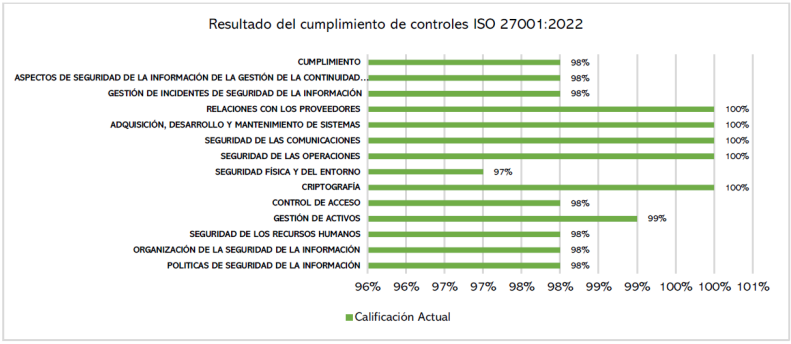
Informe de auditoría **Fecha: 2025-11-25, 12:33**

Objetivo de la auditoría :	Evaluar el diseño y efectividad de los controles internos en los procesos y procedimientos de la Corporación mediante la auditoria del proceso 0720 Gestion de Tecnologias de la informacion , con el proposito de analizar el nivel de cumplimiento y la gestión de la infomación, las aplicaciones y los recursos tecnológicos, asegurando la adecuada implementación y mejora continúa del Modelo de Seguiridad y Privacidad de la infomación (MSPI)
Alcance de la auditoría :	El alcance abarca la sede prinicipal, centros de computo, areas de servidores de aplicaciones, oficina de Tecnologías de la información OTI, servidores de archivos, la gestión de activos tecnológicos y otros espacios relacionados con el manejo de la administración de la información
Criterios de auditoría o parámetros normativos :	Los criterios a auditar son lo establecidos en las políticas, procedimientos, formatos y demás documentos que hacen parte del proceso de Gestión de las Tecnologías de la Información y la norma 27001 del 2022, Ley 1581 de 2012 Proteccion de datos personales, Ley 1712 de 2014 sobre la transparencia y acceso a la informacion publica, Resolución 500 de 2021 sobre linemaientos y estandares para la estratégia de seguridad digital del Ministerio de Tecnologías de la Información y las Comunicaciones
Metodología :	La Auditoria se realizará en forma presencial, se realiza la socialización del proceso de auditorias de sistemas con el equipo de funcionarios asignados, reasaltando la importancia de los hallazgos y sus consecuencias ante la gestión fe la información y continuidad del negocio con base en las auditorias anteriores. Una vez expuesto el proceso de la auditoria de sistemas al equipo de sistemas de la CVC, se realiza la visita en cada espacio de acuerdo con el acance, ejecutando la veritication del diseños implentación de buenas prácticas de seguiridad con los cambios técnicos y las respecitvas revisiones de la documentación de los procesos basados en los criterios expuestos.
	INFORME FINAL AUDITORIA AL PROCESO 0720. GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN La presente auditoria se adelantó bajo el criterio establecido en la Guía de Auditoría Interna Basada en Riesgos para Entidades Públicas emitida por el Departamento Administrativo de la Función Pública versión 4 de 2020, y la norma 27001 del 2022, por consiguiente, el equipo auditor procedió a utilizar las técnicas de entrevistas y visita en cada espacio de acuerdo con el alcance, ejecutando la verificación de los diseños implementación de buenas prácticas de seguridad con los cambios técnicos y las respectivas revisiones de la documentación de los procesos para identificar el cumplimiento de la norma general y la normatividad interna. **Desarrollo de la auditoria** Como criterio principal del proceso de seguimiento de la auditoria de sistemas en la Corporación Autónoma Regional del Valle del Cauca (CVC) fue alineado al cumplimiento del estándar ISO/IEC 27001:2022, la cual es una norma internacional que establece las mejores prácticas para la gestión de la seguridad de la información. Su objetivo principal es proteger la confidencialidad, integridad y disponibilidad de la información dentro de una organización a través de un Sistema de Gestión de Seguridad de la Información (SGSI). Se realiza entonces las siguientes actividades. • Revisión del documento de las Políticas de Seguridad Informática de la Corporación Autónoma Regional del Valle del Cauca (CVC), el cual se encuentra aprobado y publica en la intranet. • Verificación de la integración del Comité de seguridad de la información y las acciones para fortalecer los procesos de gestión de la seguridad de la información. • Exploración de los procedimientos para la asignación de equipos de cómputo al personal de la Corporación Autónoma Regional del Valle del Cauca (CVC). • Verificación del estado de los equipos de cómputos y servidores, plan de copias de seguridad y controles de acceso físicos/lógicos. • Revisión de las licencias de sistemas operativos y aplicaciones instaladas en las estaciones de trabajo, para este caso se tomaron 3 muestras aleatorias. • Comparación de planes de mantenimientos, licencias de software, inventario de activos fijos de cómputo y procedimiento para la ejecución de las copias de seguridad contra la documentación establecida La auditoría evidenció un nivel de cumplimiento superior al 97 % en los controles ISO 27001:2022, lo que demuestra el fortalecimiento de la gestión de seguridad de la información en la Corporación. **Revisión procedimientos PT.0720.24 – Gestión de Usuarios y PT.0720.29 Gestión de Incidentes de Seguridad** Durante la revisión hechas a los procedimientos PT.0720.24 – Gestión de Usuarios se evidenció incumplimientos parciales en algunas actividades, aspectos que se deben fortalecer para asegurar la trazabilidad y el cumplimiento procedimental. Entre ellos se destacan: Se identificó que las actividades del procedimiento están siendo ejecutadas principalmente por contratistas de Arquitesoft, sin la participación directa de un profesional especializado del área, tal como se contempla en el procedimiento. Este aspecto representa una oportunidad de mejora para fortalecer la coherencia entre lo establecido y la operación, así como para garantizar un acompañamiento técnico más robusto en el proceso. Se sugiere evaluar mecanismos que permitan integrar la intervención del profesional indicado. Falta de evidencias formales la aprobación o desaprobación en la autorización en la creación o modificación de cuentas. - Ausencia de actas de revisión anual de usuarios y permisos. - Registros de salida sin respaldados soportes documental físico o virtuales



