología - Daño lógico en la infraestructura tecnológica, daño físico de equipos y/o no contar con los mecanismos tecnológicos para desarrollar trabajo remoto.	ZONA RIESGO MODERADA	* El outsourcing sistemas, realiza mantenimiento preventivo y correctivo a los servidores cada año, con el fin de prevenir daños que generen pérdida de información, quedando evidenciado en OD-CAM-010 Hoja de vida de equipos. * El outsourcing sistemas, de manera permanente, realiza monitoreo, actualización, depuración, parches de seguridad, afinamiento del firewall a los sistemas operativos, bases de datos, aplicativos, etc., con el fin de detectar cualquier situación que pueda causar la indisponibilidad de la plataforma tecnológica * El outsourcing sistemas, diariamente realiza copia de seguridad de la información que reposa en el centro de datos; la cual es revisada para verificar su eficacia y de lo cual se deja evidencia en el F-CAM-340 Monitoreo a la plataforma y registro de backups. * La subdirectora de planeación junto con el outsourcing sistemas anualmente, realizan una adecuada planeación de adquisición de herramientas tecnológicas quedando evidenciado a través del POAI y del PETI, en caso de requerir con urgencia alguna herramienta no contemplada en el POAI se realiza la solicitud de ajuste. * El outsourcing sistemas, permanentemente y con previa autorización apoya el acceso de los funcionarios a los aplicativos y demás información, lo cual queda evidenciado en las solicitudes de servicio a través de mesa de ayuda.	ZONA RIESGO MODERADA
Posibilidad de pérdida de la integridad de la información por ataques cibernéticos debido a Uso de redes y equipos que no están bajo el control de la corporación, por trabajo remoto y/o vulnerabilidad de seguridad de la plataforma tecnológica.	Seguridad de la Información	* Evento externo - Ataques cibernéticos. * Evento externo - Uso de redes y equipos que no están bajo el control de la corporación, por trabajo remoto y/o vulnerabilidad de seguridad de la plataforma tecnológica.	ZONA RIESGO MODERADA	* En caso de que se evidencie modificación no autorizada o pérdida de información, el outsuursing de sistemas realiza las gestiones necesarias para controlar el ingreso no autorizado y recuperar la información a través de copias de seguridad relizadas o información que se encuentre en la nube, con el fin de reducir el impacto, dejando evidencia en la atención del ticket a través de la mesa de ayuda * El outsourcing sistemas, periódicamente envía correos electrónicos difundiendo las buenas prácticas, para el correcto uso de plataformas tecnológicas, así como para el uso de redes y equipos que no están bajo el control de la corporación, con el fin de generar acciones preventivas durante el trabajo remoto o local. En caso de evidenciar ataque cibernético de alguno de los aplicativos de la corporación la incidencia será gestionada por el área de outsurcing sistemas de la corporación. * El outsourcing sistemas, de manera permanente realiza validaciones a través de diferentes actividades con el fin de identificar correcto funcionamiento de las plataformas y redes, quedando evidenciado en el sistema	ZONA RIESGO MODERADA

4. RECOMENDACIONES

- Avanzar en la implementación de carpeta ciudadano digital para el proceso de autoridad ambiental
- Avanzar en el cumplimiento de plan de mejoramiento atendiendo a las debilidades encontradas en la medición del IDI a través del FURAG
- Garantizar que los retos de la plataforma tecnológica planteados en el PETI 2020-2023, que no se cumplieron durante la vigencia de éste plan; se gestionen en el próximo plan, entre los cuales se encuentran:

    - Unificación de Base de Datos Institucional y/o herramienta unificada de trámites ambientales.
    - Implementación de Servicios Ciudadanos Digitales
    - Optimización del sistema de impresión, tendientes a la digitalización de documentos, iniciando con una prueba piloto

- Revisar a mediano plazo la posibilidad de implementación de la norma ISO 27001 “Sistema de Seguridad de la Información”; para determinar claramente qué es lo que debe proteger la entidad para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano; a partir de la identificación de activos de información; es decir todos aquellos elementos que tengan valor para la entidad en cada uno de los procesos (información física o digital, redes, aplicativos entre otros) y frente a ellos se analizan los riesgos inherentes de la seguridad de la información: Pérdida de la confidencialidad, Pérdida de la integridad y Pérdida de la disponibilidad, para establecer las acciones que minimicen éstos riesgos.

MARTHA VIVIANA DIAZ QUINTERO
Asesor de Dirección (E)
Con funciones de control interno