Fuente. Informe de Auditoría Externa Revisoría Fiscal 2025

Contratación.

La muestra seleccionada de los contratos gestionados desde la Oficina de Tecnologías de la Información correspondió a dos (2) contratos de prestación de servicios, así:

COT	OBJETO	VALOR	ESTADO
287 -2025	Prestación de servicios profesionales para apoyar la gestión de la OTI en lo relacionado con el desarrollo, implementación uso y apropiación de la Plataforma de Gestión Ambiental PLIGA	74,676,602	En ejecución
470 - 2025	Gestión de servicios de Soporte en Tecnologías de información alineados con la Política de Gobierno Digital Verificado en Secop II	7,688,789,916.6	En ejecución

Fuente. Equipo Auditor

Las contrataciones seleccionadas se revisaron acorde con los procedimientos PT.0550.03: Contratación Directa Por Prestación de Servicios Profesionales y de Apoyo a la Gestión Versión 10 y PT.0550.35: Licitación Pública Bienes y Servicios Versión 2, encontrando ajustada la normatividad Ley 80, ley 1150, Decreto 2474 de 2008, Decreto 1510 de 2013 y procedimientos internos, así como los soportes anexos a los informes parciales de avance de las prestaciones de servicios.

Sin embargo, al momento de la entrega de expedientes para realizar la revisión en el marco de la auditoría, por parte de los responsables de los contratos, se encontró que no se diligencia la hoja de control ni estan foliados los expedientes por lo cual fueron objeto de devolución y nueva entrega.

Desarrollo de la auditoría :

Cumplimiento Políticas FURAG

Durante el desarrollo de la auditoría de Gestión de Tecnologías de la Información se evaluó el grado de cumplimiento de los lineamientos establecidos por el FURAG, considerando los modelos: Modelo de Arquitectura Empresarial (MAE), Modelo de Gestión de Gobierno de Tecnologías de la Información (MGGTI), Modelo de Gestión de Proyectos de Tecnologías de la Información (MGPTI), la adopción del protocolo de internet IPv6, la implementación de Trámites y Servicios Ciudadanos Digitales y el cumplimiento normativo en materia de protección de datos personales.

- **Cumplimiento de Modelos MAE, MGGTI y MGPTI**

La entidad cuenta con una Arquitectura Empresarial (MAE) definida y aprobada, soportada en documentos institucionales y planes de transición que orientan la alineación estratégica de las tecnologías de la información. Aunque estos instrumentos existen y están formalmente adoptados, se identifican una debilidad asociada a la actualización oportuna de los inventarios y a la necesidad de reforzar los mecanismos de articulación entre la planeación estratégica y los desarrollos tecnológicos.

En cuanto al Modelo de Gestión y Gobierno de TI (MGGTI), la Corporación dispone de actos administrativos que definen roles, responsabilidades y políticas internas para la gestión tecnológica. La información reportada en el FURAG muestra avances en madurez, con lineamientos que han sido formalmente adoptados. No obstante, la auditoría evidenció que aún existe una debilidad derivados de la no actualización de algunos insumos particularmente inventarios de hardware y direccionamiento IP lo cual puede limitar el fortalecimiento frente a la información reportada en el FURAG.

Frente al Modelo de Gestión de Proyectos de TI (MGPTI), la entidad mantiene matrices de seguimiento y cierre que permiten evidenciar trazabilidad de proyectos, cumplimiento de etapas y gestión documental asociada.

- **Adopción del Protocolo IPv6**

En el marco de las obligaciones, recomendaciones del FURAG para la política de Gobierno Digital, la auditoría analizó las acciones adelantadas por la entidad para la adopción de IPv6. Se constató que se mantiene un Inventario de Activos de Información actualizado, con clasificación por tipo de activo, propietario, ubicación y nivel de confidencialidad. Sin embargo, se identificó una debilidad documentada: en una revisión reciente, el inventario de equipos presentaba inconsistencias en seriales y direcciones IP, y no existe evidencia de que el inventario identifique explícitamente la compatibilidad de cada equipo, sistema o servicio con IPv6.

En materia de direccionamiento, la planificación contempla escenarios de coexistencia entre IPv4 e IPv6 (dual stack, túneles y NAT64), lo que favorece una transición progresiva y garantiza la continuidad operativa. La entidad ha incorporado la adopción de IPv6 dentro de proyectos de inversión, evidenciándose contratos orientados a modernización de red, soporte a protocolos IP, capacitación del personal y actualizaciones de hardware y software especializados.

Respecto al Plan de Contingencias, se verificó que no solo está formalmente diseñado, sino que también ha sido probado y simulado, con evidencias de entrenamientos, registros de simulacros, validación periódica y actualización derivada de las pruebas. Este componente representa una fortaleza importante en la preparación institucional para interrupciones o incidentes.

Finalmente, el acta de cumplimiento de las fases 2 y 3 del proceso de adopción de IPv6 cuenta con evidencias técnicas completas, tales como capturas de configuración, bitácoras, reportes de pruebas de funcionalidad, registros de capacitaciones y documentos de monitoreo, lo que respalda la veracidad de los avances reportados.

- **Trámites Digitales y Servicios Ciudadanos – Decreto 620 de 2020**

La entidad ofrece trámites parcialmente y totalmente en línea a través de su portal institucional, y presenta avances significativos en la transición hacia modalidades 100 % digitales en la entrega de los resultados de 5 tramites ambientales que adelanta la Corporación, apoyándose en herramientas del ecosistema GOV.CO y en los Servicios Ciudadanos Digitales.

	Se evidenció que la entidad realiza medición sistemática de satisfacción del usuario mediante encuestas y analítica web integrada en la sede electrónica, resultados que son utilizados para identificar puntos de mejora y fortalecer la experiencia ciudadana. Aunque la autenticación digital del ecosistema GOV.CO no se utiliza debido a la naturaleza del portal, orientado principalmente a trámites de consulta y generación de solicitudes pública, la entidad sí presenta avances relevantes en la implementación de la Carpeta Ciudadana Digital, siendo una de las pocas entidades de su tipo en incorporar este mecanismo en trámites específicos. Los informes de gestión reflejan una reducción en los tiempos de respuesta y en el consumo de papel, coherente con lo reportado en el FURAG y con políticas ambientales de sostenibilidad. También se evidencian mecanismos funcionales de interoperabilidad con otras entidades por medio de los Servicios Ciudadanos Digitales. • **Cumplimiento Normativo: Protección de Datos Personales (Ley 1581 de 2012)** La auditoría verificó el cumplimiento de los requisitos legales en materia de tratamiento de datos personales, encontrando que la entidad mantiene una Política de Protección de Datos Personales alineada con la Ley 1581 de 2012 y el Decreto 1377 de 2013, con procedimientos específicos para el manejo, acceso y supresión de la información personal. Existen controles técnicos y organizacionales para garantizar confidencialidad, integridad y disponibilidad, con asignación clara de responsabilidades y mecanismos de acceso para titulares. Se realizan actividades de capacitación y sensibilización al personal, y se mantienen procesos para el ejercicio de derechos de los titulares de datos, así como los reportes obligatorios al Registro Nacional de Bases de Datos. **Seguimiento al cumplimiento de planes de mejoramiento suscritos con la Contraloría General de la Republica y Planes de mejora resultado de Auditorias Internas** Actualmente la Oficina de Tecnologías de la Información cuenta con una actividad derivada del plan de mejoramiento a la Auditoria Especial “Auditoria utilización y uso del aplicativo Ventanilla Integral de Tramites en Línea (Vital)-2022” realizada por la Contraloría General de la República, la cual consiste en. Formular una estrategia para dar continuidad a las acciones entre la CVC y el Ministerio de Ambiente y Desarrollo Sostenible para la integración entre el Sistema Corporativo y VITAL. Se encontró que para la implementación de las Políticas de Gobierno en Línea, se realizarán ejercicios de caracterización con las entidades, con el ánimo de adoptar estrategias diferenciales en términos de gradualidad y acompañamiento, sin dejar de lado los contextos de operación y ajustando procesos de transformación digital a la medida, es así como para la interoperabilidad con otro sistemas, no solo VITAL, se encuentran a espera de la aprobación por parte de las entidades competentes, existiendo evidencias de mesas de trabajo con las entidades competentes y con entidades de la misma naturaleza para su implementación. Esta acción se tiene como fecha de vencimiento 30/11/2027. Con respecto a las actividades originadas en la auditoria hecha al proceso en la vigencia 2024, se dejó como oportunidad de mejora “Establecer los controles necesarios a efecto de mantener la continuidad de la empresa para proteger sus operaciones y servicios en caso de que se presenten eventos imprevistos y reducir el impacto de las interrupciones en las actividades de los procesos Corporativos”, para lo cual se suscribieron 7 actividades 3 de las cuales se encuentran cerradas en aplicativo Daruma con sus correspondientes evidencias, alcanzando un porcentaje de avance de 43% dentro del término que vence el 30/11/2025. Se encuentran pendientes por ejecutar las siguientes actividades suscritas. • Identificar las zonas seguras del Data Center y centros de cableado, marcando las restricciones de acceso y aplicando controles de acceso a las mismas • Proponer a la Dirección General, crear el Comité de Gestión de Seguridad de la Información y articularlo al SGSI de la CVC. • Proponer a la Dirección General, Oficina Asesora de Jurídica y a la Dirección Administrativa y de Talento Humano, incluir la suscripción de Acuerdos de Confidencialidad y No Divulgación de información, como requisito para la posesión de funcionarios y la suscripción de contratos de prestación de servicios. • Gestionar los Activos de Información a cargo de la OTI desde el Módulo de Activos de Información en Daruma Software Al respecto el auditor (experto técnico) pudo identificar que, en aplicativo DARUMA se encuentra la relación de activos de información, sin embargo, queda pendiente vincularlos al módulo de gestión de riesgos del mismo aplicativo para consolidar la gestión de activos de información en una misma herramienta. En cuanto a la gestión de activos de cómputo, equipos de infraestructura y redes de comunicación en la CVC se encuentra gestionada por herramientas personalizadas integradas al monitoreo en tiempo real desde la mesa de servicio, siendo esta una práctica avanzada y efectiva para el control y seguridad tecnológica. Sin embargo, se exhorta a la Oficina de Tecnologías de la Información a gestionar el Plan de Mejora Institucional con el fin de dar cumplimiento a las actividades relacionadas que no presentan avances. Es necesario señalar que la no atención oportuna de estas recomendaciones representa un riesgo residual que, de no ser tratado, podría derivar en futuras No Conformidades si las debilidades son materializadas, comprometiendo así la confidencialidad, integridad o disponibilidad de los activos de información críticos para la Corporación **Gestión de Riesgos de la Oficina de Tecnologías de la Información** Se evidencia que los mapas de riesgos de gestión y de corrupción no han sido actualizados conforme a la Política de Administración del Riesgo – Resolución 0100 No.0550-0368-2024, la cual establece la obligación de revisión y actualización anual, así como la definición específica de controles para cada riesgo identificado. En ambos instrumentos, el apartado de controles no refleja acciones verificables ni medibles, y la redacción de los riesgos no se ajusta a la metodología institucional, ni a la guía del DAFP.
Análisis de riesgo :	Inoportunidad o falta de entrega de documentos fisicos y virtuales

Conclusiones, hallazgos y/o recomendaciones :	• **CONCLUSIONES** Se evidenció que la Corporación Autónoma Regional del Valle del Cauca (CVC) mantiene un Sistema de Gestión de Seguridad de la Información (SGSI) consolidado, documentado y en constante evolución, alineado con la ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información (MSPI). Los resultados reflejan una gestión madura en la protección de la información, la infraestructura tecnológica y la continuidad del negocio, con una calificación de cumplimiento superior al 97 % en los controles verificados. El proceso auditado demuestra un avance significativo en los componentes evaluados por el FURAG, particularmente en los ejes de Gobierno Digital, Seguridad y Privacidad de la Información, y Gestión de TI. Durante la Auditoria, no se identificaron No Conformidades. Se reconocen y destacan como fortalezas los significativos avances en la madurez de los controles de seguridad implementados en la infraestructura física y lógica, lo cual demuestra un compromiso con la mejora continua del SGSI, conforme a la política de la entidad. **OPORTUNIDADES DE MEJORA** • OM 1. Se recomienda establecer y documentar áreas seguras —como los centros de datos y los cuartos de comunicaciones— dentro de las instalaciones de la Corporación Autónoma Regional del Valle del Cauca (CVC). Esto constituye un requisito esencial para garantizar la protección física de los activos de información y de la infraestructura tecnológica que los soporta. • OM 6. Se sugiere establecer indicadores específicos que permitan medir el avance real de la implementación de IPv6 (fase 2 y 3), tales como porcentaje de equipos configurados, servicios migrados, pruebas completadas, incidentes reportados y niveles de disponibilidad. • OM 7. Se recomienda ajustar el procedimiento PT.0720.24 Gestión de usuarios, pues se evidencia que el responsable de las actividades técnicas es el profesional especializado, pero al contrastarlo con la realidad encontrada, son actividades desarrolladas por el contratista a cargo, por lo cual no existe coherencia entre lo establecido y la operación. • OM 2. Es recomendable crear el Comité de Gestión de Seguridad de la Información como el mecanismo formal mediante el cual la Alta Dirección puede demostrar liderazgo y compromiso con el Sistema de Gestión de Seguridad de la Información (SGSI), en cumplimiento de la Cláusula 5.1 de la norma ISO 27001:2022. • OM 3. Se recomienda incorporar la Política de Seguridad de la Información - PSI y sus requisitos en todas las etapas del ciclo de vida del personal: antes del ingreso, durante la permanencia y al finalizar la relación contractual. Esta integración es un componente obligatorio del SGSI y corresponde a controles auditables definidos en el dominio de Controles de Personas (Anexo A.6) de la norma ISO 27001:2022. • OM 4. Se recomienda adelantar un proceso integral de actualización y depuración del Inventario de Activos de Información de la Corporación Autónoma Regional del Valle del Cauca (CVC), garantizando que cada equipo, sistema y componente de red cuente con información completa, precisa y verificable. La actualización debería incluir seriales, direcciones IP, propietario del activo, estado operativo y cualquier atributo requerido para su clasificación. • OM 5. Es recomendable incluir, dentro del Inventario de Activos de Información, la identificación explícita de compatibilidad con IPv6 para todos los equipos, sistemas, aplicaciones, servidores y servicios tecnológicos. Este atributo debe convertirse en un campo obligatorio dentro de la gestión de activos. Su inclusión permitirá evaluar la madurez de la infraestructura frente a los requerimientos de la Política de Gobierno Digital, reducir riesgos de obsolescencia y facilitar la planificación técnica asociada a la transición del protocolo IPv4 a IPv6
Firmas :	JAIME ALBERTO ESCUDERO JIMENEZ - Jefe Oficina de Control Interno

Firmas	Nombre	Cargo	Fecha
Coodinador	JAIME ALBERTO ESCUDERO JIMENEZ	JEFE DE LA OFICINA DE CONTROL INTERNO (C)	
Auditado	ALBERTO NOE GIRALDO SANCHEZ	PROFESIONAL ESPECIALIZADO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION	
Auditado	DIEGO ALEXANDER MILLAN LONDOÑO	JEFE DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION	
Auditor	PAULA ANDREA POSSU CATACOLI	PROFESIONAL ESPECIALIZADO DE LA OFICINA DE CONTROL INTERNO	
Auditado	EDWIN RUANO GAMBOA	PROFESIONAL ESPECIALIZADO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION	
Auditor	JUAN MANUEL TORO MONTOYA	PERSONAL DE APOYO OFICINA DE CONTROL INTERNO	